



# O Preparo da Próxima Geração de Guerreiros Cibernéticos Profissionais

TEN CEL TIMOTHY FRANZ, USAF

EM 1924, os líderes do Exército norte-americano enfrentaram o dilema de alocação de fundos com um orçamento bastante restrito, devido as condições fiscais. Conceder prioridade à devida área seria desastroso à outras. Um programa em particular atraiu grande interesse – o Plano Lassiter, projetado para expandir o Serviço Aéreo a um custo estimado em 90 milhões de dólares anuais, o que consumiria mais de um terço do orçamento alocado ao Exército.<sup>1</sup> Atualmente, a Força Aérea e, na verdade, todo o Departamento de Defesa (*DoD*) enfrentam o mesmo tipo de dificuldade. Devido ao clima econômico desfavorável, ao mesmo tempo em que tenta reconstituir a antiga capacidade, o *DoD* encara cortes radicais de recursos financeiros e mão-de-obra. Muitos programas passam por séria redução e, em alguns casos, confrontam a possibilidade de eliminação. A situação é a mesma enfrentada durante a década de 20: Conferir prioridade a dada área resultará em graves consequências à outras. No entanto, assim como o poder aéreo revolucionou as Forças Armadas no início do século XX, a guerra cibernética causará a mudança radical neste milênio.

## Surge o Operador de Guerra Cibernética

O *DoD* atingiu grande progresso durante os últimos cinco anos em desenvolvimento de especialidades para a guerra cibernética. Criamos os especialistas *17D* para oficiais e *oIB4* para os graduados. As outras Forças seguiram o exemplo, estabelecendo carreira similares.<sup>2</sup> Todas iniciaram de forma sólida, identificando a série de habilidades críticas ao campo e os rumos sofisticados e formais da carreira.



No entanto, tais especialidades servem apenas de primeira etapa ao que, inevitavelmente, virá a ser um campo muito mais diversificado de profissionais.

Este artigo explora quatro pontos fundamentais que devemos reconhecer, à medida que o *DoD* expande o próximo estágio de profissionais dedicados à guerra cibernética. Primeiramente, uma vez que se trata de *jogo de equipe*, exige empenho em formação de ampla gama de profissionais. A seguir, a diversidade ciberespacial gera a necessidade de sistema para identificar e categorizar, de forma mais eficaz, a tecnologia e suas diferentes funções dentro do domínio. Terceiro, devemos expandir a etnologia dos guerreiros cibernéticos profissionais para que possa também abranger a guerra. Finalmente, a capacidade da guerra cibernética varia em termos de sofisticação. Requer meios eficazes para ilustrar tais níveis de perspicácia. Embora o conteúdo e certos exemplos neste artigo baseiem-se na experiência da Força Aérea, seus conceitos transcendem a mesma e são adequados a qualquer organização em processo de estabelecer a capacidade para a guerra cibernética.

## Primeiro Ponto: O Combate Cibernético é *Jogo de Equipe*

Muitas vezes as pessoas não familiarizadas com a Força Aérea perguntam aos nossos Militares: “você voa o que?”. No entanto, assim como o sucesso das operações aéreas necessita de uma série de recursos e pessoal qualificado, além de pilotos, o sucesso das operações de guerra cibernética depende de muitos outros, além de “operadores”. Na verdade, é necessária toda uma equipe de profissionais cibernéticos, cada qual com sua série de responsabilidades e habilidades para estabelecer, controlar e projetar o poder de combate em todo o ciberespaço. Assim, podemos agrupar esses profissionais dentro de quatro funções distintas. Os operadores de guerra cibernética planejam, dirigem e executam atividades ofensivas e defensivas ciberespaciais. Os técnicos proveem e mantêm as áreas a que foram designados.<sup>3</sup> Os analistas e selecionadores de alvo oferecem o

apoio de inteligência às operações de combate. Finalmente, os produtores projetam e fabricam ferramentas e armas especializadas para este tipo de guerra.

A série de responsabilidades e habilidades difere para cada função, dependendo do tipo de apoio às operações: defensivas ou ofensivas. Quando na ofensiva, os operadores empregam sistemas de armas e ferramentas de guerra cibernética terrestres, aéreos ou lançados de plataformas espaciais. Para manter a eficácia, esses operadores devem estar em dia com a qualificação de prontidão-de-combate (*Combat Mission Ready*) para esses sistemas de armas e dispositivos, bem como de posse de perícia em tecnologia e funções das redes e sistemas adversários. Os técnicos encarregados da defesa mantêm o sistema de armas de guerra cibernética e a infraestrutura de apoio. A responsabilidade varia de instalação e configuração à solução de problemas e concerto de peças de equipamento e programação da plataforma da qual estejam encarregados. Os analistas e selecionadores de alvos combinam os dados de todas as fontes para analisar as redes do adversário e preparar soluções ofensivas de alvos para armas e ferramentas cibernéticas. Assim como os operadores, também devem ser especialistas no emprego prático da rede e dos sistemas pertinentes. Finalmente, os produtores mantêm a habilidade em engenharia e desenvolvimento de programas de computação, a fim de desenvolver novos sistemas de armas, armas e ferramentas, ou modificar os existentes. Da mesma forma, a natureza do trabalho dos produtores exige a manutenção de perícia em tecnologia de alvos em potencial que suas armas e ferramentas são projetadas a impactar.

Para operações defensivas, a série de responsabilidades e habilidade dos guerreiros cibernéticos profissionais difere um pouco. Os operadores encarregados dessas missões defendem e controlam áreas ciberespaciais específicas, o que pode variar de simples rede de área local [*Local Area Network – LAN*], em uma só instalação ou plataforma a bordo de aeronave, à completa rede global. Não obstante o escopo de responsabilidade, os operadores devem ser especialistas em sua completa

esfera de ação e, até certo ponto, em toda a tecnologia que a compõe. Empregam sistemas de armas e ferramentas defensivas e as responsabilidades individuais variam, dependendo do cargo. Os operadores táticos podem controlar os sensores da rede de perímetro para defesa contra tentativas não autorizadas de acesso à mesma, enquanto os encarregados de operações dirigem mudanças dinâmicas de configuração em grande escala, em reação a ataques inimigos. Os técnicos, trabalhando lado a lado com os operadores que defendem a rede, proveem e mantêm as áreas ciberespaciais de que são encarregados. Assim como os operadores, suas funções e responsabilidades variam. Alguns especializam-se em computadores pessoais, enquanto outros em componentes de infraestrutura, como roteadores e comutadores [*routers and switches*]. Qualquer que seja a tarefa, os técnicos devem possuir habilidade em tecnologia e funções em sua área de especialização, operando de acordo com as prioridades da missão e estratégias defensivas estabelecidas para a rede em questão. Os analistas em inteligência apresentam estudos referentes à ameaças antecipadas em apoio às operações defensivas da rede. Combinam todas as fontes de análise de ações técnicas, sociais, econômicas e até mesmo políticas, a fim de recomendar medidas defensivas proativas e, quando necessário, reativas, aos operadores de guerra cibernética. Esses analistas devem demonstrar perícia em capacidade e táticas inimigas, bem como manter o conhecimento da função e tecnologia das redes que protegem. Finalmente, os coordenadores encarregados de operações defensivas possuem competência básica semelhante à dos pares encarregados das ofensivas. No entanto, concentram-se em projetos de sistemas de armas e ferramentas de guerra cibernética que protegem e defendem as redes.

