A Utilidade do Poder Cibernético

Ten Cel Kevin L. Parker,
Força Aérea dos EUA

O Ten Cel Kevin L. Parker, da Força Aérea dos EUA, comanda o 100º Regimento de Engenharia Civil na base da RAF em Mildenhall, Reino Unido. É bacharel em Engenharia Civil pela Texas A&M University; mestre em Desenvolvimento de Recursos Humanos pela Webster University; e mestre em Arte e Ciência Operacional Militar e em Estratégia Militar pela Air University. Serviu em missões na Arábia Saudita, no Quirguistão e, em duas ocasiões, no Iraque.

Decorridos mais de 50 anos, a Guerra da Coreia não terminou oficialmente, mas barragens de artilharia raramente atravessam a zona desmilitarizada[1]. As Forças norte-americanas continuam a combater no Afeganistão após mais de uma década, sem nenhuma declaração formal de guerra[2]. Um outro conflito transcorre hoje sem munições nem declarações. Nele, os adversários dos EUA conduzem sondagens, ataques e assaltos diariamente[3]. As ofensivas não são visíveis nem audíveis, mas são tão reais quanto granadas ou dispositivos explosivos improvisados. Esse conflito ocorre diariamente no ciberespaço, ou espaço cibernético.

Para cumprir seu objetivo de defender o país e promover os interesses nacionais, as Forças Armadas dos Estados Unidos da América (EUA) enfrentam um complexo ambiente de segurança que requer uma participação cada vez maior no ciberespaço[4]. Por essa razão, o Departamento de Defesa dos EUA hoje o considera um domínio operacional[5]. À semelhança de outros domínios, o ciberespaço tem seu conjunto próprio de características. Esses atributos apresentam vantagens especiais e limitações correspondentes. Conforme o caráter da guerra muda, compreender a utilidade do poder cibernético requer uma avaliação de suas vantagens e limitações em possíveis contextos estratégicos.

Definições de Ciberespaço e Poder Cibernético

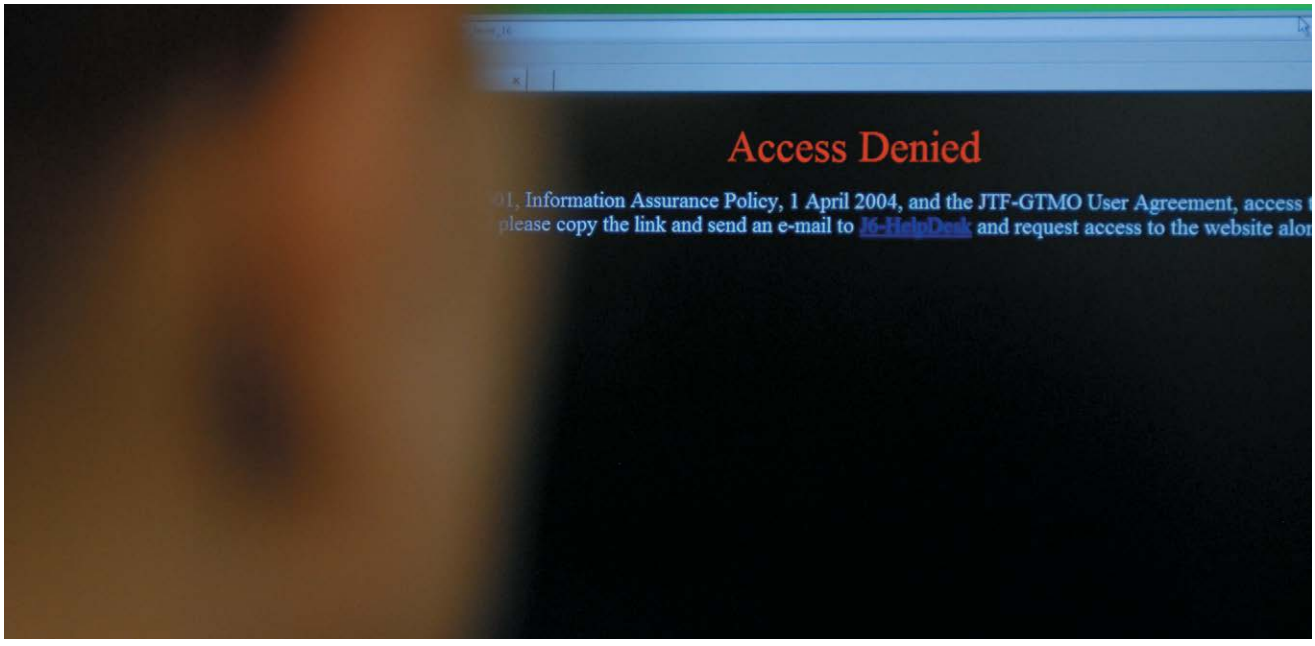
O ciberespaço (espaço cibernético) e o poder cibernético são

