(Foto de Lawrence Torres III)

Militares da 2ª Brigada de Comunicações concluem missão no Centro Conjunto de Controle Cibernético durante a Operação *Deuce Lightning*, em Grafenwoehr, na Alemanha, 23 Fev 11. Uma equipe de mais de 60 militares do Exército e da Força Aérea dos EUA e da Alemanha participaram do exercício para avaliar a capacidade da 2ª Brigada de Comunicações para prover apoio à rede.

A Relevância da Cultura

Reconhecendo a Importância da Inovação nas Operações Cibernéticas

Gen Div Edward C. Cardon; Cel David P. McHenry; e Ten Cel Christopher Cline, Exército dos EUA

No congresso e exposição anual da Associação do Exército dos Estados Unidos da América (EUA), realizados em outubro de 2015 em Washington D.C., os Capitães Brent Chapman, Matt Hutchinson e Erick Waage, do Exército dos EUA, demonstraram a ferramenta "fuzil cibernético", que haviam desenvolvido em dez horas, usando US$ 150 em peças sobressalentes. Essa ferramenta incapacitou, remotamente, um veículo aéreo não tripulado[1]. Logo após a demonstração, os

capitães, que serviam no Instituto Cibernético do Exército, da Academia Militar dos EUA, em West Point, Estado de Nova York, escreveram no blog *War on the Rocks* que as Forças Armadas dos EUA precisavam de um processo de inovação aberta. Opinaram que os processos de aquisições militares existentes não estão à altura das atuais e futuras ameaças cibernéticas, que geram a necessidade de que as Forças Armadas implementem respostas inovadoras rapidamente[2].

Estamos em meio a uma transformação na condução da guerra. No passado, os comandantes utilizavam a informação para moldar as operações. Atualmente, vemos como os ambientes informacional e operacional têm elementos em comum e, em alguns casos, coincidem totalmente. Na Ucrânia, a Rússia dominou o espectro eletromagnético, interrompendo as comunicações militares ucranianas, geolocalizando batalhões ucranianos com veículos aéreos não tripulados e, em seguida, destruindo-os com ataques de artilharia devastadores[3]. Os russos também desligaram os computadores de distribuição de eletricidade da Ucrânia e atacaram as linhas telefônicas para impedir que os clientes ligassem para informar a falta de energia[4].

Quiçá ainda mais importante: os adversários estão utilizando as mídias sociais de modo mais efetivo que as forças dos EUA para moldar a percepção do público e facilitar operações militares. Por exemplo, o predomínio do governo russo sobre as mídias sociais tem determinado quais informações estão disponíveis aos cidadãos russos e onde eles as obtêm. Da mesma forma, o Estado Islâmico explora as mídias sociais como uma arma estratégica para moldar a narrativa pública e para recrutar e levantar fundos. Esse uso crescente da guerra eletrônica (GE), guerra cibernética (G Ciber) e operações de informação (Op Info) na guerra híbrida indica a necessidade de valorizar a inovação nas operações cibernéticas (Op Ciber).

O Exército dos EUA está perdendo terreno diariamente por não explorar as inovações de seus adversários e do segmento civil. O setor cibernético do Exército dos EUA, como a maioria dos outros, vem assistindo à necessidade de mudanças paradigmáticas no modo pelo qual os líderes contemplam, facilitam e promovem a inovação. É preciso reexaminar como o Exército inova internamente ao mesmo tempo que explora a indústria de novas formas para inovar utilizando soluções externas. Os velhos modelos estão obsoletos, e o que se vê no ciberespaço faz com que essas mudanças paradigmáticas sejam um imperativo para as Forças Armadas como um todo.

Conforme demonstram Chapman, Hutchinson e Waage, o Exército dos EUA possui o talento que pode proporcionar o caminho para a inovação. Os comandantes precisam utilizar esse talento interno para desenvolver uma cultura de inovação que assegure o êxito das missões atuais e futuras. Para enfrentar os desafios de ambientes informacionais e operacionais complexos e em constante evolução, faz-se necessário examinar muitos de nossos próprios paradigmas para como lidamos com a inovação em toda a Força.

