

Execução Centralizada, Caos Descentralizado: A Força Aérea Está Programada para Perder A Guerra Cibernética

1ST LT JOHN COBB, USAF*

Uma só vitória [a Operação Desert Storm] varreu todos os problemas por debaixo do tapete. A liderança dos EUA em armamento e tecnologia moderna, jamais desafiada, encobre o fato de que sua organização e estratégia são obsoletas, deixando de manter passo com a tecnologia.

—Qiao Liang e Wang Xiangsui, *Unrestricted Warfare*

NA SITUAÇÃO ATUAL de guerra cibernética, redes centralizadas maciças são, na melhor das hipóteses, frágeis e muitas vezes indefensíveis.¹ O paradigma das operações em rede da Força Aérea [*Air Force's Network Operations – AFNETOPS*] depende de controle ciberespacial centralizado. Embora supostamente adequado à manutenção e contra-inteligência durante “paz ciberespacial”, poderia vir abaixo, de forma espetacular, caso colocado à prova em sério ataque cibernético.

Atualmente, a Força Aérea depende de um punhado de equipes da 67ª Ala de Guerra em Rede [*67th Network Warfare Wing – 67 NWW*] para controlar a maioria dos aspectos de defesa.² Esta consolidação ocorreu devido a: redução em mão-de-obra; benefícios decorrentes do estabelecimento de equipe de comando em todo o ciberespaço; redução em treinamento e seu grande consumo de tempo; táticas, técnicas e procedimentos de defesa. Contudo, ao buscar a unificação de comando, a Força Aérea, quase que por completo, abandonou a execução descentralizada, deixando seu ciberespaço vulnerável a uma variedade de ataques que poderiam isolar as redes locais dos grupos, da rede central. Para complicar a situação, esse problema é o que faz com que a

maioria dos Militares da Força Aérea não fique ciente dessas vulnerabilidades, cegamente assumindo que os ataques cibernéticos inimigos jamais afetarão sua esfera de ação. O paradigma atual da *AFNETOPS* deve dar lugar a modelo mais eficaz em defesa de rede. A Força deve tomar dois passos específicos para atenuar os riscos de falha de rede e, por conseguinte, da missão, através de todo o domínio. (1) Os operadores cibernéticos nas Bases devem possuir a habilidade de manter as redes em funcionamento e reagir a ataques de grupos mais sofisticados. (2) As Alas devem levar a efeito exercícios, durante os quais operam em cenários de isolamento, degradação e quedas de rede.

O *AFNETOPS* inclui grupos responsáveis pelas operações de rede e defesa. A 24ª Força Aérea [*Twenty-Fourth Air Force*] é responsável pela maioria dos aspectos cibernéticos, bem como quase toda a administração da rede. Dentro da 24ª, a 67 *NWW* responsabiliza-se pela maioria da defesa. Dentro daquela Ala, os grupos principais de defesa incluem os Centros de Operações de Rede Integrada e Segurança [*Integrated Network Operations and Security Centers – INOSC*], Equipe de Reação à Emergência Informática da Força Aérea [*Air Force Computer Emergency Response Team –*

*Atualmente, o autor desempenha as funções de Oficial Encarregado do *Information Engineering Branch* no Quartel-General da Universidade da Aeronáutica [*Headquarters Air University*]. Anteriormente desempenhava as funções de Oficial Encarregado de Operações em Rede e fazia parte do *Misawa Blue Team* para o 35º Esquadrão de Comunicações, Base Aérea Misawa, Japão.

