(Foto de Cap Meredith Mathis, Exército dos EUA)

Militares da 201ª Brigada de Inteligência Militar Expedicionária e da 2ª/2ª Brigada de Combate *Stryker* proveem segurança a integrante da 780ª Brigada de Inteligência Militar, que instala uma antena de painel de conexão durante um exercício de adestramento cibernético em 20 Out 15, na Base Conjunta de Lewis-McChord, no Estado de Washington.

*Nunca me culpo quando não estou rebatendo. Só culpo o taco e, se continua assim, troco por outro*[1].

—Yogi Berra

Ao desenvolver capacidades, o Exército dos Estados Unidos da América (EUA) poderia usar um pouco da sabedoria paradoxal de Yogi Berra, lenda do beisebol norte-americano, que vai ao âmago de praticamente qualquer questão. Poderia perguntar-se, por exemplo: "Se os comandantes táticos do Exército são tão dependentes do ciberespaço, por que, então, não têm nenhum modo para visualizá-lo?" Todas as capacidades cibernéticas do Exército dos EUA operam em algum tipo de rede; contudo, praticamente não existe uma maneira de fornecer um entendimento situacional em tempo real do domínio cibernético às unidades de combate táticas[2]. Isso deixa os comandantes táticos cegos para possíveis ameaças e oportunidades cibernéticas, diminui sua capacidade para defender suas próprias redes e põe em risco formas tradicionais do poder de combate.

# Entendimento Situacional Cibernético para os Comandantes Táticos do Exército

## Feito é Melhor que Perfeito

Ten Cel (Res) William Jay Martin,
Força Aérea dos EUA, e
Emily Kaemmer

O Exército dos EUA está plenamente consciente dessa situação e considera o entendimento situacional cibernético [as referências 2 e 3 adiante contêm uma explicação sobre o emprego de *understanding* (entendimento) e *awareness* (consciência) — N. do T] como uma prioridade máxima, mas a criação de uma solução tecnológica que proporcione um sistema com essa finalidade às unidades de combate convencionais parece estar a anos de distância[3]. Atualmente, o Exército dos EUA está, simplesmente, esforçando-se para definir exatamente *o que* os comandantes táticos precisam saber sobre o ciberespaço. Ademais, mesmo depois que ele identifique o que, a seu ver, deve ser o entendimento situacional cibernético, precisará sobreviver à "realpolitik" do processo de aquisições. Até mesmo as melhores propostas de capacidades podem acabar sendo diluídas, distorcidas ou combinadas com outros programas, com resultados aquém do ideal. Além disso, ao tentarem criar uma solução que resolva tudo, os desenvolvedores de capacidades não raro tornam os requisitos tão rigorosos e complexos que todo o esforço fica paralisado. Todos esses cenários podem levar a prazos prolongados

ou soluções limitadas ou até obsoletas antes mesmo de alcançarem a capacidade operacional inicial. Este artigo detalha por que a busca de entendimento situacional cibernético pelo Exército dos EUA está estagnada e recomenda uma abordagem simplificada para corrigir esse problema.

## Uma Necessidade Justificada para o Entendimento Situacional Cibernético

*Quero agradecer-lhes por tornarem este dia necessário.*[4]

—Yogi Berra

Qualquer debate sobre uma melhor abordagem para adquirir um sistema de entendimento situacional cibernético precisa começar com a demonstração de sua necessidade, e há muitas evidências nesse sentido. O documento *Joint Concept for Cyberspace* ("Conceito Conjunto para o Ciberespaço", em tradução livre), do Departamento de Defesa dos EUA, afirma que a consciência situacional compartilhada do ciberespaço é um de oito elementos principais para as operações cibernéticas conjuntas[5]. Esse conceito deu origem a *Joint Cyber Situational Awareness Initial Capabilities Document* ("Documento de Capacidades Iniciais de Consciência Situacional Cibernética Conjunta", em tradução livre), que descreve as necessidades relacionadas à consciência situacional do ciberespaço nos escalões estratégicos[6]. Coincidentemente, muitas das mesmas informações que se aplicam aos escalões estratégicos conjuntos também são relevantes para os escalões táticos do Exército, nos quais a necessidade do entendimento situacional cibernético é mais urgente, segundo a Força[7].

