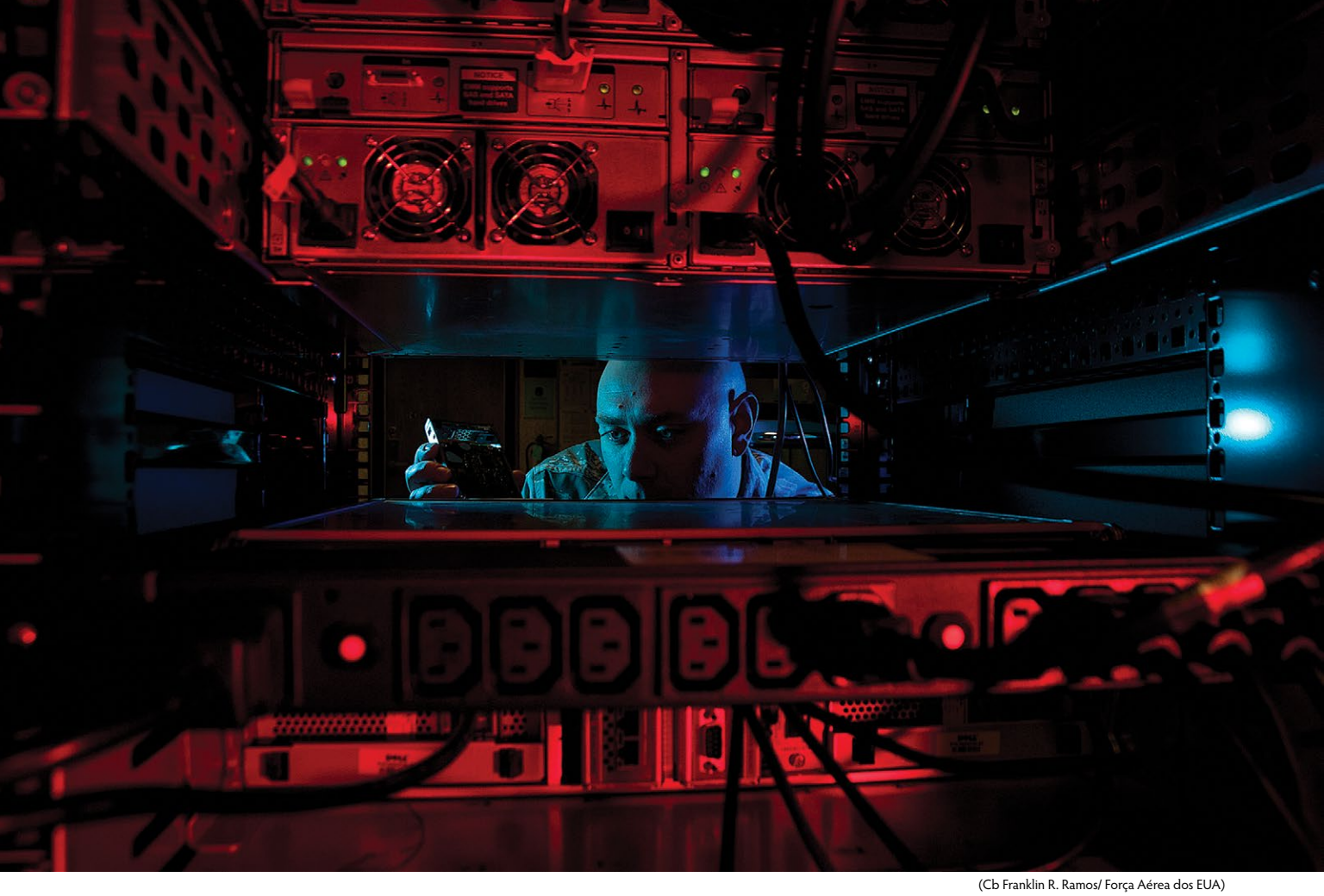


(Cb Franklin R. Ramos/ Força Aérea dos EUA)

O Sgt Jerome Duhan da Força Aérea dos EUA, um administrador de rede de computação do 97º Esquadrão de Comunicações, insere um disco rígido no servidor de retina do centro de controle de rede na Base da Força Aérea Altus, na Oklahoma, em preparação para uma inspeção de comando na área de prontidão cibernética, 24 Jan 14.