AFCERT], o 624º Centro de Operações [*624th Operations Center*] e o 26º Esquadrão de Operações de Rede [*26th Network Operations Squadron*]. Especificamente, os dois *INOSCs*: responsabilizam-se pelas regiões geográficas *INOSC Leste* e *INOSC Oeste* [*INOSC East* e *INOSC West*]; configuram e operam os serviços básicos das redes da Base em seu domínio; responsáveis pela maior parte da proteção da Base; e dispositivos de segurança da rede (o *INOSC* opera a maioria das ferramentas e dispositivos de programas de defesa, embora às vezes estejam fisicamente localizados na Base local). Os peritos da *AFCERT* “diagnosticam e tratam” vírus e outros tipos de tecnologia maliciosa durante emergências da rede. O [*624º Centro de Operações*] mantém-se ciente da situação cibernética da Força Aérea (inclusive todas as questões principais de rede) para a 24ª Força Aérea e todos os outros comandantes pertinentes. Finalmente, o 26º Esquadrão de Operações da Rede [*26th Network Operations Squadron*] é responsável pela segurança e superintendência geral. Por exemplo, se a Base X for infectada por vírus, o *INOSC* cerra parte das “entradas e saídas” da rede (portais de defesa), tentando consertar qualquer dano causado. O *AFCERT* ajudará a identificar a agressão, providenciando contramedidas. O *624th Operations Center* fornecerá a coordenação e manterá os comandantes a par da situação.

A maior parte dos serviços fundamentais de rede em toda a Força Aérea é controlada por essas dependências centralizadas. Embora os técnicos da Base talvez controlem grande parte das funções rotineiras, tais como a modificação de contas e a adição de novo equipamento à rede, somente o pessoal da 67 *NWW*, fora do local, pode tratar de questões e mudanças maiores, porque o acesso do administrador que se encontra na Base não está configurado para permitir que os técnicos locais modifiquem os servidores ou serviços básicos.³ Uma vez que os destacamentos da 67 *NWW* tipicamente residem em uma só Base por comando, dependem de boas conexões entre as Bases para cumprir com a missão.⁴ Os técnicos da Base são um tanto similares aos empregados de postos de gasolina que lavam

e reabastecem os carros. Entretanto, não possuem o equipamento para levar a cabo consertos maiores. O emprego deste tipo de abordagem centralizada de defesa de rede de plantão, pressupõe que as equipes de reparos conseguem alcançar o posto menos acessível, a fim de auxiliar um consumidor cujo “veículo” foi danificado por agressores. Além do mais, esse conceito deixa postos distantes desprevenidos, quando agressores enfocam-se em vias de acesso, impedindo que as equipes obtenham acesso para assistir ao “motorista” abandonado.

Quando a infraestrutura da rede da Força Aérea não se encontra sob ataque, o serviço centralizado da rede, causa certa frustração, mas funciona relativamente bem. Contudo, se economiza dinheiro e mão-de-obra, quando comparado a possíveis alternativas, é algo discutível. Entretanto, em face de sério ataque cibernético, esse modelo cairá aos pedaços. O conceito da *AFNETOPS* é a personificação da execução centralizada, com debilidades operacionais que a acompanham, tais como reação apática aos comandantes locais, demoras em aprovação e execução de mudanças, bem como dificuldade em adaptar práticas e equipamento padronizados a locais fora do normal. O pior é que deixa as redes da Base paralisadas, se ficarem isoladas de redes de mais alto nível ou, especificamente (se ficarem isoladas de acesso administrativo de nível hierárquico mais elevado).

Qual é a probabilidade de isso acontecer? Durante guerra cibernética é praticamente inevitável. A Força Aérea arrenda a maior parte dos “circuitos” que conectam as Bases, de companhias particulares de telecomunicações. Esses circuitos são vulneráveis à ataques de negação distribuída de serviço [*distributed denial of service – DDoS*] de *botnets* hostis. [Os *botnets* são aglomerações de milhões de computadores sequestrados, utilizados simultaneamente, para atacar certo alvo. É o equivalente à interferência de rádio]⁵ As linhas arrendadas não são o único problema. Os ataques *DDoS* também podem ter como alvo as fortificações (*firewalls*) e roteadores, onde as redes da Força Aérea conectam-se pelo mundo afora. Como demonstrado pelo isola-

mento da Estônia em 2007, a tecnologia nem sempre permite rápida reação a grandes ataques *DDoS* contra as conexões de longa distância entre locais físicos (especialmente em engarrafamentos principais, tais como cabos transoceânicos).⁶ Deve-se notar, contudo, que existem defesas contra ataques *DDoS* (muitas vezes são variações de bloqueio de tráfego de outras partes da *Internet* ou de toda a *Internet*). Contudo, não é garantia.⁷ Um inimigo cibernético capacitado não limitará os ataques à mera porção isolada de redes da Base que, se não fosse por isso, continuaria funcionando.