Apesar de todas as Forças militares norteamericanas haverem tomado certas medidas para o estabelecimento de grupos de guerreiros cibernéticos, o empenho para profissionalizar as funções de técnico, analista e coordenador, até agora, foi tentativo. Como antigamente, quando os líderes tentaram, de forma deliberada, transformar mecânicos de

caminhão em pessoal de manutenção de avião e os agentes do serviço secreto em especialistas em seleção de alvos aéreos, devemos também entrar em ação para treinar profissionais em guerra cibernética se quisermos estabelecer uma força de combate superior.

## Segundo Ponto: A Diversidade Ciberespacial

O ciberespaço engloba vários tipos de tecnologia configurados em redes que desempenham ampla variedade de funções. Embora não exista definição universalmente aceita para ciberespaço, a maioria dos especialistas concorda que sua abrangência é extensa e inclui uma infinidade de sistemas em rede, desde as administrativas mais comuns (*LAN* residencial ou comercial) até comunicações a longa distância, baseadas no espaço, bem como sistemas de controle complexos para meios de infraestrutura crítica. Um exame mais minucioso revela diferentes tecnologias (sistemas operacionais, padrões de procedimento em comunicações, aplicativos, etc). Além disso, observamos que a tecnologia nem mesmo pertence exclusivamente a dada rede. Pelo contrário, o mesmo tipo de tecnologia pode permear diferentes redes, com aplicações distintas para cada uma. Por exemplo, pode-se instalar uma rede baseada em *Microsoft Windows* e *Internet Protocol (IP)* de maneira a funcionar como serviço bancário ou sistema de controle de fabricação. Em outras palavras, uma só tecnologia possui múltiplas aplicações práticas.

Para defender uma rede de forma eficaz, a equipe deve entender a tecnologia que a compõe e a função que desempenha (a missão que apoia). Embora a composição de um sistema de controle industrial comparada à rede do centro de operações aeroespaciais [*Air and Space Operations Center – AOC*] possa exigir perícia em tecnologia similar, o primeiro possui composição, missão e esquema de priorização completamente distintos do segundo (i.e., função). Em função ofensiva, a equipe deve compreender a tecnologia do sistema-alvo, bem como sua função. Por um lado,

compreender a tecnologia permite a seleção de arma ou tática correta para obter acesso, expandir privilégios, extrair dados, degradar os sistemas inimigos e assim por diante.<sup>4</sup> Por outro, compreender a função permite saber como, quando e onde “afetar o alvo.”

Os profissionais atuais (operações ofensivas e defensivas) mantêm especialização em apenas número bastante limitado de redes práticas e tipos de tecnologia. Infelizmente, a ameaça é onipresente. Requer a expansão de habilidades além da capacidade atual. Com relação à capacidade de defesa, as ameaças agora vão além de agressões contra redes administrativas e redes globais comuns. Os ataques atuais afetam infraestrutura crítica, tais como sistemas de controle de tráfego aéreo e Controle de Supervisão e Aquisição de Dados [*Supervisory Control and Data Acquisition System – SCADA*] para o Gerenciamento de Força Elétrica [*Electric Utility-Management*].<sup>5</sup> Em relação à ofensiva, as principais fontes de poder\* contra as quais levaríamos a cabo operações também incluem diversos tipos de redes e tecnologia. Os alvos militares comuns contêm uma variedade de funções fabricadas com uma mescla de diferentes tecnologias: aquelas desenvolvidas por particulares e as disponíveis no mercado, que estão além de nossa perícia ofensiva atual. Para ambas, é razoável supor que o nível de sofisticação da ameaça só irá aumentar com o passar do tempo. À medida que o mundo, a passos lentos, chega à conclusão de que o ciberespaço é o ponto fraco das nações (inclusive o da nossa), os Estados Unidos serão obrigados a ampliar o alcance de sua competência em combate além da potência atual.

Neste momento em que o *DoD* expande a capacidade em guerra cibernética, não podemos simplesmente dizer, indiscriminadamente, que necessitamos de maior número de operadores, técnicos ou analistas de guerra cibernética, do mesmo modo que não podemos dizer que necessitamos de maior número de pilotos, oficiais de sistema de armas ou de

manutenção de aeronaves. O antigo Corpo Aéreo do Exército [*Army Air Corps*] e, mais tarde, a Força Aérea, constataram que piloto algum conseguiria operar todos os tipos de fuselagem.<sup>6</sup> Da mesma forma, profissional de guerra cibernética algum consegue a mesma qualidade de desempenho em todo o ciberespaço. Todo piloto militar apreende os fundamentos de operações aéreas, mas cada um é especializado em sistemas de armas e missões específicas. Devemos exigir de nossos profissionais cibernéticos o mesmo tipo de exclusividade. Embora todos necessitem de fundamentos básicos em dado domínio, cada qual deve especializar-se em plataformas, missões e áreas ciberespaciais específicas. Caso contrário, a aquisição do conhecimento necessário para que dado indivíduo consiga compreender a tecnologia de forma a causar impacto ofensivo ou proteger todas as funções, levaria mais de uma vida.