Definição de Inovação

Em novembro de 2014, o então Secretário de Defesa dos EUA, Chuck Hagel, anunciou a Iniciativa de Inovação da Defesa, a fim de destacar a necessidade de que o Departamento adote práticas e meios inovadores de operar em ambientes cada vez mais contestados. Hagel observou: "Estamos entrando em uma era em que a superioridade norte-americana em importantes áreas bélicas vem se desgastando, e precisamos encontrar formas novas e criativas para manter e, em algumas áreas, ampliar nossas vantagens, mesmo enquanto lidamos com recursos mais limitados"[5]. O atual Secretário de Defesa Ash Carter tem conservado esse impulso. O Departamento de Defesa continua a ampliar esforços de cooperação com o Vale do Silício por meio de iniciativas como a Unidade Experimental de Inovação da Defesa (*Defense Innovation Unit–Experimental — DIUx*), que busca criar e fortalecer relacionamentos com inventores novos e já conhecidos[6]. Com isso, o Secretário ressalta que muitas inovações militares podem e devem proceder de nossos parceiros na indústria.

Em vários aspectos, "inovação" tornou-se um termo vago, que descreve tudo que seja novo, de automóveis a colchões. A inovação é, simplesmente, qualquer coisa nova e útil que se implemente. Geoffrey A. Moore descreve a *inovação de aplicações* como a "criação de diferenciação por meio da identificação e exploração de uma nova aplicação ou emprego para uma tecnologia existente"[7]. Enquanto isso, Elaine Dundon fala da "implementação proveitosa de criatividade estratégica"[8]. No caso das Op Ciber, oferecemos a seguinte

definição de inovação: a implementação e integração de novos conceitos, processos e materiais que ampliem a capacidade da missão. As organizações podem aumentar a inovação por meio da colaboração, flexibilidade, criatividade e alocação de recursos.

Embora a inovação militar tenha sempre exercido um papel no avanço do combate, o comando institucional não raro teve dificuldades para incorporar e apoiar inovações táticas. Em muitos casos, isso resulta na busca de inovações fora da organização e

(Foto da Cap Meredith Mathis, Exército dos EUA)

Militar da 780ª Brigada de Inteligência Militar no Forte Meade, Estado de Maryland, prepara equipamento de interceptação de voz durante um exercício de integração cibernética na Base Conjunta de Lewis-McChord, no Estado de Washington, 21 Out 15.

Inovação no Ciberespaço

A natureza inconstante do ciberespaço apresenta uma série de novos desafios ao combatente. O fluxo constante de novas tecnologias, práticas e técnicas define os ambientes informacional e operacional. O tempo entre a aquisição e a obsolescência aumenta essa complexidade. As ameaças advêm de atores estatais, organizações e indivíduos terroristas e criminosos e hacktivistas extremamente capazes e providos de recursos. Os obstáculos relacionados ao custo vêm diminuindo cada vez mais para os adversários: uma invasão de hacker só precisa dar certo uma única vez; uma defesa capaz precisa funcionar 100% das vezes.

Diferentemente da guerra convencional, os EUA não têm um monopólio sobre os meios de conduzir Op Ciber. Isso requer que o segmento militar realmente avalie seus pontos fortes e vulnerabilidades quando se trata de ataque e defesa. O Exército precisa abordar o ambiente informacional com o reconhecimento de que soluções inovadoras podem ser tanto externas quanto internas. em sua adoção para o uso interno por meio de uma abordagem de cima para baixo. Dentro das Forças Armadas, os comandantes costumam favorecer mais as iniciativas de uns poucos "eleitos" nos escalões mais elevados — muitas vezes independentemente de sua especialização — do que as da população em geral. Contudo, o Departamento de Defesa precisa de inovações que sejam introduzidas por indivíduos — uma abordagem de baixo para cima — para manter a iniciativa em ambientes informacionais e operacionais dinâmicos.

Para influenciar as operações, o segmento cibernético precisa desafiar as normas militares e transformar-se em uma comunidade com os recursos, valores e comportamentos que promovam uma mentalidade inovadora e a capacidade de evoluir. Uma cultura de inovação enxerga como norma o novo pensamento e experimentação que abordam os desafios operacionais, processuais, técnicos e de outra natureza que influenciam as Op Ciber.