O ataque *DDoS* é mero método de sabotagem de rede da Base. A hierarquia da rede da Força Aérea também é vulnerável a simples ataque cibernético. O inimigo consegue, facilmente, concentrar-se em nossas vulnerabilidades, degradando, assim, as redes, em preparativos de ataque *DDoS* ou em lugar do mesmo. Se o adversário consegue infectar a vírus, alguns computadores, até mesmo aqueles simples e rudimentares, pode também aleijar a rede, simplesmente sobrecarregando-a com mais tráfego do que pode comportar. (Esse tipo de negação de serviço difere de *DDoS*, no qual a sobrecarga advém da rede da vítima e normalmente têm como alvo dispositivos de limites exteriores que conectam a rede da vítima à *Internet*.) Normalmente, esse tipo de ataque de negação de serviço, inclui *phishing* para implantar o vírus. Requer certa habilidade, a fim de evitar as defesas da rede. Sua execução é difícil, se todos os computadores da rede estiverem recebendo as atualizações e os reparos corretos.⁸ Infelizmente, tanto as diferentes nações como delinquentes possuem a habilidade de lançar ataques de negação de serviço. A maioria das redes da Força Aérea (inclusive as mantidas pelo autor) possuem equipamento em listas de espera de semanas e meses para as atualizações necessárias.⁹ Com frequência, o equipamento mais importante é o menos seguro. Isso ocorre porque os técnicos, preocupados que os reparos romperão a logística ou o agendamento da base de dados, acabam recusando as atualizações de segurança necessárias, durante meses a fim. De qualquer modo, quando alguns

computadores são infectados e começam a “expelir o tráfego” (com o rápido envio de grandes quantidades de dados, acabam inundando a rede. Os exercícios de segurança passados sugerem que até mesmo os ataques de *phishing* mais mal concebidos encontram lá seu par de vítimas, enquanto que os ataques mais sofisticados são devastadores.¹⁰

Atualmente, as permissões necessárias (acesso administrativo), a experiência prática e treinamento exigidos para reagir a ataques, encontram-se somente nas equipes da 67 NWW.¹¹ Se, contudo, um ataque saturar dada rede (os computadores infectados enviam tantos dados que pessoa alguma consegue estabelecer uma conexão com o equipamento na rede da vítima), os administradores de fora descobrirão sua completa impotência, quando tentarem prestar assistência. Toda rede conta com engarrafamentos e pontos de estrangulamento: os dispositivos que conseguem acomodar somente certa quantidade de dados por segundo; servidores que podem acomodar somente uns poucos milhares de conexões cada vez; e os dispositivos de segurança que bloqueiam o tráfego, quando a fila de inspeção de matriz de dados for demasiadamente longa. Quando esses pontos alcançam saturação, os segmentos da rede são desconectados uns dos outros e do resto do mundo. As ferramentas utilizadas pelos técnicos (em todos os níveis), a fim de manter e reparar as redes fracassarão, incapazes de conectar-se com computadores distantes (quer seja no continente ou do outro lado da rua). Dependendo da quantidade de equipamento infectado, os efeitos do ataque variam, de alguns prédios sem conexão, à maioria do pessoal da Base incapaz de inicializar o computador [*log in*]. Em casos mais sérios, os técnicos conseguem solucionar o problema somente ao remover, fisicamente, o equipamento infectado para proceder com o reparo. Uma vez que a manutenção da rede moderna é feita, na maioria, via acesso remoto, para que alguém consiga encontrar e consertar o equipamento infectado, em pessoa, vai levar dias e até mesmo semanas, assumindo que os técnicos “da casa” possuam as ferramentas corretas para o conserto, após encontrar o equipamento infectado.