A Força Cibernética dos EUA

Prevendo a Próxima Guerra

Maj Matt Graham, Exército dos EUA

No livro *A Riqueza das Nações*, publicado em 1776, Adam Smith explica como a divisão do trabalho permite a maior eficiência: fazendeiros se concentram na produção de comida, ferreiros na manufatura de artigos de metal, e assim por diante[1]. O princípio ainda é válido hoje; indivíduos e organizações desenvolvem suas habilidades ao se concentrarem em uma única atividade. Nas Forças Armadas dos EUA, a divisão do trabalho entre as Forças Singulares consegue essa perícia: a Força Aérea se concentra na superioridade aérea, permitindo que o Exército se dedique à guerra terrestre e a Marinha

se preocupe com o combate marítimo. O Corpo de Fuzileiros Navais (CFN) desenvolve a sua perícia ao preencher a lacuna entre a terra e o mar.

Embora possua algumas características muito diferentes dos domínios físicos, o ciberespaço tem emergido recentemente como um domínio independente que exige a sua própria perícia militar. Com as nações buscando obter vantagens nesse novo domínio, a competição dentro do ciberespaço já assumiu muitas das características de guerra e, atualmente, exige o mesmo nível de perícia que é necessário para vencer guerras no mundo físico. As Forças Armadas precisam de uma Força Cibernética dos EUA independente, equivalente ao Exército, à Marinha, à Força Aérea e ao Corpo de Fuzileiros Navais, para se concentrar no domínio do ciberespaço.

A Abordagem Atual ao Ciberespaço

As Forças Armadas não têm estado inativas durante o advento e o desenvolvimento do ciberespaço e da guerra cibernética. O Departamento de Defesa estabeleceu o Comando Cibernético dos EUA (CYBERCOM), em 2009, como um quartel-general conjunto para coordenar os esforços do departamento no ciberespaço. Integrantes de todas as Forças Singulares se unem dentro do CYBERCOM para abordar as ameaças ao ciberespaço. Uma parte do orçamento do Departamento de Defesa é diretamente alocada ao CYBERCOM, e alguns dos seus recursos são provenientes das Forças Singulares. Sob o CYBERCOM, cada Força Singular estabeleceu um comando do componente (e.g., o Comando Cibernético do Exército ou o Comando Cibernético da Esquadra) para apoiar os esforços do Departamento de Defesa no ciberespaço. A importância emergente do ciberespaço, com certeza, justifica cada uma dessas ações. Contudo, o fato de cada Força Singular dedicar uma fração da sua atenção ao ciberespaço garante apenas dois resultados: elas estão se desviando dos seus papéis tradicionais de combate nos domínios físicos e os esforços no ciberespaço são ineficientes (na melhor das hipóteses), incoerentes (provável) ou fratricidas (no pior dos casos). Atualmente, essa ineficiência não é uma grande preocupação e resulta, principalmente, em frustração burocrática. No entanto, quando os riscos aumentarem e os guerreiros cibernéticos dos EUA precisarem provar que são melhores que seus adversários, essas ineficiências não serão toleradas.

A abordagem atual (com cada Força Singular contribuindo para o esforço conjunto do controle do ciberespaço) não é apenas ineficiente, mas também desnecessária. Uma operação no ciberespaço é predominantemente autônoma da plataforma ou do domínio físico pelo qual o guerreiro cibernético acessa o ciberespaço. O raciocínio empregado ou a vulnerabilidade da rede explorada pelo guerreiro cibernético são os mesmos se forem executados na ponte de comando de um navio-aeródromo, dentro da barriga de uma aeronave de comando e controle ou em uma escrivaninha com ar condicionado de um complexo comercial.

Decisiva em uma operação no ciberespaço é a exploração das vulnerabilidades do sistema do adversário antes que ele possa identificar e mitigá-las (e vice-versa). Quando considerado nesse contexto, os guerreiros cibernéticos da Marinha e da Força Aérea compartilham mais semelhanças com os seus homólogos do ramo do que com outros marinheiros e soldados da sua Força Singular.