Uma melhor gestão das capacidades de guerra cibernética exige sistema lógico para identificar e categorizar as funções e a tecnologia ciberespacial. Um dos métodos agrupa a tecnologia e redes práticas, de acordo com características ou utilidade comuns. Como “classes” tecnológicas, um exemplo fácil de entender seria combinar todas as variações do *UNIX* em uma só classe e todos os sistemas baseados em *Windows* em outra. Alguns ou todos os protocolos de vínculo de dados digitais táticos fariam parte de dada classe (por exemplo, *Link 16*, *Link 22*), enquanto o conjunto de protocolos de controle de sistemas (e.g., *MODBUS*, *RP-570* ou *Conitel*) pertenceria à outra.<sup>7</sup> Quanto ao agrupamento de redes práticas, notamos que dois exemplos de “classes” práticas poderiam incluir redes bancárias e de *AOC*. Também teria sentido organizar certas classes de acordo com similaridades geográficas ou padrões da empresa prevalente. Por exemplo, talvez todos os sistemas de controle de fornecimento de água no sudeste dos Estados Unidos sejam semelhantes o suficiente para pertencer à mesma classe,

\**Nota da Redação:* *Centers of Gravity – CoG* é um conceito formulado por Carl von Clausewitz, um teórico militar prussiano, apresentado em sua obra *Vom Kriege*. A definição de CoG é “a fonte de poder que fornece força moral ou física, liberdade de ação ou desejo de agir.” Assim a tradução de *Centers of Gravity* neste caso não é: *Pontos de Equilíbrio*, mas sim, *Fontes de Poder*.

ou talvez todas as instalações de produção química construídas por determinada empresa possam compartilhar afinidades de rede de forma razoável para, logicamente, fazer parte de uma só classe. Os exemplos acima não se destinam a solucionar a classificação, servindo apenas para ilustrar o conceito. As classes reais podem muito bem diferir em tamanho e composição. De qualquer forma, o estabelecimento formal de classes lógicas de tecnologia e redes práticas ajudaria a identificar claramente as especialidades e a série de habilidades necessárias. Além disso, a natureza modular de tal estrutura ofereceria diversas vantagens em organização, treinamento e suprimento de recursos para a guerra cibernética.<sup>8</sup> Os pontos a seguir continuam com a ilustração.

## O Emprego de Conceitos: Exemplo de Ofensivo

As “classes” práticas e tecnológicas, se organizadas de maneira inteligente, viriam a ser uma série de habilidades que o pessoal conseguiria dominar em período de tempo razoável, mantendo-se dentro de um programa estruturado de treinamento contínuo.<sup>9</sup> Com os indivíduos sempre atualizados em certo número de classes práticas e tecnológicas, seria possível o fácil agrupamento da equipe apropriada para missões específicas. No exemplo teórico que segue, uma missão ofensiva requer o preparo operacional do campo de batalha contra o sistema bancário do país X. A tecnologia conhecida para esse sistema inclui protocolo baseado em *IP* e tecnologia *Windows 2000*. Dada a informação, os comandantes selecionam a seguinte tripulação para a missão:

- Cabo João e o Soldado Especializado Pedro (técnicos): mantêm a plataforma de sistema de armas que o Capitão Ronaldo opera. Também ajudam a configurar e a carregar o complexo de armas *Babbage*.
  - Tenente Maria (combatente cibernético-analista e selecionadora de alvos): perita qualificada em Classe Prática *R* (sistemas bancários), conta com especialização em bancos no território do país X e qualificação básica em Classe Tecnológica *B* (baseada em *IP* e tecnologia *Windows/UNIX*).
  - Sr. Pereira (*fabricante* de armamentos): membro da equipe que projetou o conjunto de armas *Babbage*, é especialista em Classe Tecnológica *B* (baseada em *IP* e tecnologia *Windows/UNIX*).
- Ao expandirmos o exemplo, podemos ver como uma estrutura de classe modular teria outra vantagem: a de pares flexíveis para a tripulação. Suponhamos que em missão subsequente a demanda seria a interrupção da produção de produtos químicos do país Y. Os dados secretos indicam que esse sistema utiliza tecnologia semelhante à do sistema bancário do país X. Neste caso, a indústria de produção química inclui servidores baseados em *UNIX* que utilizam protocolos baseados em *IP*. As similaridades aos alvos tecnológicos da missão anterior permitem que o operador, técnicos e o *fabricante* de armamentos permaneçam os mesmos, trocando o analista e o planejador de alvos de guerra cibernética pela perícia mais relevante em redes práticas:
- Capitão Ronaldo (operador): perito qualificado em Classe Tecnológica *B* (baseada em *IP* e tecnologia *Windows/UNIX*), possui qualificação básica em Classe Prática *S* (indústria de produtos químicos) e é qualificado em complexo de armas *Babbage*.
  - Cabo João e o Soldado Especializado Pedro (técnicos): mantêm a plataforma de sistema de armas que o Capitão Ronaldo opera. Também assistem a configurar e a carregar o complexo de armas *Babbage*.

- Sargento Paulo (analista de guerra cibernética e selecionador de alvos): perito qualificado em Classe Prática *S-4* (instalações químicas de produção construídas pela *Sunnybell Inc.*), possui qualificação básica em Classe Tecnológica *B* (baseada em *IP* e tecnologia *Windows/UNIX*).<sup>10</sup>
- Sr. Pereira (*fabricante* de armamentos): membro da equipe que projetou o complexo de armas *Babbage*, é especialista em Classe Tecnológica *B* (baseada em *IP* e tecnologia *Windows/UNIX*).

Conforme ilustrado, o conceito acima permite identificar e selecionar facilmente a tripulação apropriada para combater redes específicas. No entanto, com o aumento em sofisticação, provavelmente o objetivo das missões será, não só uma única rede prática, mas também uma combinação de diferentes redes interconectadas. Um exemplo mais amplo ilustra como equipes distintas, identificadas através de diferentes classes práticas integram-se para produzir maiores efeitos através de rede que contém uma multiplicidade de classes práticas. Por exemplo, suponhamos que uma missão exija a interrupção das redes de energia elétrica do país *Y*. A inteligência compilada indica que certo sistema *SCADA* conectado à interface da rede comercial local gerencia a rede elétrica em questão. Além disso, a inteligência também indica que em certo ponto do país uma conexão de frequência de rádio serviria de ponto de acesso àquela rede comercial local (*LAN*).