As investidas cibernéticas, acima mencionadas, são relativamente fáceis, executadas por uma só pessoa ou pequeno grupo de *hackers*. Um país com programa de guerra cibernética mais sólido consegue lançar agressões muito mais sofisticadas, capazes de controlar e até mesmo destruir grande quantidade de equipamento. De rotina, dentro de um mês, descobrimos mais de uma dezena de falhas de segurança em programação utilizada pelos computadores normais do Departamento de Defesa.¹² Um ataque baseado em uma dessas vulnerabilidades, antes do reparo ser autorizado, alastraria-se durante horas ou mesmo dias antes que os técnicos pudessem reassumir controle. É possível que cause interrupção da rede durante dias e mesmo semanas, dependendo em grau e alcance do dano (regional ou mundial).¹³

Se existe a probabilidade dessas investidas mais sofisticadas de diferentes nações em qualquer tipo de guerra cibernética – e futuros conflitos incluirão tanto batalhas cinéticas como cibernéticas – que preparativos podemos fazer?¹⁴ Devemos tomar dois passos importantes para atenuar o impacto desses ataques cibernéticos à Força Aérea. Em primeiro lugar, descartar o paradigma *AFNETOPS* atual, que pressupõe que os peritos centralizados tomarão conta do recado em período de guerra. Esses especialistas estarão inundados e isolados da maior parte das Bases que necessitam de ajuda. Os técnicos nas Bases requerem treinamento e experiência para combater ataques maiores, quando a Base ficar isolada. Além do mais, devem ter acesso administrativo, com privilégios suficientes para atuar como a “assistência de primeiros socorros cibernéticos”, sem depender de especialistas da *67 NWW*. Em segundo lugar, a Força Aérea deve aprender a operar durante degradação e interrupção de serviço.

Há meios para dar aos técnicos locais da Base as ferramentas e treinamento de que necessitam, sem perturbar a cadeia de comando cibernético. Por exemplo, incentivar as equipes de comunicação da Base a manter pequenas redes de treinamento ou exercício, oferece a acesso à habilidade dos técnicos residentes. A FA deve assegurar-se de que cada

Base conta com mais de uma dezena de dispositivos de rede e computadores com configurações aprovadas pela *67 NWW*. Esses sistemas simulariam e defenderiam contra ameaças, possivelmente com a assistência de equipes de inteligência ou agressoras. Servindo de “simuladores de voo cibernético” para os agentes de *primeiros socorros*, dariam aos residentes a prática essencial em como lidar com cenários de ameaça local e operar rede quando o apoio do mais alto nível for suspenso.

Talvez ao darmos a esses técnicos demasiado controle sobre a rede durante emergências, acabamos aumentando o número de ameaças ao grupo de comando. Mesmo assim, necessitam acesso administrativo para completo controle da rede da Base. Este acesso não deve ser usado – ou mesmo estar disponível – durante operações rotineiras. Contudo, é essencial em caso de ataque. Finalmente, a FA deve considerar treinamento de alto nível em defesa de rede para grande número de técnicos indispensáveis, para que possam combater tais ataques. Embora dispendioso, o *status quo* não é suficiente para defender o ciberespaço. Se a decisão acerca da *AFNETOPS* for firme, o próximo passo será providenciar defensores de rede com o treinamento e a experiência necessários para utilizar as ferramentas de forma eficaz. Caso contrário, as redes continuarão sendo vulneráveis, não importa quem esteja em controle do acesso administrativo. A FA deve corrigir as sérias vulnerabilidades, como já mencionado. Ameaçam isolar as redes da Base da hierarquia da rede. O acesso, durante emergências, aumenta muito mais a chance de sobrevivência cibernética.