A Força Cibernética dos EUA Proveria Foco

Em contraste com a abordagem atualmente usada pelo Departamento de Defesa, uma força cibernética independente pode proporcionar o nível necessário de concentração nas operações no ciberespaço. Maior atenção é necessária para construir competência no ciberespaço por todas as Forças Armadas, e avanços particulares podem ser antecipados em três áreas: o desenvolvimento de liderança, a formação de guerreiros cibernéticos e a atuação dentro do ciberespaço.

Liderança A Força Cibernética dos EUA garantiria que os comandantes mais antigos do ramo possuíssem uma experiência profunda nas operações no ciberespaço. Atualmente, os oficiais mais antigos dentro de cada uma das Forças Singulares são promovidos pelo desempenho no domínio da sua Força (e.g., o Comandante da Força Aérea é piloto de caça, e o Comandante da Marinha é oficial de submarino). É apropriado que esses oficiais tenham experiência no tipo de combate do seu domínio. Precisam transmitir os desafios associados com os seus domínios aos formuladores de políticas. Depois, esses comandantes interpretam a orientação política e disseminam a verba para a sua Força Singular. A questão é: quem realiza essa função para o domínio cibernético? O comandante do CYBERCOM,

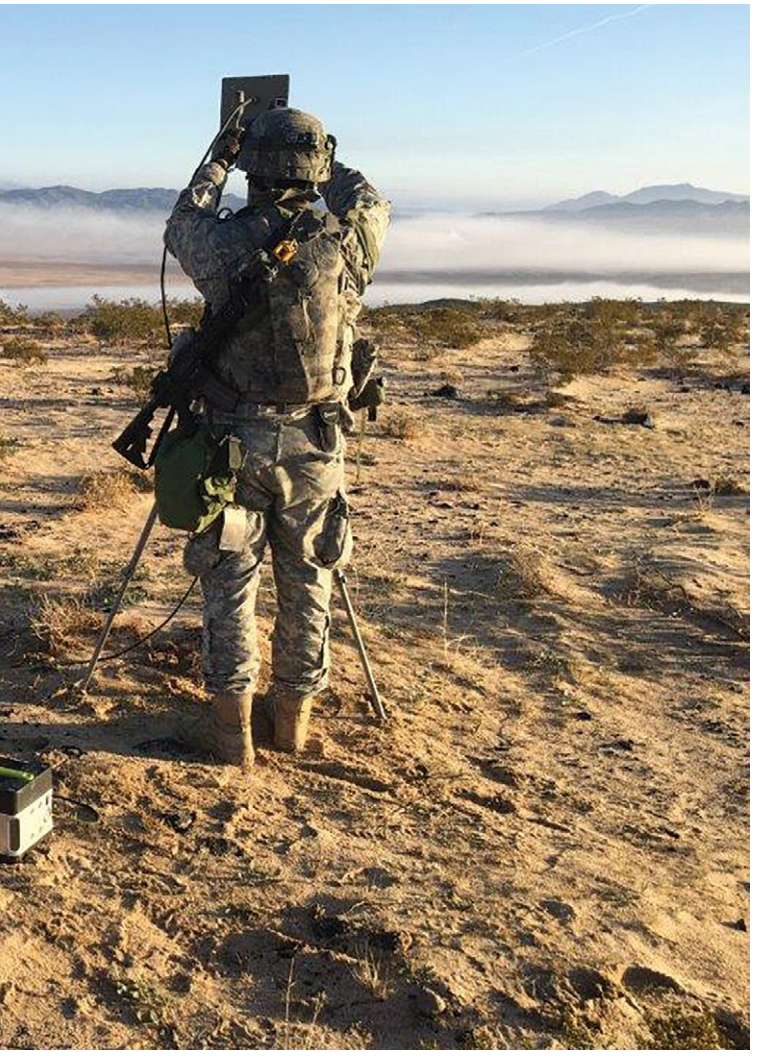
atualmente, intercede a favor do ciberespaço. Contudo, o CYBERCOM é subordinado ao Comando Estratégico (STRATCOM) dos EUA, possuindo vários escalões entre ele e os formuladores de políticas. Além disso, o Comandante do CYBERCOM ascendeu ao posto de dentro de uma das Forças Singulares, em grande medida governada por oficiais que se concentram nos seus domínios físicos. Considerando que as Forças Singulares determinam quais oficiais são promovidos, até o Comandante do CYBERCOM precisa dividir a sua atenção entre o espaço cibernético e o domínio da sua Força Singular ou corre o risco de não conseguir avançar. O estabelecimento da Força Cibernética, inclusive com o seu próprio membro na Junta de Chefes de Estado-Maior, permitiria que comandantes com profunda experiência no ciberespaço comuniquem efetivamente os desafios da guerra cibernética aos formuladores de políticas. Por sua vez, os chefes da Força Cibernética podem empregar eficientemente a orientação e os recursos destinados às operações militares no ciberespaço.