O Imperativo da Inovação

Enfrentar desafios cibernéticos respondendo ao imperativo da inovação requer que os comandantes adotem uma cultura que estimule e recompense práticas inovadoras. Sem o apoio do comando, as iniciativas de inovação fracassarão. O Gen Ex (Res) Stanley McChrystal relata, no livro *Team of Teams*, como se deu conta de que precisava de um estilo de liderança diferente para derrotar um inimigo extremamente adaptável. Em vez de atuar como um "mestre do xadrez" e direcionar resultados por meio de decisões vindas do topo, McChrystal assumiu o papel de "jardineiro", concentrando-se em moldar o ecossistema[9]. McChrystal descreve como configurou o ambiente cultural dando o exemplo e guiando, constantemente, a narrativa[10]. Da mesma forma que McChrystal, para moldar uma cultura que impulsione as Op Ciber adiante, é preciso que os comandantes valorizem a autonomia, a colaboração e a adaptabilidade.

As boas ideias não se restringem a um grau hierárquico ou posição em particular. O papel de "jardineiro" que McChrystal assumiu como estilo de liderança apoiou-se na confiança em todos os níveis de comando e espelhou diversos princípios do Comando de Missão ao reconhecer a importância de conferir poder de decisão a líderes ágeis e adaptáveis[11].

Como um jardineiro, os líderes podem criar as condições regando e capinando, mas não podem fazer a planta crescer. Devem inspirar a criatividade, a geração e compartilhamento de ideias e a iniciativa em seus subordinados, ao mesmo tempo que os incentivam a correr riscos com base em suas ideias[12]. Os líderes devem evitar obstáculos à criatividade apenas por medo de correr riscos baseados em ideias inovadoras dos outros. Não basta que proclamem que a força de trabalho deve compartilhar ideias e não temer o fracasso. Precisam certificar-se de que haja sistemas e recursos adequados para possibilitar o compartilhamento de ideias e conferir proteção contra alguns fracassos[13].

Um *site* de *crowdsourcing* [busca de soluções baseada no trabalho e conhecimentos coletivos — N. do T.], aliado à inovação baseada em desafios, oferece uma forma de possibilitar o compartilhamento de ideias. Os integrantes de um comando podem compartilhá-las e votar nas de sua preferência. O comando pode, então, selecionar e implementar aquelas que, a seu ver, devam melhorar as operações. Os comandantes devem ser participantes ativos. No Comando Cibernético do Exército dos EUA e Segundo Exército, o *crowdsourcing* é uma forma de mostrar que a inovação é coerente com a missão da organização. Os integrantes de uma equipe também podem apresentar suas sugestões diretamente ao comando, perante uma banca de investimento de recursos ao estilo do show norte-americano "Shark Tank" [no qual empresários de sucesso selecionam e investem nas melhores ideias— N. do T][14].

(Foto do Exército dos EUA)

Militar da 780ª Brigada de Inteligência Militar conduz operações de apoio cibernético com o uso improvisado de equipamentos comerciais durante exercício de adestramento da 2ª Brigada de Combate *Stryker*, 2ª Divisão de Infantaria, no Centro Nacional de Adestramento, Forte Irwin, Califórnia, 24 Jan 16.

Embora seja necessário tirar proveito da inovação interna, também existe a necessidade de se olhar fora da organização para desenvolver novas proficiências. É preciso aprender com a inovação dos outros. O setor cibernético deve continuar estabelecendo relacionamentos com o meio acadêmico e com a indústria para ampliar as oportunidades de inovação. Precisaremos dessas perspectivas externas e de atividades de parceria, à medida que continuarmos a enfrentar desafios imprevistos no ciberespaço. A função de combate "engajamento", proposta pelo Exército, reforça o fato de que os futuros desafios operacionais serão numerosos e

complexos demais para serem enfrentados pelas Forças Armadas e órgãos civis dos EUA isoladamente[15].

O governo e a indústria vêm reconhecendo a importância do Vale do Silício e da comunidade de *start-ups* em não atuarem sozinhos. Por exemplo, a nomeação, em março de 2016, do diretor executivo da empresa Google, Eric Schmidt, para presidir o Comitê Consultivo de Inovação da Defesa; do empresário de tecnologia Chris Lynch para presidir o Serviço Digital de Defesa do Pentágono; e o estabelecimento da DIUx absorvem o talento e os conhecimentos do Vale do Silício para servirem ao Departamento de Defesa[16]. O Comando Cibernético do Exército dos EUA e Segundo Exército lançaram o programa piloto Silicon Valley Innovation e participaram do programa *Hacking4Defense*, da Universidade Stanford[17]. O programa Connect and Develop, da empresa Proctor and Gamble, oferece um exemplo proveniente da indústria. Esse programa permite que a empresa colabore com organizações e indivíduos ao redor do mundo para buscar, sistematicamente, tecnologias, embalagens e produtos que ela possa aprimorar, aumentar em escala e comercializar por conta própria ou com outras empresas[18].