Em última análise, tal sobrevivência é importante, em vista das missões que permitem ao longo de todos os domínios. Se a falha da rede ocorrer, devido a perda de ferramentas que permitem aos centros de operações aéreas ficarem cientes da situação, o colapso da logística de prontidão ou demora em sistemas de alerta da Base, leva a rápido declínio em eficácia para a maioria dos destacamentos aéreos.¹⁵ Por conseguinte, não só os técnicos da rede, mas também os Militares da Força Aérea, devem estar preparados para combates cibernéticos, adaptando-se à situação e aprendendo

dendo a operar sob ataque. Até mesmo quando os técnicos conseguem consertar o pior do dano, horas, provavelmente dias passarão, antes da volta à operação normal. Durante treinamento os pilotos aprendem a desempenhar as funções de forma tática, sem comunicações. Mesmo assim, poucas são as Alas que oferecem aprendizado em como lidar com isolamento de rede, degradação ou interrupção de operações. As Alas individuais (especialmente as de voo e equivalentes) devem corrigir tal omissão, avaliando, periodicamente, como operar frente a ataque cibernético. Talvez requeira a simulação de interrupções de sistema, infectando a rede com vírus artificial, imitando interrupção em comunicações durante horas e dias, continuando a desempenhar as funções em face de sistemas corrompidos. Fazer com que toda uma Ala tome parte em exercício, durante o qual o grupo agressor lança ataques cibernéticos reais, possa ser um tanto fora da real. No entanto, a maior parte dos esquadrões de comunicações da Base podem simular efeitos

criados por ataques cibernéticos. Ao praticar a projeção do poder aéreo ao longo de vários dias, controlando, ao mesmo tempo, pouco ou nenhum acesso à rede, as Alas conseguem estar preparadas para futuros conflitos que provavelmente incluirão ataques cibernéticos que causarão confusão.

Uma vez que grandes ataques cibernéticos farão parte normal de guerras em futuro próximo, a Força Aérea deve adaptar-se de acordo, a fim de manter a segurança nacional nesse novo ambiente. Ao reduzir a supercentralização da estrutura *AFNETOPS* atual, treinando todos os Militares da Força a desempenhar as funções, apesar do dano à rede, reduzimos o impacto de ataques cibernéticos e asseguramos que a degradação não produzirá falhas catastróficas à missão. Em suma, tanto os usuários, quanto os técnicos devem estar preparados e compreender os efeitos associados e as limitações que serão obrigados a encarar. □

Maxwell AFB, Alabama

Notas

1. Ver Qiao Liang e Wang Xiangsui, *Unrestricted Warfare* (Beijing: People's Liberation Army Literature and Arts Publishing House, February 1999). (Tradução do autor, com a assistência de Man Tsang.) Para tradução do texto completo ao Inglês, ver "PLA Colonels: 'Unrestricted Warfare': Part I," em "Chinese Doctrine," Federation of American Scientists, <http://www.fas.org/nuke/guide/china/doctrine/unresw1.htm>. Redigida em reação à Operação Desert Storm e à conversão dos EUA à guerra rede-cêntrica, *Unrestricted Warfare*—obra clássica moderna acerca da teoria militar chinesa, considera como a China (e seus pares) podem negar aos EUA vantagens tecnológicas e táticas, via várias estratégias assimétricas. Embora nem todas as predições dessem certo, a obra foi, sob muitos aspectos, visionária, um dos primeiros textos em chinês acerca da guerra cibernética.