Guerreiros Cibernéticos Além de desenvolver comandantes experientes para o ramo, a Força Cibernética iria atrair e formar guerreiros cibernéticos mais qualificados. Atualmente, civis que querem defender a nação no ciberespaço precisam escolher entre uma das Forças Singulares existentes e passar pelo seu currículo de treinamento básico. Embora esses programas sejam adaptados precisamente para a produção de soldados, marinheiros, aviadores e fuzileiros navais, talvez sejam desnecessários e intimidadores para civis que simplesmente querem participar na competição predominantemente mental da guerra cibernética. Com certeza, o Departamento de Defesa emprega muitos civis que estão envolvidos nas atividades do ciberespaço, porém isso não é a solução ideal. Há complicações legais ter civis conduzindo a guerra, e o recrutamento de guerreiros cibernéticos como militares mais precisamente reconhece a sua contribuição e permite mais mobilidade ascendente e comando. Ao estabelecer a Força Cibernética, as Forças Armadas iriam apropriadamente recrutar e categorizar os seus guerreiros cibernéticos, sem dissuadir civis interessados e influenciá-los a entrar nas indústrias lucrativas de computação e comunicações.

O treinamento dos guerreiros cibernéticos também ficaria mais eficiente na Força Cibernética. Atualmente, cada Força Singular está formando um programa de treinamento para os seus respectivos guerreiros cibernéticos. Por exemplo, o Exército estabeleceu o Centro Cibernético de Excelência, no Forte Gordon, na Geórgia. Esse método distribuído para o desenvolvimento de guerreiros cibernéticos quase garante ineficiência para o maior esforço do Departamento de Defesa no ciberespaço. Embora o CYBERCOM

trabalhe para estabelecer padrões comuns para o treinamento cibernético entre todas as Forças Singulares, as interpretações entre elas divergirão, embora apenas ligeiramente. Os professores em cada um desses centros produzirão resultados desiguais. Por exemplo, o Exército pode empregar o melhor instrutor de código de programa, enquanto o CFN talvez contrate o melhor instrutor de redes de computadores. Apesar de padrões comuns de treinamento, as interpretações diferentes e as habilidades variadas dos instrutores produzirão

guerreiros cibernéticos de qualidade inferior ao ideal. De modo inverso, a Força Cibernética poderia concentrar os melhores professores em um único centro de instrução do ciberespaço e, assim, melhor supervisionar a implantação dos padrões. Além disso, considerando que os estudantes estariam também no mesmo lugar, haveria uma maior interação entre eles, principalmente entre os destaques das turmas, e o corpo docente facilitaria uma pesquisa mais aprofundada sobre o ciberespaço.



(Exército dos EUA)

Militares da 780ª Brigada de Inteligência Militar conduzem operações no ciberespaço durante um rodízio de treinamento para a 2ª Brigada de Combate Stryker, 2ª Divisão de Infantaria, no Centro Nacional de Treinamento, no Forte Irwin, Califórnia. A unidade, com sede no Forte Meade, Maryland, era uma de várias organizações cibernéticas que participaram no rodízio como parte de um programa piloto planejado para ajudar o Exército a construir e empregar capacidades cibernéticas nas suas formações táticas.

