(Photo by Capt. Meredith Mathis, U.S. Army)

Spc. Casey Payne (left), 201st Expeditionary Military Intelligence Brigade, and Sgt. Andrew Lee, Company D, 14th Brigade Engineer Battalion, 2-2 ID (SBCT), pull security for a soldier from the 780th Military Intelligence Brigade as he sets up a patch panel antenna during a cyber training exercise 20 October 2015 on Joint Base Lewis-McChord, Washington.

I never blame myself when I'm not hitting. I just blame the bat, and if it keeps up, I change bats.[1]

—Yogi Berra

When developing capabilities, the Army could use a little of Yogi Berra's paradoxical wisdom that quickly gets to the heart of almost any matter. Like asking, "If Army tactical commanders are utterly dependent on cyberspace, then why do they have no way of seeing it?" All U.S. Army cyber capabilities ride on some kind of network, yet there is almost no means to provide real-time situational understanding of the cyberspace domain for tactical combat units.[2] This leaves tactical commanders blind to potential cyberspace threats and opportunities, lessens their ability to defend their own networks, and places traditional forms of combat power at risk.

The Army is keenly aware of this predicament and considers cyberspace situational understanding (cyber SU) a top priority, but a technological solution to bring a cyber SU system to conventional combat units seems years away.[3] At present, the Army is simply struggling to define precisely *what* tactical

Cyberspace Situational Understanding for Tactical Army Commanders

The Army Is Swinging for the Fence, but It Just Needs a Single

Lt. Col. William Jay Martin, U.S. Air Force, Retired
Emily Kaemmer

commanders need to know about cyberspace. What's more, even after the Army figures out what it wants cyber SU to be, it must survive the realpolitik of the acquisition process. Even the best capability proposals can become watered down, distorted, or combined with other programs, resulting in less than ideal outcomes. Moreover, it is not uncommon for capability developers, in an attempt to create a solution that does it all, to make requirements so stringent and complex that the entire effort becomes paralyzed. All of these scenarios can lead to protracted timelines or solutions that are marginal or even obsolete before reaching initial operational capability. This article details why the Army's pursuit of cyber SU is stagnant and recommends a simplified approach toward fixing it.

A Justified Need for Cyber SU

I want to thank you for making this day necessary.[4]

—Yogi Berra

Any discussion of a better approach toward acquiring a cyber SU system must first begin with proof that such a system is needed, and there is plenty of evidence to support that it is. The Department of

Defense's (DOD) *Joint Concept for Cyberspace* states that shared situational awareness of cyberspace is one of eight key elements to joint cyberspace operations.[5] This concept gave birth to the Joint Cyber Situational Awareness Initial Capabilities Document, which describes requirements for situational awareness of cyberspace at strategic echelons.[6] Coincidentally, much of the same information applicable at joint strategic echelons is also relevant at Army tactical echelons, where the Army has asserted that its need for cyber SU is most urgent.[7]

The *U.S. Army Capstone Concept* asserts that in order to maintain an advantage in cyberspace, the future Army must provide a capability for leaders and soldiers that helps them to understand how and when adversaries employ cyberspace capabilities, and how to respond.[8] It also recommends investments in mission command capabilities and systems that allow the Army to network the force and improve common situational understanding in order to gain and maintain a cyber electromagnetic activities advantage.[9] The *U.S. Army Operating Concept* identifies key capability development areas focused on science and technology initiatives to provide increased commanders' situational understanding through common operational pictures down to the tactical edge. This, it states, "may help commanders gain and maintain a position of relative advantage across the contested cyberspace domain and electromagnetic spectrum."[10]

Joint and Army doctrine publications also point toward the need for cyber SU. JP 3-12(R), *Cyberspace Operations*, explicitly states that cyberspace operations depend upon "current and predictive knowledge of cyberspace and the operational environment (OE)."[11] ADRP 6-0, *Mission Command*, stresses the importance of the common operating picture (COP) in building situational understanding.[12] FM 6-02, *Signal Support to Operations*, says "by integrating information from across the breadth of the area of operations, Army forces are able to maintain more relevant and complete situational understanding … [allowing] commanders to employ the right capabilities, in the right place, and at the right time."[13] Not surprisingly, these doctrine documents reflect the strategic message of senior cyber leaders.