O caráter mutável do ciberespaço e a alta rotatividade de tecnologia e práticas requerem uma força cibernética flexível e adaptável. À medida que o Exército dos EUA lidar com os desafios operacionais atuais e futuros, o papel das Op Ciber aumentará em todos os níveis da guerra. O ciberespaço está se tornando indissociavelmente ligado à superioridade no domínio terrestre. Conforme evidenciado na Ucrânia, as aplicações táticas dos efeitos cibernéticos passarão a ser regra, com a integração de capacidades cibernéticas à manobra e ao Comando de Missão. Precisamos aprender com os conflitos em curso, que destacam os novos desafios das Op Ciber, Op Info e GE. É preciso, então, aplicar essas lições em nossas políticas e doutrina e em nossos centros de adestramento para o combate.

Muitos na indústria, junto com McChrystal, aprenderam que a inutilidade de planos estratégicos de cinco anos em ambientes dinâmicos aumenta com a incerteza. Para combater isso, buscam uma vantagem adaptativa. Unidades como a 780ª Brigada de Inteligência Militar e a Brigada de Proteção Cibernética do Exército dos EUA — em que equipes estão na vanguarda de nossas Op Ciber em curso — já estão obtendo avanços. Sua contínua integração em rodízios nos centros de adestramento para o combate permite que equipes cibernéticas efetuem mudanças enquanto conduzem experiências rapidamente, não apenas com equipamentos e serviços, mas também com modelos, processos e estratégias.

A fabricação da ferramenta "fuzil cibernético" demonstra que indivíduos com autonomia de decisão que trabalhem cooperativamente encontrarão soluções adaptáveis para problemas operacionais. Os comandantes precisam estabelecer uma rede de sistemas e processos que facilite a criatividade dessas inovações rápidas, pois elas levam à adaptação. Estar preparado para a adaptação é a maneira pela qual tiraremos proveito das características emergentes do ciberespaço. Equipes cibernéticas com autonomia de decisão são a solução para nos adaptarmos a esse desafio operacional.

Conclusão

A crescente interseção entre ambientes informacionais e operacionais requer que o Exército dos EUA repense como abordará a inovação para enfrentar seus desafios operacionais. Os paradigmas estão mudando. A futura superioridade no domínio terrestre depende, em grande medida, de nosso sucesso nas Op Ciber. Para assegurá-la, comandantes devem priorizar a inovação e criar as condições em que ela possa desenvolver-se. O Exército dos EUA deve reformular o modo pelo qual explora inovações externas, ao mesmo tempo que incentiva a promessa de seus inovadores internos. Deve efetuar essas mudanças para que permaneçamos relevantes e prontos para enfrentar nossos adversários tanto em terra quanto no ambiente cibernético. ■

O General de Divisão Edward C. Cardon, do Exército dos EUA, é o Comandante do Comando Cibernético do Exército dos EUA e Segundo Exército. É bacharel pela Academia Militar de West Point e mestre pelo National War College e pelo U.S. Naval Command and Staff College. Serviu, anteriormente, como Comandante da 2ª Divisão de Infantaria; Subcomandante do U.S. Army Command and General Staff College; e Subcomandante (logística) da 3ª Divisão de Infantaria.

O Coronel David P. McHenry, do Exército dos EUA, é o Oficial de Planejamento do Comando Cibernético do Exército dos EUA e Segundo Exército. Concluiu o bacharelado na University of Northern Colorado e dois mestrados na School of Advanced Military Studies, Forte Leavenworth, Estado do Kansas. Serviu no Pentágono e em missões no Iraque.