O desenvolvimento continua após o treinamento. As designações e a prática começam quando o treinamento termina. Como uma Força Singular independente, a Força Cibernética pode habilidosamente adaptar o desenvolvimento de carreira dos seus guerreiros cibernéticos. Campos apropriados podem ser estabelecidos (e.g., codificação, comunicação inter-rede, proteção antivírus ou controle de intrusões), e os planos de carreira podem, também, ser projetados, incluindo designação nas unidades de ciberespaço, agências de desenvolvimento de capacidade e estados-maiores conjuntos, onde podem integrar efeitos do ciberespaço com operações nos domínios físicos. Atualmente, os guerreiros cibernéticos devem obediência às necessidades dos recursos humanos da sua Força Singular e, frequentemente, são vistos como intercambiáveis com o pessoal de comunicações. Embora certamente exista uma justaposição entre os campos de comunicações e de guerra cibernética, uma força cibernética capacitará melhor o discernimento de perícia e melhor gestão do capital humano.

Atuação dentro do ciberespaço. A vantagem principal do estabelecimento de uma Força Cibernética independente é a capacidade de desenvolver a força mais competente possível. Contudo, a atuação dentro do ciberespaço também ficará menos arriscada e mais eficiente. Nos domínios físicos, é relativamente fácil dividir o campo de batalha por localização física: o Exército opera no interior, a Marinha no mar, o CFN nos litorais e a Força Aérea no céu. No entanto, não existem essas fronteiras óbvias no ciberespaço, e todas as quatro Forças Singulares atuam por todo ele. A oportunidade de uma Força Singular infringir, ou sabotar inadvertidamente, uma operação no ciberespaço de outra é muito maior do que nos domínios físicos separados. O ônus de comando e controle e o risco de fratricídio no ciberespaço aumentam com o número de guerreiros cibernéticos das quatro Forças Singulares diferentes atuando independentemente no domínio. Outra consequência de quatro distintos esforços no ciberespaço é o potencial de redundância não intencional (i.e., duas Forças Singulares podem dedicar recursos para resolver o mesmo problema ou desenvolver a mesma capacidade). Um esforço conjunto de supervisão pode reduzir um pouco da redundância, porém mais burocracia acrescenta tempo e custos a um processo de desenvolvimento de capacidade já demorado. A

remoção das quatro Forças Singulares do combate pelo ciberespaço reduz o risco de elas pisotearem umas às outras e de desperdiçar recursos.

As vantagens para as Forças Armadas. No livro *Good to Great - Empresas Feitas para Vencer*, Jim Collins moderniza alguns dos pensamentos de Adam Smith e observa que as empresas bem-sucedidas se apegam aos seus conceitos centrais, repudiando distrações. Collins oferece três perguntas para ajudar a determinar um conceito central de uma empresa: Está apaixonado profundamente com o que? Em que pode ser o melhor do mundo? O que compele o seu motor econômico?[2] Embora a última pergunta seja difícil traduzir para o setor público, as primeiras duas ajudam a esclarecer a razão pela qual o ciberespaço não deve ser uma competência central para as Forças Singulares existentes. É difícil imaginar a Marinha como a melhor do mundo na guerra cibernética, ao mesmo tempo em que é a melhor do mundo na guerra marítima. Da mesma forma, poucos fuzileiros navais se descreveriam como profundamente apaixonados com a guerra cibernética. A natureza delicada e distante da guerra cibernética se conflita com a cultura de combate aproximado e pessoal do CFN. Ao tirar a distração da guerra cibernética e transferi-la para a nova Força Cibernética, as Forças Singulares atuais mantêm a sua concentração nos seus domínios específicos.

(Imagem cortesia do CERDEC)

Os limites entre as ameaças cibernéticas tradicionais e as ameaças tradicionais de guerra eletrônica têm se tornado indistintos. O Programa Integrado de Guerra Cibernética e de Guerra Eletrônica, do Centro de Pesquisa, Desenvolvimento e Engenharia de Comunicações-Eletrônica (CERDEC), emprega as capacidades de guerra cibernética e eletrônica como um sistema integrado para aumentar o conhecimento da situação do comandante.