O documento *U.S. Army Capstone Concept* ("Conceito Fundamental do Exército dos EUA", em tradução livre) afirma que, para manter a vantagem no ciberespaço, o Exército do futuro precisará conceder aos comandantes e subordinados uma capacidade que os ajude a entender como e quando os adversários empregarão capacidades cibernéticas e como responder[8]. Também recomenda investimentos em capacidades e sistemas de Comando de Missão que permitam que o Exército dos EUA interconecte a Força e melhore o entendimento situacional comum, a fim de adquirir e manter a vantagem em atividades eletromagnéticas cibernéticas[9]. O documento *U.S. Army Operating Concept* ("Conceito Operativo do Exército dos EUA", em tradução livre) identifica as principais áreas de desenvolvimento de capacidades focalizadas em iniciativas de ciência e tecnologia, com o objetivo de proporcionar maior entendimento situacional aos comandantes por meio de cenários operativos comuns até o nível tático. Afirma que isso "pode ajudar os comandantes a adquirir e manter uma posição de relativa vantagem por todo o conflituoso domínio cibernético e espectro eletromagnético"[10].

As publicações doutrinárias conjuntas e do Exército dos EUA também apontam para a necessidade do entendimento situacional cibernético. A Publicação Conjunta 3-12 (R), *Operações Cibernéticas* (JP 3-12 (R), *Cyberspace Operations*), afirma, expressamente, que as operações cibernéticas dependem do "conhecimento atual e preditivo do ciberespaço e do ambiente operacional"[11]. A Publicação de Referência Doutrinária 6-0, *Comando de Missão* (ADRP 6-0, *Mission Command*), do Exército dos EUA, ressalta a importância do cenário operativo comum na geração do entendimento situacional[12]. O Manual de Campanha 6-02, *Apoio de Comunicações às Operações* (FM 6-02, *Signal Support to Operations*), afirma: "ao integrarem informações provenientes de toda a extensão da área de operações, as forças do Exército conseguem manter um entendimento situacional mais relevante e completo [...] [permitindo] que os comandantes empreguem as capacidades certas, no local e momento certos"[13]. Como seria de se esperar, esses documentos doutrinários refletem a mensagem estratégica de comandantes cibernéticos dos escalões mais elevados.

Em seu artigo para a revista *Joint Force Quarterly*, "Ten Propositions Regarding Cyberspace Operations" ("Dez Proposições sobre as Operações Cibernéticas", em tradução livre), o Gen Bda Brett Williams explica a urgência da consciência situacional cibernética. Afirma: "Desenvolver a consciência situacional cibernética é uma alta prioridade para o Departamento de Defesa. O desafio é fornecer um cenário completo do domínio que seja coerente, correto, atual e adaptável para comandantes em todos os escalões"[14]. Williams conclui, ainda, que os comandantes precisam estar aptos a visualizar e entender o ciberespaço para defendê-lo[15]. Essa simples verdade justifica a necessidade de uma capacidade de entendimento situacional cibernético para o Exército

(Foto de David Vergun, Exército dos EUA)

Combatentes cibernéticos defendem a rede no centro de operações táticas para a 2ª/1ª Brigada de Combate Blindada durante a Avaliação de Integração de Rede 16.1, realizada entre 25 Set 15 e 08 Out 15, no Forte Bliss, Texas.

dos EUA. Contudo, os esforços de desenvolvimento de capacidades do Exército com respeito ao entendimento situacional cibernético estão estagnados atualmente.