O Tenente-Coronel Christopher Cline, do Exército dos EUA, é estrategista do Exército junto ao Comando Cibernético do Exército dos EUA e Segundo Exército. É bacharel pela Academia Militar dos EUA, mestre em Filosofia pela U.S. Air Force Air University School of Advanced Air and Space Studies e mestre em Assuntos Internacionais pela Texas A&M University. Serviu, anteriormente, como Planejador Estratégico para o Oitavo Exército e Comandante Regional na Diretoria de Admissões da Academia Militar dos EUA, em West Point. ***O Tenente-Coronel Cline é o principal autor deste artigo.***

Referências

1. Brent Chapman, Matt Hutchinson e Erick Waage, "It Is Time for the U.S. Military to Innovate like Insurgents", *War on the Rocks* (blog), 18 October 2015, acesso em 17 mai. 2016, http://warontherocks.com/2015/10/it-is-time-for-the-u-s-military-to-innovate-like-insurgents/.

2. Ibid.

3. Sydney J. Freedberg Jr., "Russian Drone Threat: Army Seeks Ukraine Lessons", *site* Breaking Defense, 14 October 2015, acesso em 17 mai. 2016, http://breakingdefense.com/2015/10/russian-drone-threat-army-seeks-ukraine-lessons/.

4. Jose Pagliery, "Scary Questions in the Ukraine Energy Grid Attack", *site* CNN Money, 18 January 2016, acesso em 17 mai. 2016, http://money.cnn.com/2016/01/18/technology/ukraine-hack-russia/.

5. Secretary of Defense, memorandum from Chuck Hagel to principal officials of Department of Defense, et al., *The Defense Innovation Initiative*, 15 November 2014, acesso em 17 mai. 2016, http://www.defense.gov/Portals/1/Documents/pubs/OSD013411-14.pdf.

6. Maureen Schumann, "Defense Innovation Unit–Experimental (DIUx): Silicon Valley", fact sheet, n.d., acesso em 17 mai. 2016, http://www.defenseinnovationmarketplace.mil/resources/2015828_DIUxFactSheet.pdf.

7. Geoffrey A. Moore, "Darwin's Dictionary", *site* Dealing with Darwin, acesso em 17 mai. 2016, http://www.dealingwithdarwin.com/theBook/darwinDictionary.php#Innovationtypes.

8. Elaine Dundon, *The Seeds of Innovation: Cultivating the Synergy That Fosters New Ideas* (New York: AMACOM, 2002), p. 6–7.

9. Stanley McChrystal, Tantum Collins, David Silverman e Chris Fussell, *Team of Teams: New Rules of Engagement for a Complex World* (New York: Portfolio, 2015), p. 226.

10. Ibid.

11. Army Doctrine Publication 6-0, *Mission Command* (Washington, DC: U.S. Government Printing Office, 17 May 2012), p. iv.

12. Roger Schwarz, "What the Research Tells Us about Team Creativity and Innovation", *site* Harvard Business Review, 15 December 2015, acesso em 17 mai. 2016, https://hbr.org/2015/12/what-the-research-tells-us-about-team-creativity-and-innovation.

13. James R. Detert e Ethan R. Burris, "Can Your Employees Really Speak Freely?", *Harvard Business Review* (January-February 2016), acesso em 17 mai. 2016, https://hbr.org/2016/01/can-your-employees-really-speak-freely.

14. "Shark Tank", *site* ABC, acesso em 17 mai. 2016, http://abc.go.com/shows/shark-tank. No show de televisão "Shark Tank", indivíduos de todo tipo de profissão apresentam ideias comerciais perante uma banca de "magnatas multimilionários e bilionários exigentes e que venceram na vida por seu próprio esforço", com o objetivo de obter seu investimento.

15. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-8-5, *The U.S. Army Functional Concept for Engagement* (Fort Eustis, VA: TRADOC, 24 February 2014), p. 10.

16. Davey Alba, "Pentagon Taps Eric Schmidt to Make Itself More Google-ish", site Wired, 2 March 2016, acesso em 17 mai. 2016, http://www.wired.com/2016/03/ex-google-ceo-eric-schmidt-head-pentagon-innovation-board/.

17. Kevin McCaney, "Army, Silicon Valley to Tackle Social Media Challenge", *site* Defense Systems, 10 March 2016, acesso em 17 mai. 2016, https://defensesystems.com/articles/2016/03/10/army-silicon-valley-social-media-challenge.aspx.

18. Larry Huston e Nabil Sakkab, "Connect and Develop: Inside Proctor & Gamble's New Model for Innovation", *Harvard Business Review* (March 2006), acesso em 17 mai. 2016, https://hbr.org/2006/03/connect-and-develop-inside-procter-gambles-new-model-for-innovation.