Como uma Força Singular, a Força Cibernética pode prover contingentes a cada um dos comandos combatentes, na forma de um Comando do Componente Cibernético (CCC). Da mesma forma que os componentes existentes das Forças Singulares servem, frequentemente, duplas funções como componentes funcionais (e.g. um comando componente da Força Aérea pode, também, servir como um comando componente da força aérea conjunta), o CCC arcaria com as responsabilidades funcionais da guerra cibernética. A Força Cibernética pode equipar cada um dos comandos combatentes geográficos com um CCC focado nos sistemas da área de responsabilidade. O CCC do Comando Estratégico dos EUA (STRATCOM) pode servir como um sincronizador mundial das ameaças que atravessam áreas de responsabilidade, e o CCC do Comando das Operações Especiais dos EUA (SOCOM) pode prover guerreiros cibernéticos capazes de infiltração física para obter acesso direto aos sistemas de circuito fechado do adversário. Talvez com o consentimento alvará do Departamento de Defesa, o CCC do Comando de Transporte dos EUA poderia fortalecer os sistemas cibernéticos dos parceiros-chave do setor de transporte (e.g., empresas particulares de transporte de carga, controladores de tráfico aéreo e empresas ferroviárias), ajudando a força conjunta a superar os desafios de antiacesso. Operar uma força cibernética é muito mais simples e mais eficiente do que ter as Forças Singulares existentes a contribuir com o CYBERCOM, o qual tem que juntar improvisadamente as unidades cibernéticas e entregá-las aos comandos combatentes posteriormente.

(Sgt Chuck Burden, Exército dos EUA)

O Comandante do Exército, Gen Ex Mark Milley, observa oficiais do Instituto Cibernético do Exército na Academia Militar dos EUA, em West Point, Nova York, demonstrar o abatimento de um veículo aéreo não tripulado (VANT) utilizando-se de um fuzil com capacidades cibernéticas.

Outra abordagem para aumentar a eficiência. Uma terceira abordagem, separada da abordagem atual do Departamento de Defesa e de uma força cibernética completamente independente, envolveria a promoção do CYBERCOM atual para um comando combatente funcional, no mesmo nível do STRATCOM ou do SOCOM. A elevação do CYBERCOM para esse nível seria um passo intermediário apropriado e provável para o estabelecimento da Força Cibernética independente. Isso pode remover uma das camadas hierárquicas entre o CYBERCOM e os formuladores de políticas. Além disso, o SOCOM conta com bastante influência sobre o desenvolvimento de tropas especiais das Forças Singulares. No entanto, esse arranjo resolve apenas uma parte do problema. Como um comando combatente, o CYBERCOM ainda seria dependente das Forças Singulares existentes para a execução das suas operações. Os guerreiros cibernéticos ainda enfrentariam a decisão de ter de escolher um canal de ciberespaço entre as Forças Singulares para navegar o caminho para o trabalho no CYBERCOM. Esse arranjo funciona para o SOCOM porque o treinamento para um piloto AC-130 da Força Aérea é diferente do de um SEAL (Forças Especiais) da Marinha, que é, também, diferente do desenvolvimento de um soldado das Forças Especiais do Exército, mas isso não é verdadeiro considerando o ciberespaço. Uma operação no ciberespaço é a mesma, independente do domínio físico do qual é lançada. A solução que fornece ao Departamento de Defesa unidades de ciberespaço melhor alocadas de pessoal, treinadas e equipadas é uma força cibernética independente.

O Estabelecimento da Força Cibernética dos EUA: Após a Próxima Guerra

Com tantas razões que apoiam o estabelecimento da Força Cibernética dos EUA, o que o impede? Há dois grandes obstáculos. Primeiro, o ciberespaço ainda não foi provado ser uma zona de combate nas mentes de muitos oficiais de alto escalão na área de segurança.

(Foto cortesia da Agência de Segurança Nacional)

O Comando Cibernético dos EUA é localizado no Forte Meade, Maryland, junto com as sedes da Agência de Segurança Nacional e do Serviço de Segurança Central.

Segundo, na ausência de uma ameaça de segurança significativa, os recursos de segurança nacional necessários para tal grande revisão permanecerão indisponíveis. O próximo grande conflito dos Estados Unidos provavelmente eliminará os dois obstáculos.

Como provar que o ciberespaço é um espaço de combate. O domínio aéreo exerceu um papel na Primeira Guerra Mundial, sendo que balões de observação e duelos entre aeronaves (guerra aérea, no estilo do Barão Vermelho) foram as características aéreas predominantes desse conflito. No entanto, os combatentes da Segunda Guerra Mundial realmente entendiam a significância da superioridade aérea. A Batalha da Grã-Bretanha, a campanha de bombardeio estratégico dos aliados, o advento de unidades paraquedistas e, por último, o bombardeio de Hiroshima e Nagasaki demonstraram a importância do combate no céu.