In his *Joint Force Quarterly* article, "Ten Propositions Regarding Cyberspace Operations," Maj. Gen. Brett Williams explains the urgency of cyberspace situational awareness. Williams writes, "Developing cyber situational awareness is a high priority for DOD. The challenge is providing a complete picture of the domain that is consistent, accurate, current, and customizable for commanders at all levels."[14] Williams also concludes that commanders must be able to see and understand cyberspace in order to defend it.[15] This simple truth justifies a cyber SU capability for the Army. However, Army capability development efforts for cyber SU are presently stagnant.

Why Army Cyber SU Capability Development Efforts are Stagnant

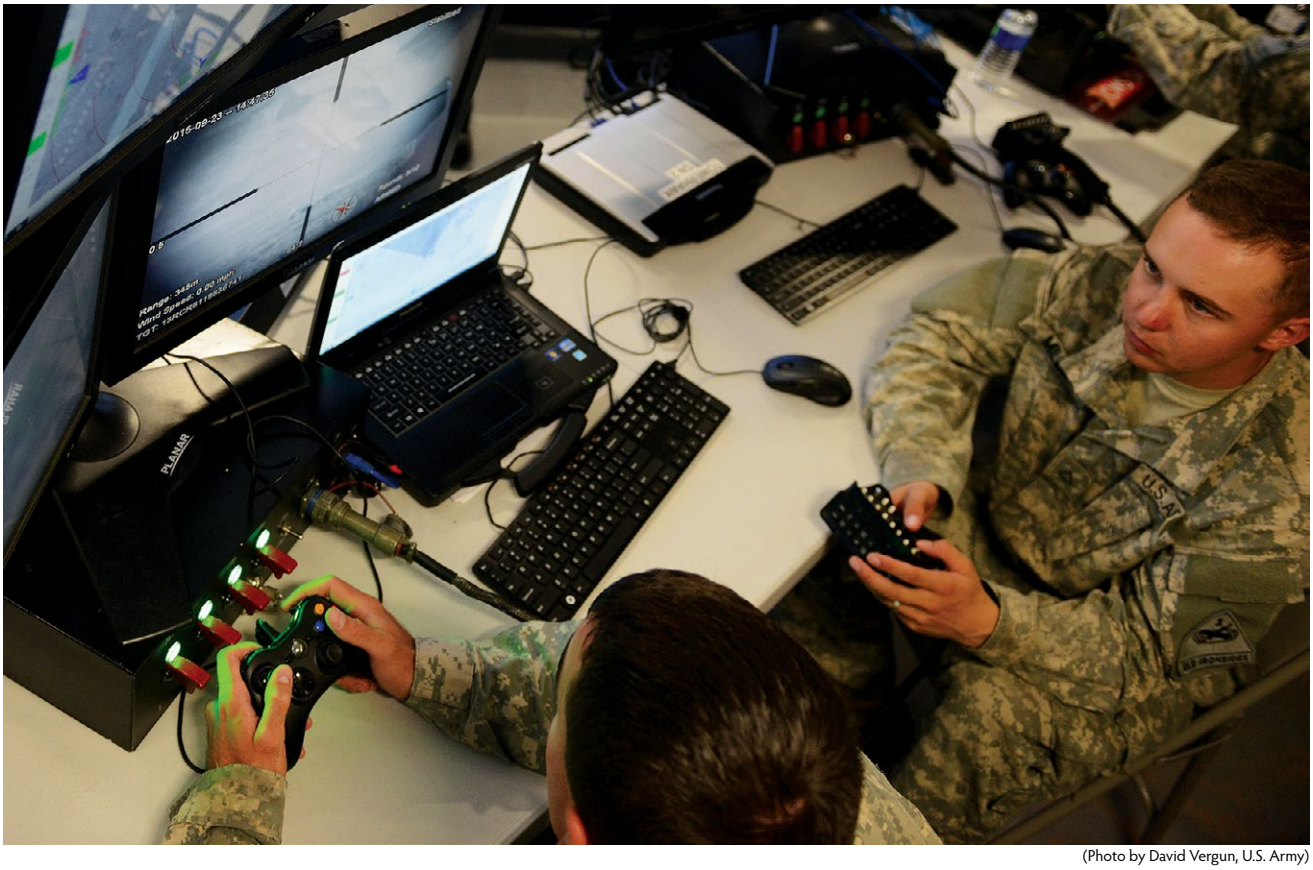
If you don't know where you are going, you might wind up someplace else.[16]