definidos de várias maneiras, mas até a importância de se estabelecer uma definição é objeto de debate. Daniel Kuehl chegou a compilar 14 definições diferentes para ciberespaço, oriundas de diversas fontes, mas acabou concluindo que deveria propor sua própria versão[6]. É fundamental que haja uma definição exata? Em organizações burocráticas, as definições importam por facilitarem uma divisão clara de papéis e missões entre os Departamentos e as Forças Singulares. No Departamento de Defesa, um certo grau de duplicação de esforços talvez seja desejável, mas acarreta um alto custo. Portanto, é preciso estabelecer definições para facilitar as rigorosas análises que são essenciais à estipulação de limites organizacionais e orçamentos[7]. Na execução das funções atribuídas, as definições têm grande importância para a comunicação e coordenação entre organizações.

Por mais importante que sejam, é difícil propor definições precisas que satisfaçam a todos os pontos de vista e contextos. Suponha, por exemplo, que se defina "mar" como sendo o conjunto de todos os oceanos do mundo. Essa definição não é clara o suficiente para demarcar baías ou canais. Ainda que pareça ser algo sem importância, a ambiguidade tem grandes consequências para organizações cuja jurisdição seja demarcada pela margem de um rio. Ao contrário do mar, a internet é um fenômeno relativamente novo, que continua a crescer e a evoluir rapidamente. Talvez seja inútil buscar definições de ciberespaço e poder cibernético que resolvam todas as questões. David Lonsdale propôs

O Comando Cibernético dos EUA realizou um exercício cibernético conjunto em novembro de 2011 na Base Aérea de Nellis, Nevada. O exercício contou com a participação de aproximadamente 300 profissionais de cibernética e tecnologia da informação, 02 Nov 11.

Exército dos EUA



Acesso Negado! O setor de Garantia da Segurança das Informações da Divisão Conjunta de Computadores e Cibernética opera *proxies* para proteger os servidores da Força-Tarefa Conjunta Guantánamo contra *sites* maliciosos. Esse setor defende os servidores da Força-Tarefa Conjunta contra ameaças internas e externas, ao mesmo tempo que garante sua conformidade com procedimentos e políticas da Agência de Sistemas de Informações do Departamento de Defesa, Exército dos EUA e Comando Sul dos EUA, Baía de Guantánamo, Cuba 08 Jul 08.
Marinha dos EUA

que, de uma perspectiva estratégica, definições não importam muito. A seu ver, "o que realmente importa é enxergar a *infoesfera* como um lugar que existe, entender sua natureza e considerá-la como algo passível de ser manipulado e utilizado para vantagem estratégica"[8]. As definições adiante são coerentes com a ótica de Lonsdale e suficientes para os fins desta discussão, mas é improvável que satisfaçam profissionais que queiram aplicá-las fora de uma perspectiva estratégica.

Ciberespaço ou espaço cibernético: o domínio que existe para a inserção, armazenamento, transmissão e extração de informações utilizando o espectro eletromagnético. Inclui todos os tipos de *hardware*, *software* e mídias de transmissão utilizados, desde os dados inseridos por um "iniciador" (ex.: pressionando teclas, falando ao microfone ou escaneando documentos) até a apresentação das informações à percepção do usuário (ex.: imagens na tela, sons emitidos pelos alto-falantes ou reprodução de um documento) ou alguma outra ação (ex.: guiar um veículo não tripulado ou fechar válvulas).

Poder cibernético: O potencial para utilizar o ciberespaço para obter os resultados desejados[9].

Vantagens de Empregar o Poder Cibernético

Considerando essas definições suficientes para esta discussão, analisemos as vantagens das operações por meio do ciberespaço.

O ciberespaço proporciona um alcance mundial. O número de pessoas, lugares e sistemas interligados pelo ciberespaço vem crescendo aceleradamente[10]. Essas conexões aumentam a capacidade das Forças Armadas para alcançar pessoas, lugares e sistemas em todo o mundo. Atuar no ciberespaço possibilita o acesso a áreas negadas em outros domínios. Os defensores iniciais do poder aéreo alegaram que os aviões ofereciam uma alternativa ao emprego de tropas terrestres e eram capazes de ultrapassar as defesas do inimigo e atacar os centros de poder

diretamente[11]. Sistemas sofisticados de defesa antiaérea evoluíram rapidamente, aumentando o risco para a condução de ataques aéreos e diminuindo sua vantagem. Apesar de existirem defesas cibernéticas, o ciberespaço hoje oferece a vantagem de acesso a áreas contestadas, sem colocar os operadores em perigo. Um exemplo em que o ciberespaço foi utilizado para alcançar diretamente os decisores inimigos foi um evento ocorrido em 2003, antes da invasão norte-americana do Iraque. O Comando Central dos EUA teria, supostamente, enviado um *e-mail* aos oficiais iraquianos pela rede sigilosa, orientando-lhes a deixar seus postos[12]. Nenhum outro domínio teve tamanho alcance com tão pouco risco.