Atualmente, o ciberespaço se encontra no tipo de incerteza que o poder aéreo tinha durante os anos entre-guerras. Não obstante, houve uns poucos casos isolados de guerra cibernética entre Estados. Em abril de 2007, a Rússia conduziu um ataque efetivo de negação de serviço contra as grandes redes da Estônia, paralisando muitas das funções econômicas e governamentais dessa nação[3]. Da mesma forma, a Rússia atacou a Geórgia pelo ciberespaço, junto com a sua invasão da Ossétia do Sul, em 2008[4]. Além disso, os governos rotineiramente usam o ciberespaço para penetrar redes, roubando planos de mísseis, fórmulas químicas e dados financeiros[5]. Contudo, semelhante ao poder aéreo em 1920, as operações cibernéticas desempenharam um papel relativamente pequeno durante as últimas guerras dos EUA, e alguns céticos ainda consideram o ciberespaço uma arena de uma pessoa dedicada a um hobby ou *o domínio que pode-se desligar*.

As atividades no ciberespaço impactam cada vez mais as operações cotidianas das Forças Armadas e a economia dos EUA, bem como as operações dos seus aliados e adversários (tanto estatais, quanto não estatais). Durante a próxima guerra, é provável que o

ciberespaço seja uma característica mais predominante do que nos conflitos anteriores. Se os Estados Unidos vencerem ou perderem as batalhas no ciberespaço da próxima guerra, a importância dos combates justificará a criação de uma Força Cibernética. Se os guerreiros cibernéticos dos EUA saírem-se vitoriosos, como os aviadores fizeram nos céus da Europa em 1944, o ciberespaço haverá sido provado como um domínio legítimo de combate, e o argumento para a independente Força Cibernética será validado. Se os Estados Unidos não conseguirem superioridade no ciberespaço e sofrerem as consequências sufocantes, as ineficiências da eficiência. Depois, quando os orçamentos são menores e a eficiência é realmente necessária, o capital necessário para otimizar as práticas não pode ser dispensado. Com um dividendo da paz como objetivo, a despesa requerida para estabelecer uma força militar nova e mais eficiente não está disponível. Conforme as guerras da última década se acabarem, os orçamentos de defesa também diminuirão. É verdade que o orçamento de defesa diminuiu depois da Segunda Guerra Mundial, e a nação ainda conseguiu estabelecer a Força Aérea. Nessa situação, os chefes das políticas de segurança nacional corretamente identificaram a ascendente ameaça co-

(David Vergun/ U.S. Army)

O centro de operações táticas da 2ª Brigada de Combate, 1ª Divisão Blindada participa da Avaliação de Integração de Redes 16.1, no Forte Bliss, Texas. O exercício, que decorreu entre 25 Set a 8 Oct 15, avaliou uma rede de coalizão que vinculava as diversas redes de 14 outros exércitos que participaram ao vivo ou de forma virtual em um ambiente de combate simulado. As novas tecnologias avaliadas durante o exercício incluíram capacidades de rede da coalizão, postos de comando expedicionários, capacidades de energia operacional e formação de equipes tripuladas e não tripuladas (a robótica aérea e terrestre).

da abordagem atual do Departamento de Defesa para o ciberespaço serão enfatizadas, e uma força cibernética servirá como o remédio.

Carl von Clausewitz observou que a guerra exige o uso máximo de força que uma nação pode reunir: "Se um dos lados utiliza a força sem remorso ... enquanto que o outro abstém-se de utilizá-la, o primeiro estará em vantagem"[6]. Trazer a máxima força ao inimigo, incluindo efeitos pelo ciberespaço, é a garantia mais segura de sucesso, e organização ineficiente impedirá esse esforço.