A perícia necessária para explorar e obter acesso à conexão, circunavegar as defesas da rede comercial local e finalmente afetar o sistema de controle seria esperar demais de um só operador ou tripulação. No entanto, o nosso *conceito de classes* facilita a organização das equipes de forma adequada, a fim de cumprir com a missão. Primeiramente, a equipe qualificada a explorar comunicações de frequência de rádio (talvez de aeronave tripulada ou remotamente pilotada) alcança a faixa de transmissão do país *Y*, a fim de obter o acesso inicial. Em seguida, outra equipe qualificada em tecnologia e funções de interface da rede comercial aproveita o acesso à frequência de

rádio para obter acesso à rede comercial *LAN*, superar as defesas e insinuar-se pelo sistema de controle. Isso permite que a terceira equipe acesse remotamente o sistema de controle e interrompa o fornecimento de energia. A fim de completar o quadro operacional, pode-se imaginar os recursos aéreos (e.g., veículos remotamente pilotados ou imagens via satélite) fornecendo avaliação de danos da batalha em apoio ao ingresso e egresso da *carga* de ataque aéreo ou de equipe terrestre de operações especiais. Embora esse exemplo possa parecer complicado demais para funcionar, consideremos a complexidade de uma só missão de ataque aéreo. Exatamente como ocorre com as operações aéreas combinadas, as missões de guerra cibernética dessa magnitude eventualmente passarão a ser corriqueiras.<sup>11</sup>

## O Emprego de Conceitos Exemplo de Defensivo

Quando falamos em defesa de rede na Força Aérea atual, na verdade queremos dizer somente a capacidade e forças que defendem as redes *Nonsecure Internet Protocol Router – NIPRNET* e *Secret Internet Protocol Router – SIPRNET*.<sup>12</sup> No entanto, ao cruzarmos o perímetro das diferentes bases aéreas, encontramos muitas outras redes essenciais ao sucesso da missão. Por exemplo, as redes administrativas de apoio à infraestrutura das instalações, tais como sistemas de controle de abastecimento (água, energia elétrica e gás), bem como sistemas de aquecimento, ventilação e ar-condicionado. As organizações como as forças de segurança e o corpo de bombeiros contam com redes que controlam os sensores de segurança pessoal: alarme e extinção de incêndio; dispositivos de monitoramento químico, biológico, radiológico, nuclear e de explosivos. Outras redes apoiam as operações de campo de pouso, sistemas de radar e conexões de comando e controle (*C2*) aerotransportados.<sup>13</sup> À medida que expandimos as defesas de rede além do *NIPRNET* e *SIPRNET*, o conceito de classes práticas e tecnológicas comprova sua utilidade, identificando com maior facilidade os sistemas que temos a res-

ponsabilidade de defender, bem como organizar a série de habilidades nas quais os ciber-guerreiros profissionais devem receber treinamento.

Como os companheiros da ofensiva, os destacamentos designados à operação e defesa de dada rede devem manter a perícia em certos tipos de tecnologia e classes práticas. No entanto, em lugar de manter o enfoque em tecnologia e funções das redes-alvo, esses destacamentos devem entender as funções e a tecnologia das redes pelas quais são responsáveis em defender. Ao empregar o conceito de classes a dado exemplo, vemos que um dos destacamentos seria designado a operar e a defender redes da classe prática *G*, os sistemas *Patriot Battery*, e outra a defender redes da classe prática *J*, os sistemas de energia elétrica *SCADA*. Assim, esses destacamentos incluiriam pessoal qualificado na classe prática designada, bem como nas classes tecnológicas relevantes.<sup>14</sup>

## Outras Vantagens da Categorização do Ciberespaço

Além da vantagem de treinamento e organização das forças de guerra cibernética, a categorização do ciberespaço em classes práticas e tecnológicas oferece outros benefícios, como a fácil identificação de requisitos de combate. Vamos supor que um comandante combatente [*Combatant Commander – CCDR*] necessite degradar o sistema integrado de defesa aérea [*Integrated Air Defense System – IADS*] *X* do país *Y* ou defender o sistema de controle aéreo *Z* norte-americano. Os requisitos, tais como “degradar o *IADS X* do país *Y*” ou “defender o sistema de controle aéreo *Z*” seriam suficientemente claros para determinar as forças convencionais necessárias. No entanto, é difícil traduzir essa terminologia a vocabulário útil para obter e alocar a capacidade de guerra cibernética. A guerra cibernética é um bicho-de-sete-cabeças. Ao colocarmos os imperativos de combate dentro de classes práticas e tecnológicas facilitamos a clara articulação dos requisitos, quando redigimos o me-

morando [que justifica] o objetivo do programa [*Program Objective Memorandum – POM*] às autoridades competentes. Além disso, facilita o trabalho dos planejadores do *CCDR*, quando requisitam o pessoal adequado para a guerra cibernética dentre as Forças Armadas.

A fim de ilustrar o conceito do processo *POM*, podemos imaginar a tradução da tecnologia contida no “*IADS X*” do país *Y* em determinadas classes práticas e tecnológicas. Os insumos ao processo então diriam eficazmente: “Solicitamos novo (ou maior número de) pessoal, sistemas de armas, cursos de treinamento e educação, bem como campos de teste e treinamento para causar impacto em tecnologia específica e redes práticas que compõem o *IADS X* do país *Y*”. Se eliminarmos essas faltas de conexões, conseguiremos apoiar os requisitos do *CCDR*, causando impacto no *IADS X*. Ao articularmos, claramente, os requisitos de guerra cibernética no *POM*, a chance de passar o escrutínio dos comitês de financiamento, melhora. Além disso, ao vincular esses requisitos às necessidades do *CCDR*, identificamos áreas de risco se determinados programas não forem financiados (i.e., se deixarmos de financiar o desenvolvimento de capacidade de guerra cibernética para afetar o *IADS X*, os *CCDR* devem assumir o risco nessa área ou satisfazer a demanda com o uso de outras capacidades). Obviamente, esse exemplo é demasiado simples. Os exemplos da vida real provavelmente serão muito mais complexos, uma vez que qualquer uma das classes tecnológicas poderia permear várias classes práticas que, por sua vez, satisfazem grande número de requisitos do *CCDR*.

A habilidade de identificar com maior facilidade os requisitos de guerra cibernética também seria útil aos planejadores do *CCDR*, quando designam capacidades em documentos de solicitação de “forças para devido fim”, ao requisitar recursos para operações de contingência em mensagem solicitando avaliação, ou quando desenvolvem força de duração gradativa e dados de destacamento.<sup>15</sup> Atualmente, esses documentos identificam, de forma genérica, os profissionais de guerra cibernética. No entanto, em certo momento, não será sufi-

ciente designar tarefas a “ciberoperador”. Por exemplo, o indivíduo especializado em sistemas telefônicos não servirá para um *CCDR* que esteja à busca de perito em *SCADA*.

Não existe, agora, um sistema lógico formal para classificar grupos tecnológicos e funções ciberespaciais.<sup>16</sup> No entanto, será necessário, se desejarmos organizar, treinar e suprir, de forma eficaz, a guerra cibernética futura.