O ciberespaço possibilita ações rápidas e concentração. O ciberespaço não só permite um alcance mundial, mas sua velocidade é inigualável. Embora as forças aéreas possam alcançar praticamente qualquer parte do mundo com o reabastecimento aéreo, chegar até o local desejado pode levar horas. A existência de bases avançadas talvez reduza o tempo de resposta a alguns minutos, mas as informações transmitidas por cabos de fibra óptica viajam, literalmente, à velocidade da luz. Os iniciadores de ataques cibernéticos podem alcançar concentração com a ajuda de outros computadores. Ao distribuir, discretamente, um vírus treinado para responder a comandos, milhares de computadores em uma *botnet* (rede de computadores infectados) podem iniciar, instantaneamente, um ataque distribuído de negação de serviço. Os atores envolvidos podem persuadir outros usuários a aderir à sua causa voluntariamente, como no caso dos "hackers patrióticos" russos, que participaram dos ataques contra a Estônia em 2007[13]. Com essas técnicas, grandes populações interconectadas poderiam ser mobilizadas em uma escala inédita em termos de massa, tempo e concentração[14].

O ciberespaço permite o anonimato. Os criadores da internet priorizaram a descentralização, desenvolvendo sua estrutura com base na confiança mútua entre seus poucos usuários[15]. Nas décadas desde sua criação, o número de usuários e finalidades cresceu exponencialmente, indo muito além da concepção original[16]. O sistema resultante faz com que seja muito difícil seguir um rastro de evidências e identificar um usuário[17]. O anonimato permite liberdade de ação, dificultando a atribuição de responsabilidade.

Defender-se contra ataques cibernéticos requer mais que *firewalls*.

O ciberespaço favorece a ofensiva. Na época de Clausewitz, a defesa se destacava, mas, em função das vantagens enumeradas, o ciberespaço atualmente favorece o ataque [18].

Historicamente, vantagens adquiridas com saltos tecnológicos vão diminuindo com o tempo[19]. Contudo, as atuais circunstâncias obrigam defensores a enfrentar ataques rápidos e concentrados, auxiliados por vulnerabilidades de segurança estruturais, intrínsecas à arquitetura do ciberespaço.

O ciberespaço amplia o espectro de armas não letais. Joseph Nye descreveu uma tendência, especialmente em democracias, ao antimilitarismo, o que torna o emprego da força "uma escolha politicamente arriscada"[20]. O desejo de limitar danos colaterais tem sido, com frequência, foco de atenção nas operações da Organização do Tratado do Atlântico Norte (OTAN), mas ele não se restringe a contrainsurgências[21]. As munições guiadas de precisão e as bombas de pequeno diâmetro são fruto de esforços para aumentar capacidades de ataque com um menor risco de danos colaterais. Os ataques cibernéticos oferecem meios não letais de ação direta contra um adversário[22]. As vantagens do poder cibernético podem parecer tentadoras para os formuladores de políticas, mas esse entusiasmo precisa ser moderado por um entendimento das limitações existentes. A mais óbvia é o fato de que um adversário pode utilizar todas as mesmas vantagens para atacá-lo. Outra limitação evidente é seu grau mínimo de influência sobre adversários que não estejam conectados à rede. Por outro lado, quanto mais uma organização depender do ciberespaço, mais vulnerável ficará a um ataque cibernético. Há três outras limitações a serem consideradas.

Os ataques no ciberespaço contam fortemente com efeitos de segunda ordem. Utilizando os termos propostos por Thomas Schelling, não há opções de emprego de força bruta por meio do

ciberespaço; assim as operações cibernéticas apoiam-se na coerção[23]. Os exércitos continentais podem ocupar um terreno e conquistar objetivos pela força bruta, mas o êxito nas operações pelo ciberespaço muitas vezes dependem de como os adversários reagem a informações fornecidas, alteradas ou omitidas. É possível conduzir ataques cibernéticos que criem efeitos cinéticos, como comandos destrutivos enviados a sistemas de controle industriais. Contudo, o caso especial do código malicioso que causou a explosão de um oleoduto russo e o emprego do *worm Stuxnet* para paralisar os processos de uma usina nuclear iraniana não eram objetivos finais[24]. Neste último caso, apenas os dirigentes iranianos poderiam tomar a decisão de abandonar atividades ligadas à tecnologia nuclear. Os ataques cibernéticos muitas vezes contam com efeitos de segunda ordem imprevisíveis, à semelhança dos bombardeios estratégicos na Segunda Guerra Mundial, que não foram capazes de destruir o moral[25]. Se o Contra-Almirante Wylie estiver certo quanto à guerra ser uma questão de controle e "sua principal ferramenta [...] [ser] o homem em cena, com uma arma", as operações no ciberespaço só podem conferir uma forma menor de controle[26]. Evgeny Morozov afirmou: "São as pessoas, e não mensagens no *Twitter*, que derrubam governos"[27].