—Yogi Berra

In a perfect world, the Army could anticipate its capability needs far enough in advance to permit the traditional acquisition process to succeed. Unfortunately, innovation in cyberspace is moving too fast to make that timeline practical for cyber SU. The typical timeframe for identifying a need, writing the requirements, negotiating the Joint Capabilities Integration and Development System (JCIDS) process, and then producing a new widget is five to eight years. The JCIDS process attempts to accommodate information systems software development with a more efficient Information Technology (IT)-Box option.[17] Although the Army is utilizing the IT-Box, it has been slow to approve the first cyberspace-related requirements document.[18] One of the Army's challenges might lie in an acquisition system that is tied to old paradigms.

Training and Doctrine Command's Gen. David G. Perkins pointed out that the defense acquisition system is still geared toward filling gaps that differentiate us from a known enemy as opposed to increasing our rate of innovation.[19] Perkins said the Army must be willing to kill old programs and then put those resources into new and more transferrable technologies.[20] He added that in order to innovate, the Army must avoid creating requirements with too much specificity else they become self-confining.[21]

Clearly, the Army has a strong desire to innovate, but an outmoded acquisition system and old thinking are not the only things slowing them down. Another challenge is a discordant cyberspace capabilities development effort. Currently, there are several overlapping information system capability documents in draft.[22] All of them



(Photo by David Vergun, U.S. Army)

Cyberwarriors defend the network at the tactical operations center for the 2nd Armored Brigade Combat Team, 1st Armored Division, on Fort Bliss, Texas, during Network Integration Evaluation (NIE) 16.1. The NIE was conducted from 25 September to 8 October 2015.

promise capabilities applicable to cyber SU. Though the Army Capabilities Integration Center (ARCIC) attempted to coordinate these disparate efforts, no significant economies have as yet been achieved.

The assistant secretary of the Army for Acquisition, Logistics and Technology (ASA[ALT]) recently developed a coordinated approach to deliver cyberspace-related technologies.[23] However, it appears to be focused more on cyberspace defense and offense, not on enabling capabilities like cyber SU.[24] Although one of the ASA(ALT) goals is to create an integrated network operations capability that will increase understanding about the health of tactical networks, that capability appears to exclude other information pertaining to factors outside of friendly networks that might interest tactical commanders.[25] And, although in 2014 ASA(ALT) responded to ten operational needs statements from Army Cyber Command addressing near-term requirements, the primary focus has been on reducing network vulnerabilities and not cyber SU.[26] This top-down strategy is a positive step, but it has not yet translated into a coordinated cyberspace capabilities development effort at the bottom of the bureaucracy.