Novas guerras, novos orçamentos. É uma dinâmica estranha das organizações que, quando os orçamentos são grandes, seus chefes priorizam o crescimento acima munista como uma justifica pela despesa. Hoje, depois das guerras no Iraque e no Afeganistão, nenhuma única ameaça identificável emergiu para convencer a nação a adiar o esperado dividendo da paz. Portanto, a consecução da eficiência por meio da criação de uma força cibernética independente precisa esperar até que recursos financeiros estejam disponíveis. Esses recursos da defesa provavelmente se tornarão disponíveis quando o ciberespaço prova a sua viabilidade como um domínio de combate, durante o próximo grande conflito.

Conclusão

Os Estados Unidos precisam de uma força militar independente focada no ciberespaço, mas

provavelmente terão de esperar até o próximo grande conflito para o estabelecimento dele. A abordagem atual do Departamento de Defesa para o ciberespaço, onde as Forças Singulares existentes fornecem o pessoal com experiência variada ao CYBERCOM, está cheia de ineficiências. O estabelecimento da Força Cibernética permitiria que a comunidade dos guerreiros cibernéticos prosperasse, e aliviaria as Forças Singulares existentes da distração com o ciberespaço. O próximo conflito dos Estados Unidos permitirá que os guerreiros cibernéticos demonstrem a importância do seu domínio e proverá às Forças Armadas os recursos para apoiar uma grande revisão burocrática.

A previsão que levará mais um conflito para estabelecer uma força cibernética é simplesmente uma premissa baseada no provável desenrolar de eventos. A liderança inspirada pode adiantar a formação da nova Força Singular.

Clausewitz compara a guerra com uma partida de lutadores, observando que "seu propósito *imediato* é *derrubar* o seu oponente de modo a torná-lo incapaz de oferecer qualquer outra resistência [grifos no texto original]"[7]. Ele observa que se um lutador usa toda a sua força para imobilizar o seu oponente, o beligerante imobilizado talvez nunca tenha a oportunidade de reunir a sua força total. Devido ao isolamento por dois oceanos, os Estados Unidos, historicamente, têm se dado o luxo de reunir a sua força militar antes de comprometer-se à guerra. No entanto, oceanos significam pouco no ciberespaço, e, se despreparados, os Estados Unidos podem sofrer grande prejuízo durante os ataques cibernéticos iniciais da próxima grande guerra. Os líderes sábios da defesa começarão a incitar as Forças Armadas para o estabelecimento da Força Cibernética dos EUA, para conseguir foco e eficiências superiores antes do próximo conflito, em vez de depois dele.

O Maj Matt Graham é estrategista do Exército dos EUA designado à Diretoria do Estado-Maior Conjunto para o Desenvolvimento da Força Conjunta. É mestre em Administração Pública pela George Washington University e bacharel em Ciência de Computação pela Academia da Força Aérea dos EUA. Designações anteriores incluem rodízios no Alasca, Alemanha, Washington, D.C., Iraque e Afeganistão.

Referências

1. Adam Smith, *An Inquiry into the Nature and Causes of the Wealth of Nations: A Selected Edition,* ed. Kathryn Sutherland (Oxford, UK: Oxford University Press, 2008), p. 12–14.

2. Jim Collins, *Good to Great: Why Some Companies Make the Leap … and Others Don't* (New York: Harper Collins Publishers, 2001), p. 94–96.

3. Scheherazade Rehman, "Estonian's Lessons in Cyberwarfare," website da U.S. News and World Report, 14 Jan. 2013, acesso em 22 ago. 2014, http://www.usnews.com/opinion/blogs/world-report/2013/01/14/estonia-shows-how-to-build-a-defense-against-cyberwarfare.

4. E. Lincoln Bonner III, "Cyber Power in 21st-Century Joint Warfare," *Joint Force Quarterly* 74 (2014): p. 102.

5. Michael Riley, "How Russian Hackers Stole the Nasdaq," website da Bloomberg Business, 17 Jul. 2014, acesso em 4 mar. 2016, http://www.bloomberg.com/bw/articles/2014-07-17/how-russian-hackers-stole-the-nasdaq.

6. Carl Von Clausewitz, On War, ed. e trad. Michael Howard e Peter Paret (Princeton, NJ: Princeton University Press, 1984), p. 75-76. Para a tradução do inglês para o português deste mesmo livro, consulte, Carl Von Clausewitz, Da Guerra, CMG (RRm) Luiz Carlos Nascimento e Silva do Valle.

7. Ibid., p. 75.