2. A doutrina da Força Aérea define a *defesa de rede de computadores* como "actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the Department of Defense [DOD] information systems and computer networks." Documento Doutrinário da Força Aérea [Air Force Doctrine Document – AFDD] 3-12, *Cyberspace Operations*, 15 July 2010, 52, <http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-12.pdf>. Notar que o glossário de operações cibernéticas re-

cém publicado pelo Gen James E. Cartwright, USMC, emprega o termo *cyber defense* [defesa cibernética]; para a maioria dos efeitos, os termos são sinônimos. "Joint Terminology for Cyberspace Operations" (Washington, DC: Joint Staff, [November 2010]), 6, <http://www.nsci-va.org/CyberReferenceLib/2010-11-Joint%20Terminology%20for%20Cyberspace%20Operations.pdf>.

3. O termo "técnicos de Base" [*base-level technicians*] refere-se aqueles que mantêm a rede da Base local, tipicamente os membros do esquadrão de comunicações da Base, muitas vezes aqueles em posições, tais como operações de rede / centro de controle da rede, foco de comunicações, garantia cibernética e transporte cibernético. Neste artigo, os termos "residente", "base" e "técnico", correspondem, bem como "administradores" e "técnicos de rede", referindo-se aos Militares que operam e mantêm as redes. Para simplificar, o texto omite as funções dos destacamentos da *Defense Information Systems Agency*, agora parte do *US Cyber Command*. Certas ações atribuídas à 67 NWW são, na verdade, desempenhadas pelos destacamentos do Comando Cibernético [*Cyber Command*] (normalmente solicitadas e coordenadas através do pessoal da 67 NWW). Em geral, esses destacamentos são tão centralizados como aqueles da 67 NWW. Os problemas descritos neste artigo são os mesmos, não importa quem

esteja encarregado: o centro de operações de rede; ou o centro de operações de segurança. O Capítulo 2 da *AFDD* 3-12, *Cyberspace Operations*, descreve a relação básica.

4. Por motivos históricos, cada comando principal geralmente conta com destaqueamento *INOSC* que se encarrega dos aspectos mais rotineiros dos serviços básicos da rede em todo o comando.

5. Alguns especialistas especulam que os ataques recentes, atribuídos à Coreia do Norte foram ataques deste tipo, colocados à prova. Ver Elinor Mills, “*Report: Countries Prepping for Cyberwar*”, *CNET*, 16 November 2009, http://news.cnet.com/8301-27080_3-10399141-245.html. Para análise mais cética referente àquela agressão, ver Kim Zetter, “*Lazy Hacker and Little Worm Set Off Cyberwar Frenzy*”, *Wired*, 8 July 2009, <http://www.wired.com/threatlevel/2009/07/mydoom/>. De acordo com P. W. Singer, o *DoD* arrenda 95 por cento de suas conexões de comunicação de provedores comerciais, adicionando outra faceta complexa a toda forma de reação. Ver seu livro *Wired for War: The Robotics Revolution and Conflict in the 21st Century* (New York: Penguin Books, 2009), 200.

6. Durante os longos ataques *DDoS* (semanas) contra a Estônia em 2007, os sistemas governamentais e bancários ficaram fora de ação durante horas. A maioria das redes do país ficaram isoladas do resto do mundo durante dias. Ver Clark Boyd, “*Cyber-War a Growing Threat Warn Experts*”, *BBC*, 17 June 2010, <http://www.bbc.co.uk/news/10339543>.

7. Para consideração de questões afins, ver Richard A. Clarke e Robert K. Knake, *Cyberwar: The Next Threat to National Security and What to Do about It* (New York: HarperCollins, 2010), 179–218.

8. “Phishing” refere-se à mensagens eletrônicas enviadas com intento malicioso e modificadas para aparentar proveniência de pessoa, firma ou local confiável. No entanto, de acordo com o *DoD*, *phishing* inclui mensagens fraudulentas que instalam vírus. Muitos limitam a prática deste tipo de mensagens a roubo de identidade. Para maiores informações, ver *Wikipedia: The Free Encyclopedia*, s.v. “phishing,” <http://en.wikipedia.org/wiki/Phishing>.