A Simple Approach for Army Cyber SU Capability Developers

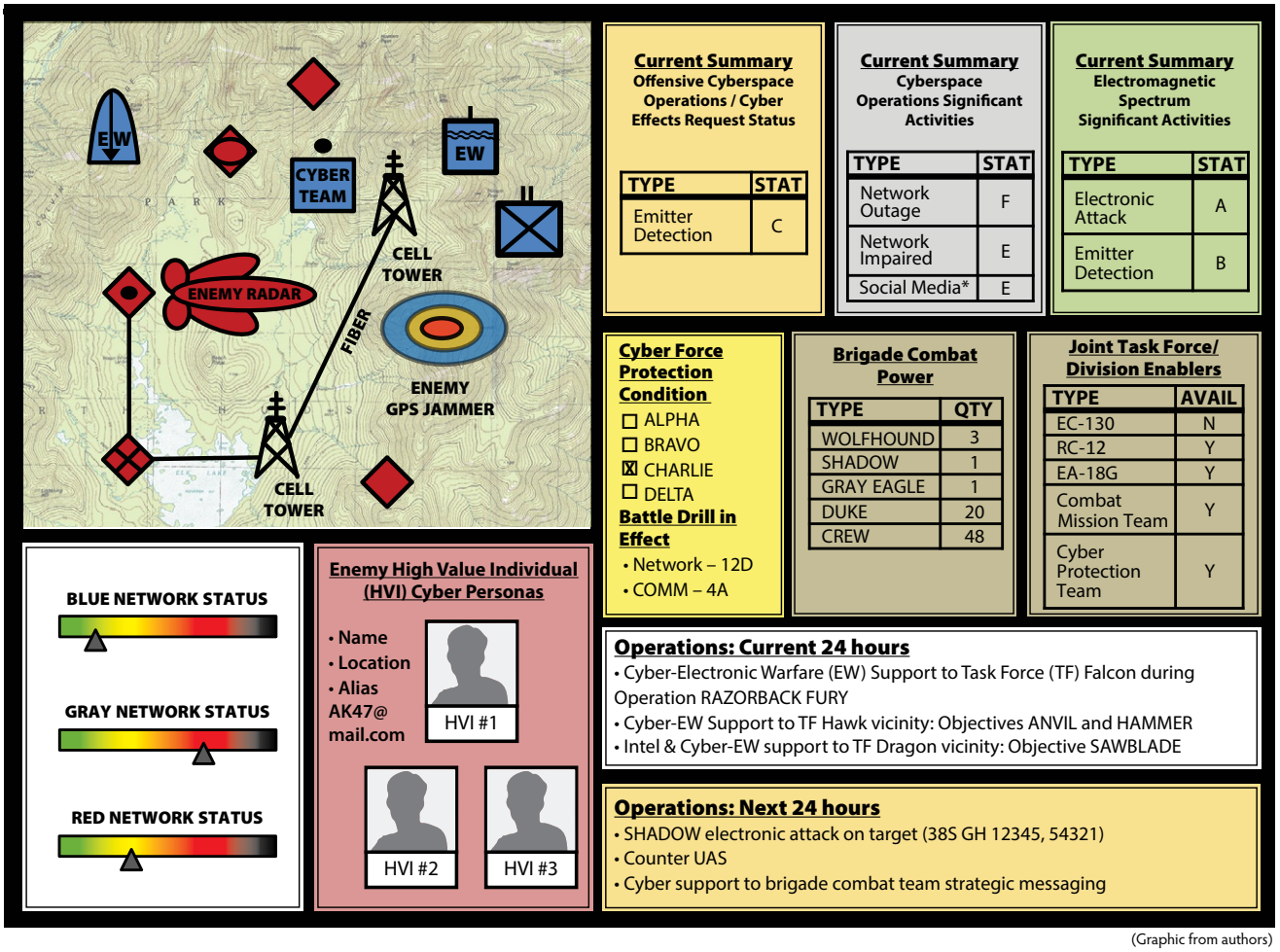
You can observe a lot just by watching.[27]

—Yogi Berra

The U.S. Army does not need a perfect cyber SU system ten years from now; rather, it needs a good enough cyber SU system *right now*. To achieve this, capability developers are advised to take a simple approach by answering three basic questions:

- What information do commanders need?
- How do we obtain and consolidate it?
- How should it be displayed?