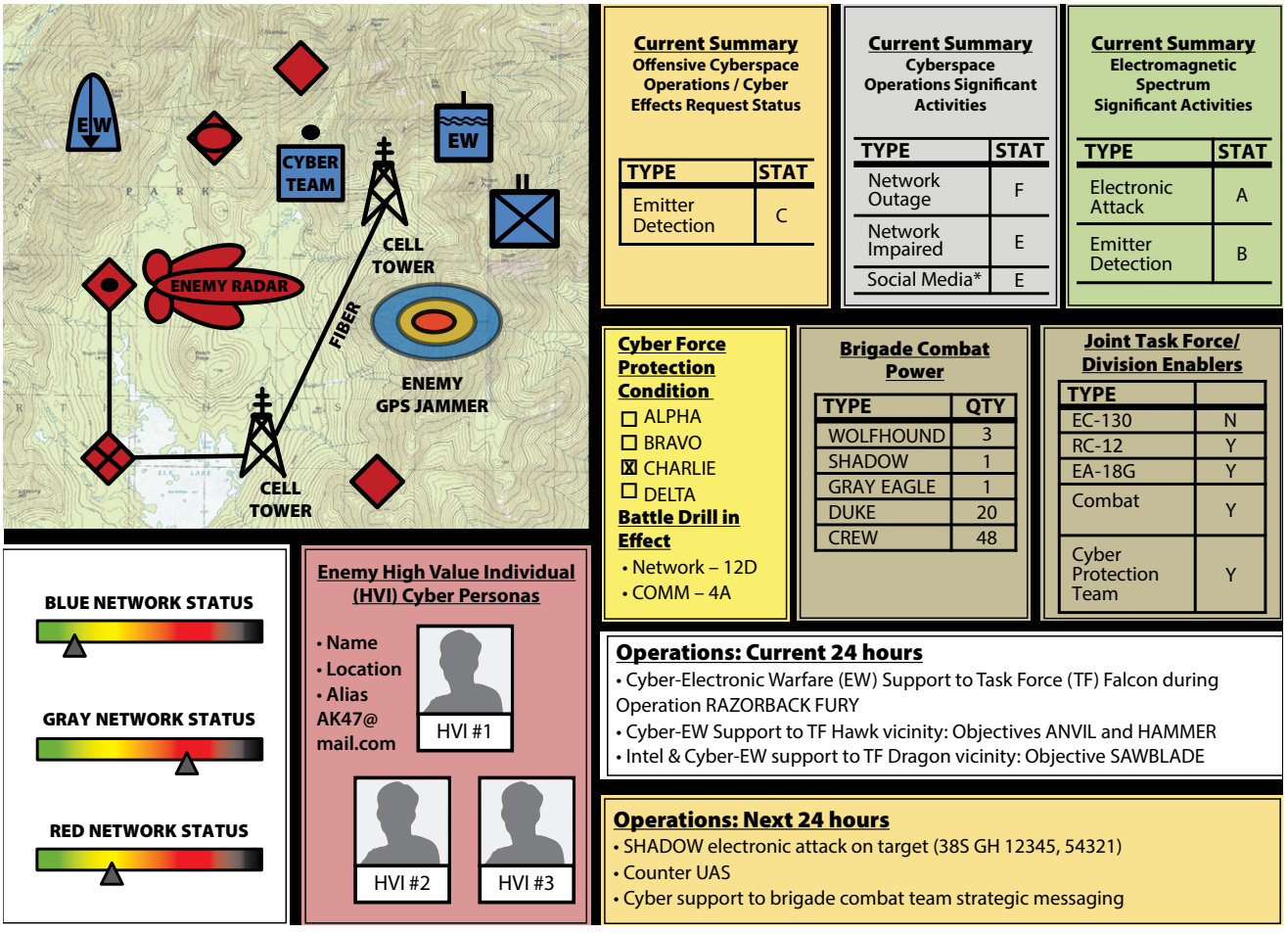
## Por Que os Esforços de Desenvolvimento da Capacidade de Entendimento Situacional Cibernético do Exército Estão Estagnados

*Se não souber para onde vai, pode acabar em um outro lugar*[16].

—Yogi Berra

Em um mundo perfeito, o Exército poderia antever suas necessidades relacionadas a capacidades com antecedência suficiente para permitir que o tradicional processo de aquisições funcionasse. Infelizmente, a inovação no ciberespaço avança rápido demais para que cronogramas tradicionais sejam praticáveis no caso do entendimento situacional cibernético. O prazo típico para identificar uma necessidade, redigir os requisitos, negociar o processo do Sistema de Integração e Desenvolvimento de Capacidades Conjuntas (*Joint Capabilities Integration and Development System — JCIDS*) e, então, produzir um novo dispositivo é de cinco a oito anos. O processo do JCIDS busca suprir o desenvolvimento de *software* de sistemas de informação com uma opção mais eficiente, o modelo *Information Techology (IT) Box* [modelo mais flexível e ágil, com maior delegação dentro de valores predefinidos — N. do T.][17]. Embora esteja utilizando o modelo IT-Box, o Exército dos EUA tem demorado para aprovar o primeiro documento de requisitos relacionados ao ciberespaço[18]. Um de seus desafios talvez consista em um sistema de aquisições preso a velhos paradigmas.