### Terceiro Ponto: A Necessidade de Estilo de Combate

A Força Aérea outorgou novo título e distintivo aos guerreiros cibernéticos, mas seu estilo profissional deve mudar se quisermos transformá-los em combatentes daquela guerra que visualizamos para o futuro. Infelizmente, vários obstáculos retardam a habilidade de criar um verdadeiro estilo de combate dentro desse clique. Em primeiro lugar, a maioria desses profissionais é proveniente dos campos de informática e comunicações. Como tal, seu enfoque principal é em manter comunicações ininterruptas, não em entender completamente as missões apoiadas por toda conexão ou nó. Por conseguinte, esses especialistas só conseguirão compreender, de verdade, o impacto à missão causado pela perda de um elo ou nó, quando a perda ocorre e os usuários começam a reclamar. Outro obstáculo em estilo é em como definimos o combate cibernético. Por exemplo, no momento limitamos a “defesa” cibernética exclusivamente à detecção de intrusos nos pontos de demarcação da rede, descobrindo programas maliciosos internos e “bloqueando” o que encontramos nos portais de entrada aos sistemas, pontos de prestação de serviços, ou dispositivos de segurança da rede [*firewalls*].<sup>17</sup> Os defensores cibernéticos necessitam de maior familiaridade com a gama completa de ameaças hostis aos sistemas de informática e maior habilidade de combate contra agressões provenientes de tais ameaças. O atual estilo profissional dos guerreiros cibernéticos deve evoluir, de prestador de serviço a aquele que oferece o equilíbrio

entre serviço, segurança e conhecimento de ameaças, tudo em nome de garantia da missão.

Para fomentarmos o “estilo de combate” entre esses profissionais devemos mudar a mentalidade. Em modo ofensivo, ela é mais natural, devido ao tipo da missão. No entanto, em defensiva, tal perspectiva exige esforço extra. As redes apoiam missões específicas. Não se pode defender uma rede de forma adequada, sem conhecer a missão que apoia, bem como a ameaça que a coloca em situação de risco. Infelizmente, o estilo de ser da área de comunicação, normalmente coloca maior ênfase na condição salutar e disponibilidade de rede e não na missão, que é a sua *razão de ser*. Necessitamos, mesmo, é de defensores cibernéticos que sejam especialistas em tecnologia dedicada à redes. Também devem ser peritos nas missões que apoiam, na maneira como colocam as mesmas em foco de prioridade e como a degradação ou perda de certas áreas da rede afeta a missão (antes que isso aconteça). Além disso, os defensores devem conhecer o inimigo: entender o escopo da ameaça; capacidades e limitações; táticas comuns, técnicas e procedimentos [*Tactics, Techniques, and Procedures – TTP*]; as tendências históricas e atuais; e o fato de que as motivações principais são fundamentais ao preparo, priorização e determinação do curso a tomar em reação à ameaça. Somente após compreender por completo, a missão e o adversário podemos até mesmo começar a defender eficazmente e, em última instância, assegurar as missões que ocorrem dentro e através do ciberespaço.

As ações defensivas de combate em guerra cibernética consistem em preparativos para o ataque, a reação ao mesmo e finalmente, a recuperação. Os preparativos requerem estabelecer e proteger a rede. Os fundamentos, tais como os planos minuciosos de defesa, mecanismos de garantia de dados e firme *C2*, fornecem tal base. A distribuição de sensores, externos e internos que detectam, erradicam e bloqueiam ameaças, completam os preparativos. A reação a ataque quer dizer a luta durante todo o período de tempo da agressão. Isso quer dizer colocar em execução conceitos como controles de configuração dinâmica

(e.g., endereços *IP* durante períodos de guerra, salto de frequência, substituição de equipamento físico e virtual com o sistema em operação), técnicas de dissimulação ativa (i.e., sedução [*honeynets*]) e uso de nomes de provedores deliberadamente falsos.<sup>18</sup> Além disso, esses técnicos devem possuir a capacidade de rápido reenvio de comunicações amigas [comunicações em azul] à rotas secundárias e terciárias no momento de perda de certos elos ou nós, bem como o envio de ataques em vermelho (inimigos) a bicos sem saída. Quando compreendem como a rede apoia as operações de dada missão, os defensores saberão onde e quando podemos tolerar interrupções. Às vezes, sofrer perda ou degradação de parte da rede é preferível se deixa de afetar missões críticas. Se o adversário acreditar que o ataque à rede está tendo sucesso, pode ser que continue a perder tempo e recursos em alvo dispensável, permitindo-nos concentrar em outras prioridades. Uma reação de defesa eficaz também requer saber como lutar de forma integrada dentro de toda a rede *C2*, bem como combater de forma isolada. Uma coisa é defender redes com a capacidade de operação e o *C2* completamente intactos. Outra é tentar fazer o mesmo após perder a conexão com o Centro de Segurança de Operações de Rede Integradas, [*Integrated Network Operations Security Center*], com o 624º Centro de Operações [*624th Operations Center*] ou com o *AOC*. Será que ainda poderemos garantir o cumprimento da missão nessa situação? A reação também inclui revidar a ameaça. Os defensores, necessariamente, não executam tais ações diretamente (já que a capacidade ofensiva inclui uma série de habilidades completamente diferente). Essas ações, ao contrário, exigem coordenação através de cadeia de *C2* para permitir que o Centro de Operações ou o *AOC* direcione a reação apropriada, quer seja cinética ou não. Finalmente, o combate inclui atividades de recuperação, como a rápida reconstituição feita de forma priorizada. Os especialistas em guerra cibernética, adequadamente treinados, podem fazer isso de forma eficaz porque entendem a missão, a rede e as prioridades.

## Quarto Ponto: Nem Todas as Capacidades de Guerra Cibernética se Parecem

Defesa cibernética alguma irá repelir todos os ataques e capacidade ofensiva alguma será bem sucedida contra todo adversário. É importante ter em mãos um mecanismo para identificar o nível de sofisticação da capacidade de guerra cibernética se quisermos administrar as expectativas da liderança e definir padrões claros de treinamento. Durante eventos como *Red Flags* [exercícios de treinamento de combate aéreo avançado] ou exercícios da Escola de Armas da Força Aérea [*Air Force Weapon School*], os agressores aéreos empregam tal mecanismo sob a forma de matriz de “réplica de ameaça” para identificar o nível de sofisticação de treinamento das forças Azuis para dado tipo de combate. Por exemplo, será que atuarão com intensidade de ameaça de nível um, que são os modelos mais antigos de aeronaves inimigas e *TTPs* mais básicos, ou de nível quatro, que é a capacidade mais avançada e com os *TTPs* empregados pelos adversários mais sofisticados? Os agressores estão a ponto de colocar em execução matriz de ameaça semelhante para replicar a capacidade do adversário durante exercícios de treinamento. Vamos utilizar esse exemplo para oferecer um conceito capaz de identificar o nível de sofisticação de operações durante guerra cibernética.

