An embedded expeditionary cyber team performs surveillance and reconnaissance of various local networks 10 August 2016 at the National Training Center, Fort Irwin, California. The team is part of a pilot program known as Cyber Support to Corps and Below, developed to provide maneuver commanders with an improved situational awareness of the information environment and tools to shape that environment. (Photo by David Vergun, Army News Service)

"More Quaint and Subtle Ways to Kill"

The Operations Process in Future War

Maj. Wesley Moerbe, U.S. Army

He hath at will / More quaint and subtle ways to kill
— James Shirley, "The Last Conqueror"

On 13 September 1862, at a recently vacated Confederate bivouac site, a Union soldier noticed an envelope left behind by the previous encampment. The soldier opened it and found that,

in addition to a few damp cigars, he had discovered Special Order 191, signed by Robert E. Lee's assistant adjutant. As a result, the whole of Lee's operational plans for the upcoming campaign fell into Maj. Gen. George McClellan's lap.[1] Although famously timid in the field, McClellan managed to close with Lee and fought him to a bloody stalemate at Antietam on 17 September, ending the Army of Northern Virginia's first gambit into Maryland.[2]

Few of us have had to face an enemy who, unknown to us, gained partial or complete access to our plans or planning process, but our reliance upon information technology renews old battlefield challenges of planning and executing operations with reliable secrecy. Our adversaries' diligent search for asymmetric advantage leads them—almost inevitably—to our dependency upon networked and interconnected systems.[3] The problem now goes beyond throwing cyberpunches to communication disruption. The heavy use of networks for collaborative planning and decision-making processes also means our operations process itself can be attacked through the mission command system. Therefore, it is plausible that we could suffer our own Special Order 191 crisis.

Precisely such a contingency unfolded during 3rd Infantry Division's Warfighter Exercise in October 2016. Cyberwar ceased to be a future problem. The contest for supremacy in the cyber domain became an urgent and personal tactical challenge for the staff.

The lessons learned from these developments demand integration into our training and preparation for future conflict. I propose that solutions have little to do with technology and quite a bit to do with how we visualize and think about the operations process and mission command as a system in future war.

The Operations Process and Mission Command Systems Unplugged

Before proceeding further, the doctrinal and theoretical basis of U.S. Army decision making deserves exploration. In the simplest terms, the command of our country's land forces requires iteration between thought and action—a cycle of acting, reacting, learning, and adapting.[4] It is easy to take for granted, but how our headquarters makes abstract thought into something tangible carries immense importance. To better understand this, we must first disentangle ideas and processes from the physical objects that support collaboration or enhance thinking.

Use of Language

Imprecise language can infect how we think about decision making and command of our forces. In his pithy style, S. L. A. Marshall explains that in our profession, "if a word comes to mean too many things, it misses fire at the critical point."[5] In this case, he spoke of communications, and opined that it had become a military catchall, meaning so many things that it "quite frequently means nothing."[6]

Concepts embedded in both the mission command system and the operations process suffer a similar loss of clarity today. The Army relies upon the operations process and its activities—plan, prepare, execute, and assess—as cognitive scaffolding throughout operations. This means that as the chosen framework for the exercise of mission command, commanders and their staffs use the operations process to consider what they must do to solve tactical and operational problems.[7] The *how* of this framework manifests as the mission command system, those components of a unit headquarters that most would recognize. The mission command system consists of people, networks, information systems, processes and procedures, and facilities.[8] Thus, some components are tangible and others theoretical.

In keeping with mission command philosophy, this system adapts to the commander, his or her staff, and the environment.[9] To do so, the relationships among these components conform to personalities, the nature of the conflict, and the environment. Like many systems, if overly dependent upon any one component, it becomes vulnerable because it is unable to "absorb disturbances" and remain functional.[10]

The components of mission command systems include the abstract and the tactile, with little distinction made between the two. This helps explain how

Maj. Wesley Moerbe, U.S. Army, serves as a planner in the 3rd Infantry Division Headquarters at Fort Stewart, Georgia. He holds a master's degree from the School of Advanced Military Studies and a BS in military history from the United States Military Academy. He has served in the 101st Airborne Division (Air Assault) and as a company commander and a combat advisor in the 4th Infantry Division's 3rd Brigade Combat Team.

some might mistakenly blend the two aspects of mission command systems. But, the mistake is more than semantic. The use of a physical object to facilitate intellectual effort must not cause one to believe the physical object is a requirement for cognitive processes. If staff members conflate product, process, and tools, they hamper their ability to react to an attack against the mission command system. A logical and inevitable consequence of such conflation is the paralysis of a headquarters' decision making upon the loss of networks or automations capability. Our staffs must realize that wires, laptops, and servers are only meant to assist human thought in operations, and that intelligent planning neither begins nor ends with such enablers.