O Gen Ex David G. Perkins, do Comando de Instrução e Doutrina, indicou que o sistema de aquisições de defesa continua voltado a preencher lacunas que nos diferenciem de um inimigo conhecido, em vez de acelerar nossa marcha de inovação[19]. Perkins




(Imagem dos autores)

**Figura – Modelo de Calco de Entendimento Situacional Cibernético no Cenário Operativo Comum**

afirmou que o Exército dos EUA precisa estar disposto a encerrar programas antigos e direcionar tais recursos para tecnologias novas e mais facilmente transferíveis[20]. Acrescentou que, a fim de inovar, o Exército dos EUA deve evitar a criação de requisitos específicos demais, para não se tornarem excessivamente restritivos[21].

Claramente, o Exército anseia por inovar, mas um sistema de aquisições desatualizado e um modo de pensar antiquado não são as únicas coisas a retardar seu avanço. Um outro desafio consiste em esforços contraditórios de desenvolvimento de capacidades cibernéticas. Atualmente, há diferentes documentos preliminares de capacidade de sistemas de informação que abordam uma mesma área[22]. Todos prometem capacidades relevantes para o entendimento situacional cibernético. Embora o Centro de Integração de Capacidades do Exército (*Army Capabilities Integration Center — ARCIC*) tenha tentado coordenar esses diferentes esforços, até agora não foi obtida nenhuma grande economia.

O subsecretário de Aquisição, Logística e Tecnologia do Exército dos EUA criou, recentemente, uma abordagem coordenada para produzir tecnologias relacionadas ao ciberespaço[23]. Contudo, parece estar mais voltada ao ataque e defesa cibernéticos, e não a capacidades facilitadoras como o entendimento situacional cibernético[24]. Embora um dos objetivos do subsecretário seja criar uma capacidade de operações de rede integradas que aumente o entendimento sobre a saúde de redes táticas, essa capacidade parece excluir outras informações, ligadas a fatores externos às redes amigas, que possam interessar aos comandantes táticos[25]. Além disso, embora o subsecretário tenha, em 2014, respondido a dez enunciados de necessidades operacionais do Comando Cibernético

do Exército dos EUA com respeito a requisitos de curto prazo, o foco principal tem sido em reduzir as vulnerabilidades das redes e não no entendimento situacional cibernético[26]. Essa estratégia de cima para baixo é um passo positivo, que ainda não se converteu, porém, em um esforço coordenado de desenvolvimento de capacidades cibernéticas nos níveis mais baixos da burocracia.

## Uma Abordagem Simples para os Desenvolvedores de Capacidades de Entendimento Situacional Cibernético do Exército dos EUA

*Dá para observar um bocado só de assistir*[27].

—Yogi Berra

O Exército dos EUA não precisa de um sistema de entendimento situacional cibernético perfeito para daqui a dez anos, e sim de um sistema bom o suficiente *já*. Para tanto, recomenda-se que os desenvolvedores de capacidades adotem uma abordagem simples, respondendo a três perguntas básicas:

- De que informações os comandantes precisam?
- Como obtê-las e reuni-las?
- Como devem ser apresentadas?

Em um sentido mais amplo, para adquirir o entendimento situacional cibernético (ou qualquer outra futura capacidade), o Exército dos EUA deve pensar em formas de inovar e reformular, gradualmente, um processo de aquisições restritivo. Primeiro, os desenvolvedores de capacidades do Exército dos EUA devem determinar quais informações sobre o ciberespaço são as mais importantes para os comandantes.

Durante operações de combate, os comandantes, apoiados por seus estados-maiores, monitoram e avaliam o avanço, tomam decisões para explorar oportunidades e combater ameaças e direcionam o emprego do poder de combate em momentos decisivos[28]. O ciberespaço é uma parte significativa desse cálculo, especialmente em relação a seus efeitos sobre o Comando de Missão e formas extremamente interconectadas do poder de combate. As informações que provavelmente consistirão no conteúdo básico do calco de entendimento situacional cibernético para o cenário operativo comum incluem o *status* de redes amigas, da nação anfitriã e inimigas; ameaças cibernéticas e capacidades inimigas; principais infraestruturas cibernéticas na área de operações; autoridades e regras de engajamento cibernéticas; e tendências das mídias sociais, entre outras.