A tabela 1 representa uma matriz teórica para identificar o nível de sofisticação de redes amigas na defensiva. A primeira dimensão de nível, intitulada “tecnologia”, reflete a sofisticação da tecnologia usada para operar e defender a rede (para simplificar, a matriz do exemplo demonstra apenas a tecnologia de sistema operacional). Uma rede operando em nível tecnológico *um* pode empregar sistemas operacionais antigos como velhas variáveis *Windows* ou sistema *Sun*. Encontraríamos algo mais atualizado ou de ponta em nível dois, como o *Windows 7* ou *Snow Leopard*. O nível três é um sistema operacional desenvolvido exclusivamente para a Força ou ambiente de computação *confiável*, que pode não estar disponível comercial-

Tabela 1. Níveis de sofisticação para redes em defensiva

Rede Defendida		GRAU DE SOFISTICAÇÃO		
		Um	Dois	Três
Redes Administrativas	Tecnologia	- Sun Operating System / Windows XP / Vista	- Windows 7 / Snow Leopard	- Base de Informática Segura de Próxima Geração / Kylin
	TTP	- LAN Simples / Unpatched	- Defesa Absoluta / Sensores Externos / Internos	- Honeynets / Negação e Dissimulação

mente para o público em geral (por exemplo, *Next-Generation Secure Computing Base* ou *Kylin*).<sup>19</sup>

A segunda dimensão do exemplo, denominada “TTP”, representa a sofisticação das TTPs defensivas empregadas. Por exemplo, o nível *um* identificaria uma rede que utiliza configurações defensivas básicas, típica de LAN de configuração simples, não reconstituído. O nível *dois* seria organizado com abordagem de defesa mais detalhada, juntamente com mecanismos de monitoramento interno ou externo. O nível *três* refletiria as defesas de rede mais sofisticadas que conhecemos, empregando técnicas avançadas como armadilhas [*honeynets*] e táticas deliberadas de negação e dissimulação. Ao combinar essas duas dimensões, dada rede operaria com equipamento de baixo nível (tecnologia de nível *um*), mas com operadores experientes que empregam TTP de nível *dois*. Outra rede portaria equipamento de ponta (tecnologia de nível *três*), mas pessoal com formação defensiva relativamente ineficaz (nível de TTP *um* ou *dois*).

Do mesmo modo, os níveis de sofisticação para a capacidade ofensiva (Tabela 2) identificam os diferentes tipos de tecnologia através

da complexidade do sistema de armas ou das ferramentas empregadas. Por exemplo, a tecnologia de nível *um* consistiria de ferramentas ou armas disponíveis pela *Internet* (ferramentas tipo “*script-kiddy*”), enquanto o nível *dois* utilizaria algo mais sofisticado, como ferramentas ou armas disponíveis comercialmente. O nível *três* refletiria capacidade ofensiva desenvolvida pela Força. Os níveis de TTP para capacidades ofensivas de guerra cibernética vão desde os menos sofisticados, com vetor de ataque de rede altamente detectável, devido a ferramentas e táticas sem sofisticação [*noisy*] e rastreáveis (nível *um*) aos que empregam técnicas avançadas (e.g., dissimulação ativa, operações anônimas altamente camufladas, etc) capazes de produzir efeitos de segunda e terceira ordens (nível *três*).<sup>20</sup>

A identificação dos níveis de sofisticação das forças de guerra cibernética possuem dupla importância. Em primeiro lugar, tais níveis servem para melhor compreender os padrões de treinamento. Em outras palavras, auxiliam os profissionais a identificar o nível de sofisticação em que operam o que, por sua vez, ajuda-os a determinar o patamar que devem atingir, a fim de satisfazer os padrões

Tabela 2. GRAU DE SOFISTICAÇÃO

Alvo Adversário		GRAU DE SOFISTICAÇÃO		
		Um	Dois	Três
Redes Administrativas	Tecnologia	-Em Wild Scripts / Ferramentas	- Mais Complexos / Comerciais a Varejo	- Orgânicos / Governamentais Disponíveis
	TTP	- Pontos Únicos de Presença / Ruidosos / Atribuíveis	- Pontos Múltiplos de Presença / Sem Atribuição	- Efeitos de Orden N / Dissimulação

para fazer frente ou derrotar os adversários conhecidos. A clara verbalização de padrões não apenas demarca os requisitos de treinamento, mas também cria rigor operacional entre as forças de combate. Em segundo lugar, a definição de níveis de sofisticação orienta as expectativas da liderança. Os recursos humanos, financiamento e prazos são três variáveis de investimento que impulsionam o nível de sofisticação de qualquer tecnologia e de *TTP* que adquirimos ou desenvolvemos. As ferramentas, como a matriz exibida, que ilustram o nível de sofisticação da capacidade de guerra cibernética farão com que os líderes possam compreender com maior clareza o que dado investimento consegue adquirir. A menos que aproveitem ao máximo os investimentos, a tecnologia resultante e os *TTPs*, seriam inferiores aos de nível mundial (i.e., nível *três*) e, portanto, menos capazes do que aqueles dos adversários. Ao compreender esse ponto os líderes conseguem melhor visualizar e aceitar o risco ou repriorizar os recursos para atingir o nível de sofisticação desejado.

## Conclusão

Dentro dos últimos 100 anos, o poder aéreo revolucionou as operações militares de tal forma que os líderes mundiais reconheceram a supremacia aérea como essencial à vitória. Nos próximos 100 anos, o mesmo acontecerá com a superioridade cibernética. À medida que o *DoD* aperfeiçoa cada vez mais a capacidade de combate cibernético devemos prestar atenção à várias proficiências para que o sucesso esteja quase ao alcance: estabelecer estratégia para cultivar todos os profissionais de guerra cibernética (e não apenas o operador); formular aquele que consegue identificar e categorizar as funções e a tecnologia ciberespacial; promover um estilo de combate entre os profissionais; e, utilizar um instrumento para ilustrar o nível de sofisticação da capacidade de guerra cibernética. Para abordar alguns deles de forma adequada, necessitaremos, sem dúvida, de grande investimento. No ambiente atual, com a escassez de recursos, quanto será que o *DoD* estará disposto a

investir no futuro da guerra cibernética? Os líderes do momento enfrentam dificuldades similares às confrontadas pelos antecessores em 1924. Naquela época a opção selecionada foi a correta. E nós? O que será que faremos?

## Notas

1. James P. Tate, *The Army and Its Air Corps: Army Policy toward Aviation, 1919–1941* (Maxwell AFB, AL: Air University Press, 1998), 28–34.