Os ataques cibernéticos arriscam gerar consequências imprevistas. Da mesma forma que atingir o sistema de abastecimento de energia de uma base militar pode ter ramificações para uma população mais ampla, é difícil limitar efeitos no ciberespaço interligado. Os instrutores de tiro ensinam os atiradores a considerar seu máximo alcance e o que está além dos objetivos. Sem mapas para todos os sistemas, isso se torna impossível no ciberespaço.

É possível defender-se contra ataques cibernéticos. A atual vantagem ofensiva não inutiliza todos os tipos de defesa. Ainda que intrusões decorrentes de ataques sofisticados e persistentes sejam inevitáveis, algumas medidas defensivas oferecem certa proteção (ex.: controles de segurança física, restrição ao acesso de usuários, filtros e *software* antivírus e *firewalls*). A redundância e a duplicação são estratégias voltadas à resiliência, ou capacidade de recuperação, que podem dissuadir alguns potenciais agressores ao fazerem com que seja inútil atacar[28]. A possibilidade de represálias pelo ciberespaço ou por outros meios também pode reforçar a dissuasão[29]. Ainda que a defesa esteja, atualmente, em desvantagem, a ofensiva não tem total liberdade de ação no ciberespaço.

Expectativas e Recomendações

As vantagens e limitações do emprego do poder cibernético servem de base a expectativas para o futuro e a algumas recomendações para as Forças Armadas.

Não conte com o estabelecimento de uma política clara e abrangente no futuro próximo.[30] Uma estratégia norte-americana abrangente para o uso de armas nucleares só foi criada 15 depois de serem empregadas pela primeira vez, e um prazo maior pode ser necessário para a formulação de uma política clara e abrangente quanto ao ciberespaço[31]. Diferentes interesses colidem no ciberespaço, obrigando os formuladores de políticas a tratar de conceitos que o povo norte-americano tem, tradicionalmente, dificuldade em resolver. O ciberespaço, como a política externa, expõe a tensão entre optar pelo realismo político em um sistema desgovernado e anárquico e aspirar ao ideal liberal de segurança pelo reconhecimento mútuo de direitos naturais. Políticas relativas ao ciberespaço exigem que se avaliem diversas prioridades baseadas em valores considerados importantes como direitos de propriedade intelectual, o papel do governo no comércio, a aplicação da lei, a liberdade de expressão, os interesses de segurança nacional e a privacidade pessoal. Nenhuma dessas questões é nova. O ciberespaço simplesmente as conecta e as apresenta a partir de novos ângulos. Por exemplo, os direitos de liberdade de expressão podem não incluir o direito de gritar "incêndio" falsamente em um teatro lotado, mas, pelo ciberespaço, todas as palavras são transmitidas a um "teatro" mundial lotado[32].

Fora do âmbito nacional, o acesso à internet cria pelo menos um dilema significativo de política externa. Embora possa ajudar a mobilizar e a fortalecer dissidentes que vivam sob governos repressores, também pode proporcionar a dirigentes autoritários mais ferramentas de controle sobre a população[33]. Separar essas questões em novos contextos não será, provavelmente, algo que possa ser feito tão

Secretário do Exército John McHugh assiste a um *briefing* apresentado por oficiais do estado-maior do Comando Cibernético do Exército dos EUA, Forte Belvoir, Virgínia, 02 Abr 12.
Exército dos EUA

rápido. Talvez requeira várias tentativas e só ocorra durante crises. Enquanto isso, as Forças Armadas devem continuar a desenvolver capacidades para atuar por meio do ciberespaço em conformidade com as atuais políticas.

Conduza a defesa em profundidade — camadas internas. Conquistar a resiliência, ou capacidade de recuperação, requer avaliar situações de dependência e vulnerabilidades em todos os níveis. Indo do âmbito interno, atrás do *firewall*, ao externo, a defesa começa no nível da menor unidade. As organizações e funções devem ter uma capacidade de recuperação suficiente para sofrerem ataques e continuarem operando. Em uma época de orçamentos cada vez menores, os decisores buscarão eficiências por meio da tecnologia[34]. Portanto, a cautela exige que parte da economia obtida com essas eficiências seja reinvestida para avaliar e compensar as vulnerabilidades criadas por novos tipos de dependência tecnológica[35]. Os futuros jogos de guerra devem não só avaliar o que as novas tecnologias podem proporcionar, mas também considerar como todas as capacidades seriam afetadas caso o acesso ao ciberespaço fosse negado.