Segundo, os desenvolvedores de capacidades precisam considerar de onde vêm as informações para o entendimento situacional cibernético e como obtê-las. Atualmente, apenas forças conjuntas de missão cibernética estão autorizadas a conduzir a Inteligência, Vigilância e Reconhecimento cibernéticos e a preparação operacional cibernética do ambiente. Assim, uma grande quantidade de informações sobre o ciberespaço se originará e residirá em bancos de dados dos âmbitos nacional e estratégico. Não obstante, dados e informações relevantes oriundos dos esforços orgânicos de busca de informações nos escalões táticos do Exército podem fornecer um contexto importante.

Um exemplo prático é conectar uma persona cibernética, obtida de um meio cibernético nacional ou conjunto, com a identidade de uma pessoa (ou organização) real que, sabidamente, esteja presente no ambiente operacional de uma unidade, conforme deduzido por meio da busca de informações locais. A combinação dessas fontes fornece maior entendimento situacional ao comandante tático e ajudará o comando superior a enxergar o ciberespaço mais claramente.

Terceiro, os desenvolvedores de capacidades precisam determinar a melhor forma de apresentar as informações. O entendimento situacional cibernético precisa fornecer uma quantidade adequada, mas não excessiva, de detalhes. O Exército não pode defender todo o ciberespaço, tampouco exibi-lo por completo em um cenário operativo comum; caso contrário, o raciocínio de um comandante pode acabar sendo obstruído por um emaranhado de informações desnecessárias. Os comandantes só precisam saber o que afeta sua missão, o que, à parte de explorar alguns efeitos cibernéticos conjuntos, consiste, primordialmente, em empregar formas tradicionais do poder de combate. Assim, o entendimento situacional cibernético também precisa possibilitar que as informações sejam apresentadas de forma contextualizada a fim de facilitar o entendimento situacional mais amplo. Isso pode ser obtido por meio de imagens, gráficos de semáforo e mostrador, setas, diagramas de linhas e de blocos e comparações lado a lado (conforme ilustra a figura).

Quarto, os desenvolvedores de capacidades devem evitar redigir especificações de requisitos para o sistema que

busquem substituir o discernimento e tomada de decisões humanos. O entendimento situacional cibernético deve proporcionar entendimento, mas cabe aos comandantes e estados-maiores táticos discernir como agir a partir dele.

Quinto, e último, o Exército dos EUA precisa pensar em formas de inovar e reformular, gradualmente, um processo de aquisições restritivo. Os documentos de requisitos cibernéticos do Exército devem buscar incentivar a inovação descrevendo um modelo abrangente, apoiado em sólidos conceitos doutrinários, que possa ser desenvolvido com o tempo por meio de sucessivas compilações de software[29]. Esse é, na verdade, o objetivo do modelo IT-Box. O desafio é, portanto, identificar os aspectos do entendimento situacional cibernético que logo ficarão obsoletos e torná-los modulares, para que possam ser rapidamente substituídos pelas últimas inovações. Além disso, os desenvolvedores de capacidades do Exército precisam decidir se o entendimento situacional cibernético será conjugado com outros sistemas, existentes ou propostos, ou se permanecerá puro. Combinar vários sistemas aumenta o risco de que eles fiquem presos durante anos na fase de desenvolvimento. Enquanto isso, o Exército não estará mais próximo de obter uma capacidade de entendimento situacional cibernético do que em 2013, quando a Análise Baseada em Capacidades (*Capabilities Based Assessment*) das Operações Cibernéticas do Exército indicou que sua principal deficiência estava no entendimento situacional dos comandantes[30].

## Conclusão

*Os outros times podem nos causar problemas se vencerem*[31].

—Yogi Berra

Ainda que vários recursos ajudem, atualmente, a fornecer o entendimento situacional cibernético, o Exército dos EUA não conta com um esforço bem coordenado de desenvolvimento de capacidades para definir e reunir os requisitos relacionados a essa área. Embora ofereça alternativas de desenvolvimento de capacidades com prazos menores, o processo do JCIDS continua sendo inadequado, ao que parece, conforme evidenciado pela incapacidade do Exército dos EUA em alcançar a aprovação de documentos do JCIDS relacionados ao entendimento situacional cibernético ou a qualquer outra capacidade cibernética[32]. Qualquer que seja o caso, os comandantes não podem continuar a abrir mão de importantes decisões operacionais sobre seu ambiente operacional por não contarem com o entendimento situacional do domínio.