2. Henry S. Kenyon, “U.S. Army Ponders Cyber Operations,” *Signal Online*, 15 de outubro de 2009, acessado em 6 de dezembro de 2010, [http://www.afcea.org/signal/articles/templates/SIGNAL\\_Article\\_Template.asp?articleid=2082&zoneid](http://www.afcea.org/signal/articles/templates/SIGNAL_Article_Template.asp?articleid=2082&zoneid;); and “General Officer Programs,” Navy Recruiting Command, acessado em 6 de dezembro de 2010, <http://www.cnrc.navy.mil/noru/oroj3/generalofficer.htm>.

3. Outros termos são comumente usados para representar essa função (e.g., “técnico”, “técnico em manutenção”, “especialista”, “comunicador”, etc.). O autor elegeu o termo “técnico” porque parece ser adequado e menos controverso do que os outros.

4. “Escalar privilégios” é vernáculo comum na guerra cibernética para descrever a tentativa de um agressor, a fim de conseguir maiores privilégios na rede, os mesmos direitos de usuário normal e até mesmo de administrador para navegar livremente pela rede.

5. Ver Rose Tsang, *Cyberthreats, Vulnerabilities and Attacks on SCADA Networks*, documento de estudos (Berkeley, CA: University of California, Goldman School of Public Policy, 2009), 5–6, acessado em 20 de dezembro de 2010, [http://gspp.berkeley.edu/iths/Tsang\\_SCADA%20Attacks.pdf](http://gspp.berkeley.edu/iths/Tsang_SCADA%20Attacks.pdf); *Global Energy Cyberattacks: “Night Dragon,”* Comunicado Oficial de McAfee (Santa Clara, CA: McAfee, 10 February 2011), 3, <http://www.mcafee.com/us/resources/white-papers/wp-global-energy-cyberattacks-night-dragon.pdf>; and *Review of Web Applications Security and Intrusion Detection in Air Traffic Control Systems*, Federal Aviation Administration, relatório no. FI-2009-049 (Washington, DC: US Department of Transportation, 4 May 2009), 4–5, [http://www.oig.dot.gov/sites/dot/files/pdffdocs/ATC\\_Web\\_Report.pdf](http://www.oig.dot.gov/sites/dot/files/pdffdocs/ATC_Web_Report.pdf). Os sistemas SCADA são “amplamente usados por companhias de eletricidade, água, gás e outras empresas de serviços públicos para monitorar e gerenciar as instalações de distribuição.” Ver Harry Newton, *Newton’s Telecom Dictionary*, 20th ed. (San Francisco: CMP Books, 2004), 725.

6. Em 1925 o Gen William “Billy” identificou três missões primárias para a força aérea (perseguir, bombardear e atacar). Ver William Mitchell, *Winged Defense: The Development and Possibilities of Modern Air Power—Economic and Military* (New York: G.P. Putnam’s Sons, 1925), 164–71.

Hoje existe mais de uma dezena de missões, inclusive: contra ataque aéreo; ataque estratégico; transporte aéreo; reabastecimento aéreo e inteligência, vigilância e reconhecimento, só para citar algumas. Ver Air Force Doctrine Document (AFDD) 3-1, *Air Warfare*, 22 January 2000, 8–24, <http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-1.pdf>. Em 1921 o número de pilotos na ativa estava abaixo de 900 e cerca de duas dezenas de diferentes tipos de aeronaves em serviço. Ver Tate, *Army and Its Air Corps*, 19; e “Air Corps Development, 1919–1935,” National Museum of the US Air Force, acessado em 13 de fevereiro de 2011, <http://www.nationalmuseum.af.mil/factsheets/factsheet.asp?id=724>. A Força Aérea norte-americana possui atualmente mais de 50 tipos diferentes de aeronaves com mais de 13 mil pilotos. Cada tipo de aeronave possui seu próprio código de especialidade. Ver *Air Force Officer Classification Directory* (Randolph AFB, TX: Air Force Personnel Center, April 2010).

7. Os protocolos definem as regras pelas quais os dispositivos comunicam-se uns com os outros. Consistem em procedimentos e convenções relacionadas a formatação e momentos precisos de transmissão de dados entre dois dispositivos, tratando de assuntos tais como estruturação, gerenciamento de erros, transparência e controle de linha. Ver Newton, *Newton's Telecom Dictionary*, 664.

8. Embora este artigo trate de como o conceito de classes práticas e tecnológicas aplica-se às Forças Armadas, também é aplicável a todos os setores civis e comerciais. Um particionamento lógico do ciberespaço através de linhas práticas e tecnológicas facilitaria o processo de instituições não militares em organizar as próprias redes de forma mais eficaz.

9. Esta declaração relaciona-se também a outras variáveis de treinamento, inclusive quantas classes práticas e tecnológicas um só indivíduo pode razoavelmente manter. Contudo, o conceito básico continua sendo o ponto importante.

10. Para efeitos desse exemplo, a fictícia Empresa *Sunnybell* constrói instalações de produção química em todo o mundo. Sua presença global faz dela boa candidata para possuir sua própria classe prática.

11. O conceito apresentado nesse parágrafo leva à ideia de identificar grupos ofensivos de guerra cibernética baseado em capacidade de afetar tecnologia específica e/ou classes práticas. No entanto, quando se considera a grande quantidade de diferentes tecnologias e redes práticas no ciberespaço, percebe-se que talvez não seja prático colocar fisicamente toda a perícia em um só lugar (é provável que jamais teremos pessoal suficiente para dar a cada destacamento ofensivo seu próprio grupo de perícia analítica em ferrovias, energia elétrica, etc.) Devemos também cogitar no uso de rede virtual de especialização prática se o plano for colocar em execução esses conceitos com sucesso. Por exemplo, talvez um grupo de peritos em dependências para indústrias químicas es-

teja distribuído por todo o País. Contudo, é possível sua interconexão virtual. Isso facilitaria a atribuição desta competência a diferentes grupos em momentos distintos, dependendo da missão em pauta. Isto é, o Grupo *X* é designado a atacar um grupo de produção química em certo dia, enquanto o Grupo *Y* é designado a atacar um grupo de produção química (talvez a mesma, talvez outra) no dia seguinte. No entanto, talvez ambos os grupos compareçam a mesma equipe de seleção de alvos qualificada em classe prática *S* (instalações de produção química).

12. A defesa de rede é o emprego de capacidades baseadas em rede para defender os dados amigos que residem na, ou transitam pela rede contra as tentativas do adversário em destruir, corromper ou usurpar a mesma. Ver AFDD 3-13, *Information Operations*, 11 de January 2005, 20, <http://www.e-publishing.af.mil/shared/media/epubs/AFDD3-13.pdf>.