Fora as responsabilidades básicas de usuário, as Forças que proveem defesa contra ataques cibernéticos requerem organizações e estruturas de comando específicas à sua função. Martin van Creveld descreveu evoluções históricas de comando e avanços tecnológicos. Com base nessa análise, os líderes militares do setor de defesa cibernética devem resistir ao ímpeto, possibilitado pela tecnologia, de centralizar e controlar todas as informações disponíveis no escalão mais elevado. Em vez disso,

suas organizações devem agir de forma semi-independente, definir limiares de decisão baixos, implementar uma divulgação constante de informações e utilizar comunicações formais e informais[36]. Esses métodos podem aprimorar o "contínuo aprendizado baseado na tentativa e erro, que é essencial para desenvolver, coletivamente, um entendimento sobre surpresas incapacitadoras" e diminuir os tempos de resposta[37]. As estruturas de rede podem ser mais adequadas para esse tipo de tarefa que as tradicionais estruturas hierárquicas militares[38]. Independentemente da estrutura, a liderança militar deve estar disposta a deixar a tradição em segundo plano e a organizar as tarefas de suas defesas com o objetivo de efetividade contra ataques cibernéticos[39]. Afinal, as armas "não triunfam no combate; ao contrário, o sucesso é o produto de sistemas de armas com a *interface* homem-máquina; seus serviços de apoio de diversos tipos; e a organização, doutrina e adestramento que os lançam em combate"[40].

Conduza a defesa em profundidade — camadas externas. Defender-se contra ataques cibernéticos requer mais que *firewalls*. Ampliar a defesa em profundidade requer utilizar a influência de forma criativa. O Departamento de Defesa não tem posse ou jurisdição sobre os setores civis que operam a infraestrutura da internet e que desenvolvem *hardware* e programas de *software*. Entretanto, os sistemas do Departamento de Defesa são vulneráveis a ataques cibernéticos por ambos esses canais, que estão fora de seu controle[41]. Richard Clarke recomendou regulamentos federais, a começar com o *backbone*

Oficiais de Ligação no Centro Conjunto de Controle Cibernético durante a Operação *Deuce Lightning* recebem uma atualização sobre a Lista de Sincronização de Eventos da Missão, Grafenwoehr, Alemanha (23 Fev 11)

Exército dos EUA, Lawrence Torres III

da internet, como melhor forma de superar vulnerabilidades sistêmicas[42]. Reações negativas a possíveis leis sobre atividades na internet ilustram a natureza problemática da regulamentação[43]. Assim, como pode o Departamento de Defesa efetuar mudanças em áreas aparentemente fora de seu controle? Qualquer que seja o rótulo adotado — "poder persuasivo" ou "conquista amigável do ciberespaço" — a resposta está em explorar meios[44].

Um dos principais meios que o Departamento de Defesa possui para esse fim é seu poder de compra. Em 2011, o Departamento gastou mais de US$ 375 bilhões em contratos[45]. As Forças Armadas devem, é claro, usar seu poder aquisitivo para insistir em rigorosos padrões de segurança ao comprar *hardware* e *software*. Entretanto, também pode usar o processo de aquisições para reduzir vulnerabilidades com sua utilização de terceirizados na defesa. Da mesma forma que os requisitos detalhados para a classificação de documentos, os contratos devem especificar protocolos de segurança de rede para todas as firmas contratadas e seus fornecedores, independentemente dos serviços prestados. A manutenção de protocolos de segurança mais rigorosos que os padrões da indústria deve tornar-se uma condição para contratos lucrativos. Por meio de seus contratos, de seus aliados e de sua posição como maior empregador do país, o Departamento de Defesa pode utilizar preferências para melhorar suas defesas na camada externa[46].

Desenvolva uma defesa ofensiva. Até na guerra defensiva, Clausewitz reconheceu a necessidade de uma ofensiva para opor-se aos ataques do inimigo e obter a vitória[47]. Fortes capacidades ofensivas podem reforçar a dissuasão ao afetar o cálculo de decisão do adversário[48]. O Departamento de Defesa deve preparar-se para contingências que requeiram apoio ofensivo a outros domínios ou ações independentes por meio do ciberespaço.

As Forças Armadas devem desenvolver capacidades ofensivas para cenários potenciais, mas definir, intencionalmente, seus preparativos como defesa. É importante transmitir uma postura defensiva para evitar acelerar uma corrida armamentista cibernética inspirada em um dilema de segurança, a qual já pode ter começado[49]. Ao que consta, mais de 20 países possuem alguma capacidade para a guerra cibernética[50]. Mesmo que seja tarde demais para retardar o desenvolvimento ofensivo de outros, continua sendo importante controlar a narrativa[51]. Da mesma forma que a designação "Departamento de Defesa" comunica uma mensagem diferente que o nome anterior — "Departamento da Guerra" — desenvolver capacidades defensivas para bloquear agressores cibernéticos soa bem melhor que desenvolver capacidades ofensivas para "nocautear [o inimigo] no primeiro *round*"[52].