O entendimento situacional cibernético pode acabar não consistindo em uma ferramenta ou sistema independente. Ao contrário, a solução pode ser uma combinação de várias capacidades facilitadoras do entendimento situacional. Portanto, o Exército dos EUA talvez ganhe mais com um sistema improvisado que lhe conceda *algum* entendimento situacional cibernético hoje que com um sistema que resolva tudo e prometa o mundo amanhã.

Muitos dos inimigos dos EUA não enfrentam uma burocracia e um problema de compartimentação de informações que prejudiquem sua capacidade para empregar novas tecnologias em combate. Assim, enquanto os desenvolvedores de capacidades do Exército dos EUA estiverem definindo necessidades, analisando alternativas e executando o processo de documentação e aprovação do JCIDS, os adversários potenciais vencerão a concorrência cibernética utilizando tecnologias comerciais amplamente disponíveis. Para conseguir virar a situação, o Exército dos EUA precisa de uma jogada revolucionária; porque, convenhamos: "O futuro já não é mais como era antes"[33]. ■

*O Tenente-Coronel William Jay Martin, da reserva remunerada da Força Aérea dos EUA, é analista militar sênior da empresa Command Decision Systems & Solutions, Inc. Concluiu o bacharelado na University of Delaware e o mestrado na Louisiana Tech University. Formou-se pela U.S. Air Force Weapons School, Air Force Air Command and Staff College e Joint Forces Staff College.*

*Emily Kaemmer é analista militar sênior da empresa Command Decision Systems & Solutions, Inc., sendo especializada no desenvolvimento de capacidades cibernéticas do Exército dos EUA.*

## Referências


1. Yogi Berra, *The Yogi Book: I Really Didn't Say Everything I Said!* (New York: Workman Publishing Company, 1998).

2. Army Doctrine Publication 5-0, *The Operations Process* (Washington, DC: U.S. Government Printing Office [GPO], May 2012). O entendimento situacional é o resultado da aplicação da análise e critério a informações relevantes para determinar a relação entre as variáveis operacionais e da missão para facilitar a tomada de decisão. Para os fins deste artigo, equivale à consciência situacional, que não é definida na doutrina conjunta ou do Exército.

3. O termo entendimento situacional cibernético (*cyber SU*) se refere a uma capacidade teórica que fornece dados e informações relevantes sobre o ciberespaço a serem exibidas em um cenário operativo comum ou painel do comandante. O "cyber SU", ou entendimento situacional cibernético (a capacidade), distingue-se da expressão "cyber situational awareness" (consciência situacional cibernética) que, segundo a Publicação Conjunta 3-12(R), *Operações Cibernéticas* (JP 3-12(R)*, Cyberspace Operations*) (Washington, DC: U.S. GPO, February 2013), refere-se ao necessário conhecimento atual e preditivo do ciberespaço e do ambiente operacional do qual as operações cibernéticas dependem, incluindo todos os fatores que afetem as forças cibernéticas amigas e adversárias.

4. Yogi Berra, *The Yogi Book*. Citado no dia de homenagem a Yogi Berra, Saint Louis, Missouri, em 1947.

5. Department of Defense, *The Joint Concept for Cyberspace* (JCC) (August 2012), p. 9 (FOUO).

6. Joint Cyber Situational Awareness (Cyber SA) Initial Capabilities Document (ICD), 23 April 2012, approved by the Joint Chiefs of Staff Requirements Oversight Council (JROC). Disponível em JROC Knowledge Management and Decision Support (KM/DS) System.

7. Esta afirmação representa a opinião dos autores após compararem Joint Cyber SA ICD com Army Cyber Command (ARCYBER)/2nd Army Support Element, *Army Cyberspace Operations Capabilities Based Assessment* (CBA) Final Report (U.S. Army Training and Doctrine Command [TRADOC], 15 December 2013), p. 34. Veja a fig. 9, "Functional Needs Analysis Gap Prioritization", e solicite documentos ao ARCYBER.