In a broader sense, to successfully acquire cyber SU (or any other future capability), the Army must think of ways to innovate and incrementally reform a constraining acquisition process. First, Army capability developers



(Graphic from authors)

Figure. Sample Cyber Situational Understanding Overlay on the Common Operational Picture

must ascertain what information regarding cyberspace matters most to commanders.

During combat operations, commanders, supported by their staffs, monitor and assess progress, make decisions to exploit opportunities and counter threats, and direct the application of combat power at decisive points in time.[28] Cyberspace is a significant part of that calculus, especially concerning its effects on mission command and highly networked forms of combat power. Information that will likely comprise the basic content of the cyber SU overlay for the COP include friendly, host-nation, and enemy network status, cyber threats and enemy capabilities, key cyberspace infrastructure in the area of operations, cyberspace authorities and rules of engagement, and social media trends, to name a few.

Second, capability developers must consider where cyber SU information comes from and how to obtain it. Currently, only joint cyber mission forces are authorized to conduct cyberspace intelligence, surveillance, and reconnaissance and cyberspace operational preparation of the environment. So a great deal of information about cyberspace will originate and reside in databases at the national and strategic levels. That said, relevant data and information derived from organic information collection efforts at Army tactical echelons can provide important context.

One practical example is connecting a cyber-persona, derived from a national or joint cyberspace asset, with the identity of a real person (or organization) known to be residing in a unit's OE, as derived through local information collection. Fusing these sources provides greater situational understanding for the tactical commander and will help higher headquarters see cyberspace more clearly.

Third, capability developers must determine the best way to display the information. Cyber SU must provide adequate detail, but not too much. The Army can neither defend all of cyberspace, nor can it display all of it on a COP; otherwise, a commander's thinking could become obstructed by needless clutter. Commanders only need to know what impacts their mission, which aside from leveraging some joint cyberspace effects, consists mainly of employing traditional forms of combat power. Therefore, cyber SU must also allow information to be displayed contextually in order to facilitate broader situational understanding. This can be achieved through pictures, stoplight charts, gauges, ribbons, line-and-block diagrams, and side-by-side comparisons (as exemplified in the figure).

Fourth, capability developers must avoid writing system requirements that attempt to replace human judgment and decision making. Cyber SU must provide understanding; but it is up to tactical commanders and staffs to discern how to act on that understanding.

Fifth, and finally, the Army must think of ways to innovate and incrementally reform a constraining acquisition process. Army cyberspace requirements documents should strive to foster innovation by describing an overarching framework, grounded in sound doctrinal concepts that can be developed over time through successive software builds.[29] This is, in fact, the goal of the IT-Box. The challenge, therefore, is to identify the aspects of cyber SU that will become quickly outdated and make them modular, so they can be rapidly replaced by new innovations. In addition, Army capability developers must decide if cyber SU will be combined with other proposed or existing systems, or if it will remain pure. Combining multiple systems increases the risk that they could become bogged down for years in development. Meanwhile, the Army would be no closer to a cyber SU capability than it was in 2013 when the Army Cyberspace Operations Capabilities Based Assessment named its number one gap as commanders' situational understanding.[30]

Conclusion

The other teams could make trouble for us if they win.[31]

—Yogi Berra

While several resources currently aid in providing cyber SU, the Army lacks a well-coordinated capability development effort to define and aggregate cyber SU-related requirements. Although the JCIDS process provides capability development options with shorter timelines, it still appears inadequate as evidenced by the Army's inability to bring neither cyber SU nor any other cyber-related JCIDS document to approval.[32] Whatever the case, commanders cannot continue to relinquish key operational decisions about their OE because they lack situational understanding of the domain.

Cyber SU may not turn out to be a self-contained tool or system. Rather, the answer might be an aggregation of multiple situational understanding enabling capabilities. Therefore, the Army might be better off with an improvised system that gives them *some* cyber SU today, rather than a cure-all system that promises to deliver the world tomorrow.