Não tenha a expectativa de que haja mudanças rápidas na ordem internacional ou na natureza da guerra. Sem dúvida, o mundo está mudando, mas a ordem internacional não é algo que se transforme da noite para o dia. Nye detalhou mudanças decorrentes da globalização e da disseminação de tecnologias da informação, incluindo a difusão do poder norte-americano para nações em ascensão e atores não estatais. Entretanto, ele alegou que não se tratava de uma "narrativa de declínio", afirmando: "É improvável que os EUA sofram um declínio como na Roma antiga ou que sejam ultrapassados por uma outra nação"[53]. Adaptar-se às tendências atuais é algo necessário, mas mudanças no ambiente estratégico não são tão drásticas quanto alguns declaram.

Da mesma forma, alguns aspectos da guerra mudam com o tempo, mas sua natureza permanece constante. Clausewitz recomendou que o planejamento levasse em conta o caráter contemporâneo da guerra[54]. Avanços no ciberespaço vêm transformando o caráter da guerra, sem, porém, ofuscar totalmente os meios tradicionais. Sir John Slessor observou: "Se existe uma postura mais perigosa que pressupor que uma futura guerra será exatamente como a anterior, é imaginar que ela será tão diferente que se possa ignorar todas as lições extraídas desta última"[55]. Além disso, Lonsdale recomendou que se explorassem avanços no ciberespaço, mas não se "esperasse que essas mudanças fossem alterar a natureza da guerra"[56]. As guerras continuarão a ser regidas pela política, afetadas pelo acaso e travadas por pessoas, mesmo que pelo ciberespaço[57].

Não prometa mais do que possa cumprir. Defensores do emprego do poder cibernético devem conter seu entusiasmo de modo a enxergar que sua utilidade só existe em um contexto estratégico. Colin Gray afirmou que os entusiastas do poder aéreo "praticamente levaram

o governo e o público a fazerem as perguntas erradas e a impor padrões irrelevantes, de uma efetividade super-heroica, ao desempenho da Força Aérea"[58]. Ao promover capacidades estratégicas, independentes e decisivas, os defensores do poder aéreo frequentemente deixaram de atender a tais expectativas exageradas em conflitos reais. Podem ter existido contextos estratégicos em que o poder aéreo, por si só, poderia obter efeitos estratégicos. Com mais frequência, porém, o poder aéreo é apenas uma das muitas ferramentas empregadas.

O mesmo se aplica ao poder cibernético. Gray alegou: "Quando uma nova forma de guerra é analisada e debatida, pode ser difícil persuadir os profetas que uma potencial eficácia não precisa ser definitiva"[59]. Defensores do poder cibernético devem reconhecer não apenas suas vantagens, como também suas limitações, aplicadas a um contexto estratégico.

Conclusão

Se o poder cibernético representa o potencial de usar o ciberespaço para obter os resultados desejados, então o contexto estratégico é chave para entender sua utilidade. A liderança militar deve avaliar seriamente quais as contribuições para a obtenção dos resultados finais, advindas de modificações das características da guerra, a partir de uma maior integração do poder cibernético no combate, ao lado de outros domínios. Os decisores devem avaliar as oportunidades e vantagens que o ciberespaço apresenta em comparação às vulnerabilidades e limitações das operações em tal domínio. Sir Arthur Tedder desprezava o debate sobre a possibilidade de que uma ou outra Força Singular fosse, por si só, capaz de vencer guerras. Insistiu: "Todos os três componentes da Defesa estão, inevitavelmente, envolvidos, embora o equilíbrio correto entre eles possa e vá variar"[60]. As guerras da atualidade podem envolver outros componentes, mas o conceito de Tedder, de aplicar uma combinação de ferramentas com base em suas vantagens e limitações no contexto estratégico, continua sendo um bom conselho.

Referências

1. Chico Harlan, "Korean DMZ troops exchange gunfire", *Washington Post*, 30 Oct. 2010. Disponível em: http://www.washingtonpost.com/wp-dyn/content/article/2010/10/29/AR2010102906427.html. Ocasionalmente, há disparos na zona desmilitarizada, mas essas ocorrências são raras.

2. Veja *Authorization for Use of Military Force*, Public Law 107-40, 107th Cong., 18 Sept. 2001. Disponível em: http://www.gpo.gov/fdsys/pkg/PLAW-107publ40/html/PLAW-107publ40.htm. O emprego da força militar no Afeganistão foi autorizado pelo Congresso dos EUA em 2001 por meio da Lei 107-40, que não inclui uma declaração de guerra.