9. Para entrevista referente à capacidade de *hackers* menos experientes com ferramentas populares, ver “*Metasploit Express*”, *noobz Network*, 5 June 2010, <http://www.noobz.net/metasploit-express/>. Notar que delinquentes experientes possuem capacidade bem mais sofisticada. Os grupos profissionais, patrocinados por diferentes nações tendem a superar quaisquer outros. Em conferência recente, o TenGen William T. Lord, o Oficial-Chefe de Informação da Força Aérea, observou que “‘possuímos mais de 19.000 aplicações (informática) na Força Aérea’ . . . notando que o *Electronic Systems Center’s IT Center of Excellence* na Base Aérea Maxwell-Gunter Annex no Alabama, examinaram cerca de 200 dentre esses. ‘Todos contavam com mais de 50 vulnerabilidades.’” Chuck Paine, “*General Calls for Network Utility, Security Balance*,”

AF.mil, 17 August 2010, <http://www.af.mil/news/story.asp?id=123218114>.

10. Para outro exemplo de eficácia em *phishing* mal articulado, ver John Timmer, “*Users Are Still Idiots, Cough Up Personal Data Despite Warnings*,” *Ars Technica*, <http://arstechnica.com/science/news/2010/08/users-are-still-idiots-cough-up-personal-data-despite-warnings.ars>. Este artigo usa a palavra *vírus* em sentido geral, a fim de descrever todo tipo de programa malicioso. De fato, o ataque descrito usaria uma combinação de vírus e minhocas [*worms*].

11. Para maiores detalhes ver “*67th Network Warfare Wing*,” 24th Air Force, <http://www.24af.af.mil/units>.

12. Em agosto de 2010, a *Microsoft* liberou consertos para 14 falhas em segurança em seu sistema *Windows*. Esta cifra não inclui questões de segurança com outros programas, tais como *Adobe Acrobat* e *Java*. Ver “*Microsoft Security Bulletin Summary para August 2010*,” *Microsoft TechNet*, 1 September 2010, <http://www.microsoft.com/technet/security/bulletin/ms10-aug.mspx>; and Emil Protalinski, “*Patch Tuesday: Microsoft’s Most Security Bulletins Ever!*,” *Ars Technica*, <http://arstechnica.com/microsoft/news/2010/08/microsoft-patch-tuesday-for-august-2010-14-bulletins.ars>.

13. Dado o número limitado de técnicos experientes em defesa de rede, as equipes da 67 NWW dentro de sua esfera de responsabilidade podem ser obrigadas a consertar o equipamento de uma a duas Bases de cada vez, até mesmo após controlar suficientemente os ataques e quando as Bases não estiverem mais isoladas. Se levar vários dias para solucionar os problemas em cada Base, as que estiverem no final da lista passarão por semanas de degradação.

14. Até mesmo os países tão “desconectados” da *Internet*, como a Coreia do Norte, estabeleceram programas de guerra cibernética. Ver Dan Raywood, “*North Korean Cyber Warfare Unit Strengthened with Recruitment of 100 Hackers*,” *SC Magazine*, 6 May 2009, <http://www.scmagazine.uk.com/north-korean-cyber-warfare-unit-strengthened-with-recruitment-of-100-hackers/article/136235/>; e Clarke e Knake, *Cyberwar*, 27. O Secretário de Defesa Adjunto declarou que “mais de 100 agências de inteligência estrangeira” têm as redes do *DoD* em mira. As ferramentas e habilidade utilizadas em espionagem cibernética são bem idênticas àquelas necessárias a ataques cibernéticos. Ver William J. Lynn III, “*Defending a New Domain: The Pentagon’s Cyberstrategy*,” *Foreign Affairs* 89, no. 5 (September/October 2010): 97–108; e Bruce Schneier, “*Cyberwar*,” *Schneier on Security* (blog), 4 June 2007, <http://www.schneier.com/blog/archives/2007/06/cyberwar.html>.

15. Para debate referente à vulnerabilidades, similares às ferramentas de tomada de consciência da situação, ver Clarke e Knake, *Cyberwar*, 170–73.