8. TRADOC Pamphlet (TP) 525-3-0, *The U.S. Army Capstone Concept* (Fort Eustis, VA: TRADOC, 2012), p. 28.

9. Ibid., p. 33.

10. TP 525-3-1, The U.S. Army Operating Concept: Win in a Complex World 2020-2040 (Fort Eustis, VA: TRADOC, 2014).

11. JP 3-12(R), *Cyberspace Operations* (Washington, DC: U.S. GPO, February 2013).

12. Army Doctrine Reference Publication 6-0, *Mission Command* (Washington, DC: U.S. GPO, May 2012).

13. Field Manual (FM) 6-02, *Signal Support to Operations* (Washington, DC: U.S. GPO, January 2014).

14. Brett T. Williams, "Ten Propositions Regarding Cyberspace Operations", *Joint Force Quarterly* 61 (2nd Quarter, 2011): p. 15. O Gen Bda (Res) Williams é o ex-subchefe de Operações Globais (J3) do Comando Cibernético dos EUA.

15. Ibid.

16. Yogi Berra e Dave Kaplan, *When You Come to a Fork in the Road, Take It!: Inspiration and Wisdom From One of Baseball's Greatest Heroes* (New York: Hyperion Books, 2001).

17. Joint Requirements Oversight Council, *Manual for the Operation of the Joint Capabilities Integration and Development System* (JCIDS Manual) (12 February 2015).

18. Uma pesquisa no Capabilities and Army Requirement Oversight Council Management System revelou que, até aquela data, nenhum documento relacionado ao ciberespaço havia sido aprovado pelo Exército; enquanto isso, a Força Aérea e a Marinha receberam aprovação para vários documentos.

19. David G. Perkins, "'Win in a Complex World'-But How?" *Army AL&T Magazine* (January–March 2015).

20. Ibid.

21. Ibid.

22. JCIDS Manual. Os documentos *Information System Capability Development Documents* (CDDs) possibilitam que os responsáveis descrevam os valores mínimos iniciais para os principais parâmetros de desempenho, principais atributos do sistema e atributos de desempenho adicionais. Os responsáveis por sistemas de *software*, que se beneficiam de contínuas inclusões de tecnologia, podem aprovar documentos subsequentes internamente em vez de apresentá-los ao *Joint Requirements Oversight Council* (Conselho Conjunto de Supervisão de Requisitos).

23. Matthew Maier e Jerry Cook, "Hacking Cyber Stovepipes", *Army AL&T Magazine* (January–March 2015).

24. As três subchefias do programa (program executive offices — PEO) que exercem as principais funções em apoio às futuras tecnologicas cibernéticas são (1) Command, Control, and Communications - Tactical (PEO C3T); (2) Enterprise Information Systems (PEO EIS); e (3) Intel, Electronic Warfare and Sensors (PEO IEW&S). O PEO C3T é o encarregado pela defesa da rede tática, o PEO EIS é o encarregado pela defesa da rede institucional e o PEO IEW&S é o responsável por esforços cibernéticos ofensivos.

25. Maier e Cook, "Hacking Cyber Stovepipes".

26. Ibid.

27. Yogi Berra e Dave H. Kaplan, *You Can Observe a Lot by Watching: What I've Learned About Teamwork From the Yankees and Life* (Hoboken, NJ: John Wiley & Sons, 2008).

28. FM 6-0, *Command and Staff Organization and Operations* (Washington, DC: U.S. GPO, May 2014).

29. Department of Defense, Instruction 5000.02, *Operation of the Defense Acquisition System*, 7 January 2015, acesso em 26 abr. 2016, http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf. Normalmente, são necessárias várias compilações e implantações de software para atender aos requisitos aprovados para um aumento de capacidade.

30. ARCYBER/2nd Army Support Element, *Army Cyberspace Operations*.

31. Michael J. Pellowski, *The Little Giant Book of Baseball Facts* (New York: Sterling Publishing Company, 2007).

32. Uma pesquisa no Capabilities and Army Requirement Oversight Council Management System revelou que, até aquela data, nenhum documento relacionado ao ciberespaço havia sido aprovado pelo Exército; enquanto isso, a Força Aérea e a Marinha receberam aprovação para vários documentos.

33. Essa citação foi atribuída incorretamente a Yogi Berra, que alega nunca tê-la dito. Contudo, há fontes conflitantes. Veja Berra e Kaplan, *When You Come to a Fork in the Road, Take It*.