3. "Os sistemas do Departamento de Defesa são sondados por usuários não autorizados aproximadamente 250.000 vezes por hora, mais de 6 milhões de vezes diariamente." Gen Keith Alexander, director, National Security Agency and Commander, U.S. Cyber Command (remarks, Center for Strategic and International Studies Cybersecurity Policy Debate Series: US Cybersecurity Policy and the Role of US Cybercom, Washington, DC, 3 Jun. 2010, 5) http://www.nsa.gov/public_info/_files/speeches_testimonies/100603_alexander_transcript.pdf.

4. "A finalidade deste documento é fornecer os métodos e meios pelos quais nossas Forças Armadas irão promover nossos interesses nacionais permanentes [...] e cumprir os objetivos de defesa na Revisão Quadrienal da Defesa de 2010". Joint Chiefs of Staff, *The National Military Strategy of the United States of America, 2011: Redefining America's Military Leadership* (Washington, DC: United States Government Printing Office [GPO], 8 February 2011), p. i.

5. DOD, *DOD Strategy for Operating in Cyberspace* (Washington, DC: GPO, July 2011), p. 5.

6. Daniel T. Kuehl, "From Cyberspace to Cyberpower: Defining the Problem", in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr e Larry K. Wentz (Dulles, VA: Potomac Books, 2009): p. 26-28.

7. Staff Report to the Senate Committee on Armed Services, *Defense Organization: The Need for Change*, 99th Cong., 1st sess., 1985, Committee Print, p. 442-44.

8. David J. Lonsdale, *The Nature of War in the Information Age: Clausewitzian Future* (London: Frank Cass, 2004), p. 182.

9. Veja Joseph S. Nye Jr., *The Future of Power* (New York: PublicAffairs, 2011), p. 123. Esta definição foi influenciada pela obra de Nye.

10. "From 2000 to 2010, global Internet usage increased from 360 million to over 2 billion people", DOD Strategy for Operating in Cyberspace, 1.

11. Giulio Douhet, *The Command of the Air* (Tuscaloosa, AL: University of Alabama Press, 2009), p. 9.

12. Richard A. Clarke e Robert K. Knake, *Cyber War: The Next Threat to National Security and What To Do About It* (New York: HarperCollins Publisher, 2010), p. 9-10.

13. Nye, p. 126.

14. Audrey Kurth Cronin, "Cyber-Mobilization: The New Levée en Masse", *Parameters* (Summer 2006): p. 77-87.

15. Clarke e Knake, p. 81-84.

16. Veja Clarke e Knake, p. 84-85. Tendências no número de dispositivos conectados à internet ameaçam utilizar todos os 4,29 bilhões de endereços disponíveis com base no sistema original de numeração de 32 bits.

17. Clay Wilson, "Cyber Crime", in *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, Larry Wentz (Washington, DC: NDU Press, 2009), p. 428.

18. Carl von Clausewitz, *On War*, ed. and trans. Michael Howard and Peter Paret (Princeton, NJ: Princeton University Press, 1976), p. 357; John B. Sheldon, "Deciphering Cyberpower: Strategic Purpose in Peace and War", *Strategic Studies Quarterly* (Summer 2011): p. 98.

19. Martin van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), p. 231.

20. Nye, p. 30.

21. Dexter Filkins, "US Tightens Airstrike Policy in Afghanistan", *New York Times*, 21 Jun. 2009. Disponível em: http://www.nytimes.com/2009/06/22/world/asia/22airstrikes.html.

22. "Vamos aprimorar nossas capacidades relativas ao ciberespaço de modo que possam obter efeitos significativos e proporcionais a um menor custo e impacto colateral." Chairman of the Joint Chiefs of Staff, *The National Military Strategy of the United States of America 2011: Redefining America's Military Leadership*, (Washington, DC: GPO, 2011), p. 19.

23. Thomas C. Schelling, *Arms and Influence* (New Haven, CT: Yale University, 2008), p. 2-4.

24. Sobre o oleoduto russo, veja Clarke e Knake, 93; sobre o *Stuxnet*, veja Nye, p. 127.

25. Lonsdale, p. 143-45.

26. Rear Adm. J.C. Wylie, *Military Strategy: A General Theory of Power Control* (Annapolis, MD: Naval Institute Press, 1989), p. 74.

27. Evgeny Morozov, *The Net Delusion: The Dark Side of Internet Freedom* (New York: PublicAffairs, 2011), p. 19.

28. Nye, p. 147.

29. Richard L. Kugler, "Deterrence of Cyber Attacks", *Cyberpower and National Security*, eds. Franklin D. Kramer, Stuart H. Starr, and Larry K. Wentz (Washington, DC: NDU Press, 2009), p. 320.

30. Veja *United States Office of the President, International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World*, May 2011.