13. Às vezes, alguns desses sistemas conseguem pegar carona na espinha dorsal da conexão *NIPRNET* ou *SIPRNET*. Contudo, seus defensores muitas vezes não estão cientes de sua existência. Na realidade, muitos desses sistemas são operados como redes independentes e, portanto, estão fora da área operacional dos defensores atuais.

14. Esse exemplo usa uma só unidade para ilustrar o conceito do uso de designações práticas e tecnológicas para grupos de guerra cibernética, em uma tentativa de estimular debate mais aprofundado. Na verdade, a extensão e a complexidade de muitas redes talvez requeiram o uso de várias unidades para cobrir todos os aspectos de operação e defesa. O tópico de como estruturar a organização de rede complexa é muito debatido no seio da comunidade ciberespacial e exige considerações fora do escopo deste artigo. No entanto, o conceito geral do uso de designações entre classes práticas e tecnológicas às unidades e pessoal encarregado da operação e defesa de redes é o ponto a salientar.

15. A comunicação do Secretário de Defesa “Forces for Unified Command Memorandum” designa forças e recursos aos comandantes combatentes. Ver Joint Publication (JP) 5-0, *Joint Operation Planning*, 26 de dezembro de 2006, I-26, [http://www.dtic.mil/doctrine/new\\_pubs/jp5\\_0.pdf](http://www.dtic.mil/doctrine/new_pubs/jp5_0.pdf). O CCDR planeja usar mensagens que contêm requisitos de avaliação para solicitar insumos referentes ao curso de ação de unidades subordinadas. Ver *ibid.*, I-15.

16. Apesar de não formalizada, existe uma base na qual podemos estabelecer uma categorização lógica. O conceito foi apresentado pela primeira vez na tese do Maj Timothy P. Franz, “IO Foundations to Cyberspace Operations: Analysis, Implementation Concept, and Way-Ahead for Network Warfare Forces” (tese de Mestrado, Air Force Institute of Technology, March 2007) como “classificações de redes.” Evoluiu a conceito de “classes práticas” e “classes tecnológicas” durante os estágios iniciais do desenvolvimento de 17D/1B4 pelo grupo de trabalho Professional Cyberspace Education Working liderado pelo Quartel-

General da Força Aérea Norteamericana e em seguida pelo Air Force's Cyberspace Technical Center of Excellence no Air Force Institute of Technology. A iniciativa cessou devido a restrições de mão-de-obra, mas a infraestrutura básica ainda existe.

17. O autor reconhece que a situação é mais complicada do que essas ações, mas a sinopse derivada é sólida.

18. *Hot-swapping* físico é o processo de substituir um componente avariado enquanto o resto do sistema continua a funcionar normalmente. Ver Newton, *Newton's Telecom Dictionary*, 400. Considerando que *hot-swapping* refere-se à permuta física de um componente, *hot-swapping virtual* refere-se aqui ao conceito de trocar uma máquina virtual ou alterar dinamicamente o endereçamento lógico em reação ou em preparo para ataque. O autor reconhece que os atuais avanços tecnológicos não apoiam, por completo, o conceito de um *hot-swapping* virtual. A *honeynet* é uma rede criada com vulnerabilidades intencionais que convidam ao ataque para que os defensores possam estudar as atividades e métodos de um agressor e usar essa informação para fortalecer a segurança de rede. Ver "Honeynet," *NetworkDictionary*, acessado em 20 de dezembro de 2010, <http://www.networkdictionary.com/security/h.php>. No contexto do parágrafo, o termo também indica o uso de *honeynets* para deter ou enganar possíveis invasores.

19. Computação confiável [*trusted computing*] é a estrutura de computador travado que garante o aplicativo de programação em operação e que permite que os aplicativos comuniquem-se de forma segura com outros aplicativos e provedores. Ver Mark Dermot Ryan, "Trusted Com-

puting and NGSCB," University of Birmingham School of Computer Science, 2004, acessado em 30 de dezembro 2010, <http://www.cs.bham.ac.uk/~mdr/teaching/TrustedComputing.html>. A Next-Generation Secure Computing Base (NGSCB) é nova tecnologia de segurança para a plataforma Windows da Microsoft, que utiliza equipamento e programação exclusivos para disponibilizar novos tipos de recursos de segurança em computação, a fim de oferecer melhor proteção de dados, privacidade e integridade ao sistema. Ver "Microsoft Next-Generation Secure Computing Base—Technical FAQ," Microsoft TechNet, acessado em 30 de dezembro de 2010, <http://technet.microsoft.com/en-us/library/cc723472.aspx#EEAA>. Kylin é um sistema operacional desenvolvido por acadêmicos da Universidade Nacional de Tecnologia de Defesa [National University of Defense Technology] da República Popular da China e aprovado para uso pelo Exército de Libertação Popular. Embora a infraestrutura fundamental desse sistema seja, na verdade, uma variável do UNIX do FreeBSD, para fins deste artigo oferece um exemplo aproximado de sistema operacional protegido por direitos autorais ou desenvolvido por particulares e não disponível ao público. Ver Rohit, "What Is Kylin Operating System?," *Spectrum*, acessado em 13 de fevereiro de 2011, <http://krititech.in/wordpress/?p=138>; e Gerard, "Kylin, a Chinese FreeBSD Based, Secure O/S," *FreeBSD News*, 4 January 2011, acessado em 13 de fevereiro de 2011, <http://www.freebsdnews.net/2011/01/04/kylin-chinese-freebsd-based-secure-os/>.

20. "Noisy" refere-se a vetor de ataque de rede altamente detectável, devido a falta de sofisticação em ferramentas e táticas empregadas pelo agressor.



**TenCel Timothy Franz, USAF** Possui Bacharelado em Ciências da Universidade Central da Flórida, Mestrado em Ciências do Instituto de Tecnologia da Força Aérea [*Air Force Institute of Technology – AFTT*]. Ex-Comandante do *57th Information Aggressor Squadron*, responsável pelo treinamento de pessoal da Força Aérea conjunta e aliados, replicando as ameaças às operações de informática atuais e emergentes. Ex-Chefe do desenvolvimento da Força no *Air Force Cyber Command* (Provisório), onde desenvolveu as estratégias de guerra cibernética e liderou o desenvolvimento da mesma como áreas especializadas da Força Aérea, incluindo o recrutamento relacionado, bem como o ingresso, treinamento e educação e programas de desenvolvimento profissional. Durante sua carreira, foi Comandante de Tripulação de Combate de Mísseis, avaliador, instrutor e Comandante de Voo, bem como analista espacial de operações de informática, especialista em tática, planejador e Chefe de Operações Técnicas Espaciais. Formou-se com distinção da Escola de Oficiais de Esquadrão e do *AFTT*, onde completou sua educação de desenvolvimento intermediário como residente.