Many of America's enemies have no bureaucracies and no stovepipes that hamper their ability to employ new technologies in battle. So, while Army capability developers are defining requirements, analyzing alternatives, and running the wickets of JCIDS documentation and approval, potential adversaries will be playing "small ball" and winning the cyber contest by utilizing commercial off-the-shelf technologies. To make a comeback, the Army needs a game changing play. Because, let's face it; "the future ain't what it used to be."[33] ■

Biographies

Lt. Col. William Jay Martin, U.S. Air Force, retired, is a senior military analyst with Command Decision Systems & Solutions, Inc. He received a BS from the University of Delaware and an MA from Louisiana Tech University. He is a graduate of the U.S. Air Force Weapons School, Air Force Air Command and Staff College, and Joint Forces Staff College.

Emily Kaemmer is a senior military analyst with Command Decision Systems & Solutions, Inc. She specializes in Army cyberspace capabilities development.

Notes

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). Situational understanding is the product of applying analysis and judgment to relevant information to determine the relationship among the operational and mission variables to facilitate decision making. For the purposes of this paper, it equates with situational awareness, which is not defined in joint or Army doctrine.

3. The term cyberspace situational understanding (cyber SU) refers to a notional capability that provides relevant data and information about cyberspace for display on a common operational picture or commander's dashboard. Cyber SU (the capability) is distinguished from the phrase cyberspace situational awareness (cyber SA), which per Joint Publication (JP) 3-12(R), *Cyberspace Operations* (Washington, DC: U.S. GPO, February 2013), refers to the requisite current and predictive knowledge of cyberspace and the operational environment upon which cyberspace operations depend, including all factors affecting friendly and adversary cyberspace forces.

4. Yogi Berra, *The Yogi Book*. Said on Yogi Berra Appreciation Day, Saint Louis, Missouri, in 1947.

5. Department of Defense, *The Joint Concept for Cyberspace* (JCC) (August 2012), 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). Available on the JROC Knowledge Management and Decision Support (KM/DS) System.

7. This statement is the authors' assessment after comparing the Joint Cyber SA ICD with the 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), 34. See fig. 9, "Functional Needs Analysis Gap Prioritization," and send document requests to ARCYBER.

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

9. Ibid., 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): 15. Retired Maj. Gen. Williams is the former J3 of U.S. Cyber Command.

15. Ibid.

16. Yogi Berra and 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. A search of the Capabilities and Army Requirement Oversight Council Management System revealed that, to date, no cyberspace-related documents have been approved by the Army; meanwhile the Air Force and Navy have several approved documents.

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. Information System Capability Development Documents (CDDs) allow sponsors to describe initial minimum values for key performance parameters, key system attributes, and additional performance attributes. Sponsors of software systems, which benefit from continuous technology insertions, may approve follow on documents internally vice through the Joint Requirements Oversight Council.

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

24. The three program executive offices (PEO) that have key roles in supporting future cyber technologies are (1) Command, Control, and Communications–Tactical (PEO C3T); (2) Enterprise Information Systems (PEO EIS); and (3) Intel, Electronic Warfare and Sensors (PEO IEW&S). PEO C3T is the lead for defense of the tactical network, PEO EIS is the lead for defense of the enterprise network, and PEO IEW&S is the lead for offensive cyberspace efforts.

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

26. Ibid.

27. Yogi Berra and 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, accessed 26 April 2016, http://www.dtic.mil/whs/directives/corres/pdf/500002p.pdf. Several builds and deployments of software will typically be necessary to satisfy approved requirements for an increment of capability.

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. A search of the Capabilities and Army Requirement Oversight Council Management System revealed that, to date, no cyberspace related documents have been approved by the Army; meanwhile the Air Force and Navy have several approved documents.

33. This is a misattributed quote, which Yogi Berra claims he never said. But there are conflicting sources. See Berra and Kaplan, *When You Come to a Fork in the Road, Take It*.