31. Veja Clarke e Knake, p. 155. A estratégia internacional em relação ao ciberespaço trata da diplomacia, defesa e desenvolvimento no ciberespaço, mas não descreve as prioridades relativas para interesses conflitantes quanto às políticas.

32. Os direitos e respectivos limites relativos à liberdade de expressão que constam da Primeira Emenda Constitucional têm sido objeto de debate há décadas. A noção de "Gritar incêndio em um teatro lotado" se origina de um processo do Supremo Tribunal dos EUA, em 1919, "Schenck v. United States". O Juiz Oliver Wendell Holmes estabeleceu o contexto como sendo relevante para restringir a liberdade de expressão. Um teste de "ação ilícita iminente" substituiu seu teste de "perigo claro e presente" em 1969, http://www.pbs.org/wnet/supremecourt/capitalism/landmark_schenck.html.

33. Morozov, p. 28.

34. "As atuais capacidades da tecnologia da informação tornaram essa visão [de logística de precisão] possível, e a futura demanda por eficiência tornou a necessidade urgente." Gen. Norton Schwartz, chief of staff, U.S. Air Force, "Toward More Efficient Military Logistics", discurso em 29 mar. 2011, durante 27th Annual Logistics Conference and Exhibition, Miami, Flórida. Disponível em: http://www.af.mil/shared/media/document/AFD-110330-053.pdf.

35. Chris C. Demchak, *Wars of Disruption and Resilience: Cybered Conflict, Power, and National Security* (Athens, GA: University of Georgia Press, 2011), p. 44.

36. Van Creveld, p. 269-70.

37. Demchak, p. 73.

38. Antoine Bousquet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), p. 228-29.

39. See R.A. Ratcliff, *Delusions of Intelligence: Enigma, Ultra, and the End of Secure Ciphers* (Cambridge, UK: Cambridge University Press, 2006), p. 229-30. A criptoanálise Enigma, conduzida pelos aliados durante a Segunda Guerra Mundial oferece um bom exemplo de organização criativa de tarefas sem um hierarquia rígida.

40. Colin S. Gray, *Explorations in Strategy* (Westport, CT: Praeger, 1996), p. 133.

41. *DOD Strategy for Operating in Cyberspace*, p. 8.

42. Clarke e Knake, p. 160.

43 Geoffrey A. Fowler, "Wikipedia, Google Go Black to Protest SOPA", *Wall Street Journal*, 18 Jan. 2012, http://online.wsj.com/article/SB10001424052970204555904577167873208040252.html?-mod=WSJ_Tech_LEADTop; Associated Press, "White House objects to legislation that would undermine 'dynamic' Internet", *Washington Post*, 14 Jan. 2012, http://www.washingtonpost.com/politics/courts-law/white-house-objects-to-legislation-that-would-undermine-dynamic-internet/2012/01/14/gIQAJsFcyP_story.html.

44. "Soft power" (poder persuasivo ou brando), veja Nye, p. 81-82; "friendly conquest" (conquista amigável), veja Martin C. Libicki, *Conquest in Cyberspace: National Security and Information Warfare* (Cambridge, UK: Cambridge University Press, 2007), p. 166.

45. U.S. Government, USASpending.gov official Web site, "Prime Award Spending Data", http://www.usaspending.gov/explore?carryfilters=on (18 Jan. 2012). "2011" se refere ao exercício fiscal.

46. DOD Web site, "About the Department of Defense", http://www.defense.gov/about (18 Jan. 2012). O Departamento de Defesa emprega 1,4 milhão de militares da ativa, 1.1 milhão de militares da Guarda Nacional/Reserva e 718.000 funcionários civis.

47. Clausewitz, p. 357.

48. Kugler, "Deterrence of Cyber Attacks", p. 335.

49. "Muitos observadores sustentam que vários atores vêm desenvolvendo capacidades avançadas de ataque cibernético". Ibid., p. 337.

50. Clarke e Knake, p. 144.

51. "As narrativas são particularmente importantes para enquadrar questões de formas persuasivas." Nye, p. 93-94.

52. Citação do Gen Robert Elder como Chefe do Comando Cibernético da Força Aérea. Veja Clarke and Knake, p. 158; Defense Tech, "ChineseCyberwarAlert!"15 Jun. 2007, http://defensetech.org/2007/06/15/chinese-cyberwar-alert.

53. Nye, p. 234.

54. Clausewitz, p. 220.

55. John Cotesworth Slessor, *Air Power and Armies* (Tuscaloosa, AL: University of Alabama Press, 2009), p. iv.

56. Lonsdale, p. 232.

57. Clausewitz, p. 89.

58. Gray, p. 58.

59. Colin S. Gray, *Modern Strategy* (Oxford, UK: Oxford University Press, 1999), p. 270.

60. Arthur W. Tedder, *Air Power in War*, (Tuscaloosa: University of Alabama Press, 2010), p. 88.