During my own service in a division-level staff, I found that organizational leaders (myself included) have an impulse to optimize our mission command system for stability environments with an uncontested cyber domain. It has taken discipline and the experience of general officers to expunge such habits. Carl von Clausewitz warned that a certain method or routine can "easily outlive the situation that gave rise to it; for conditions change imperceptibly."[11] I suspect that habits developed over nearly fifteen years of stability operations have created unrealistic expectations based on unexamined or dated assumptions. The most dangerous of these assumptions could be that networks and information systems remain relatively free from enemy interference. However, the evidence indicates that adversaries'

A member of an expeditionary cyber team provides cover for fellow cyber operators who are getting into camouflaged and concealed positions to perform surveillance and reconnaissance 10 August 2016 at the National Training Center, Fort Irwin, California. (Photo by David Vergun, Army News Service)

intentions and capabilities will require our readiness to reconfigure our mission command systems frequently due to enemy action. Adversaries believe, as do some Western analysts, that networks and information systems present such a vulnerability.[12]

The Decline of Information Security

Conrad Crane opens his article "The Lure of Strike" by saying, "there are two approaches to war, asymmetric and stupid."[13] With this aphorism in mind, lingering a moment on the operating concepts of our most capable adversaries is worthwhile.

Open-source documents and recent history show a pattern that both Russian and Chinese militaries try to blend traditional and nontraditional methods of warfare to undermine consensus that a state of war actually exists, creating ambiguity in the nature of the conflict itself. Moreover, they emphasize a complementary array of cross-domain operations intended to attack U.S. vulnerabilities at minimal costs to themselves. It follows that cyber conflict figures largely into both these states' operating concepts.[14]

The now widely referenced work, *Unrestricted Warfare,* looks to the combination of a number of nontraditional forms of warfare to gain advantage over the United States, singling out technology addiction in particular as having disproportionate effect upon Western forces.[15] *Unrestricted Warfare* stresses asymmetry and synergistic effects, and lambasts U.S. military doctrine as overly kinetic and missing the broader potential of information warfare. Written in 1999 without the endorsement of the People's Liberation Army (PLA), this volume represents the theories of two Chinese colonels. That said, unmistakably similar patterns of logic connect *Unrestricted Warfare* to the more authoritative *The Science of Military Strategy*.[16] Western analysis of this official PLA document notes that the Chinese have prioritized preparedness for operating with degraded or collapsed networks, and suggests that they could inflict the same against the United States.[17] A 2015 RAND study assessed that the PLA publications and exercises now enjoin a first strike against enemy computer systems and networks with a mind to "control the flow of information" to and among the enemy.[18]

In Russian doctrine, the holistic approach emphasizes information war and the use of nonkinetic means to shape the battlefield for the physical combat. The Russians call this *bespredel,* and it echoes the concepts that underpin *Unrestricted Warfare*.[19]

Russia's recent belligerence offers evidence of its perspective on cyberwar. During its 2008 conflict with Georgia, Russian hackers deliberately targeted military digital communications, delaying order distribution and sowing confusion among decision makers.[20] This approach, the combination of traditional and nontraditional forms of conflict, integrates the full spectrum of offensive capabilities to create ambiguity.

More recently, operations in Ukraine demonstrated an even more refined execution of gray war and, like earlier conflicts, paralyzed Ukraine's military response by shattering its decision-making cycle through information control.[21] Russian sources, both official and unofficial, place a premium on information isolation.[22]

Understandably, U.S. policy makers and security specialists fix their attention on the possible threats that these doctrines have for the homeland. Certainly, we would prefer to avoid serious disruptions to life in the homeland, but in a major conflict these are inevitable to some extent. In fact, John Arquilla, a noted RAND theorist, criticizes fears over cyberattacks against the homeland as overwrought, citing the resiliency of civilian populations against strategic bombing campaigns in the Second World War.[23] After all, bugs can be patched, financial institutions can rebound, and order can be restored to a major city suffering from cyberattacks against infrastructure.

However, a nation's operational and tactical formations in the midst of an active conflict have little time to recover from a collapse of information networks. Timely decision making will not wait for a trouble-ticket to be processed. In our present age, strategic thinkers must concern themselves with cyber conflict for sure, but we must also consider the resilience of operational and tactical formations against what John Arquilla calls a "bitskrieg."[24]

In a revealing chapter of *Dark Territory*, Fred Kaplan describes how U.S. forces in concert with interagency partners executed a startlingly effective campaign behind the curtain of the Iraq surge conducted by Gen. David A. Petraeus. Less publicized than the counterinsurgency efforts, but just as important, were the efforts of Gen. Stanley A. McChrystal's targeting operations, which effectively

pierced the insurgent network's mission command system and wreaked havoc on their operations process from within. Joint Special Operations Command led enemy forces into ambushes with false information and isolated cells by severing the links between them.[25] Despite the strength and resilience of networked organizations, in this case, enemy forces lost the initiative entirely. Later, Petraeus singled out McChrystal's operations as a critical component of the overall strategy, noting that he had swept "senior and mid-level leaders" from the battlefield, the results of which allowed time and space for the population-centric strategy to work.[26]

Of note, the enemies McChrystal defeated used commercially available tools and Internet capabilities, and while one might suppose that private networks established by state militaries to be more secure, this may not be so for long. The United States now reports it has the capability to access wireless tactical networks like our own.[27] Now imagine if the enemy, rather than McChrystal, had such capabilities. Imagine that an adversary had breached our own mission command system. Indeed, it seems unwise to suppose future enemies will not possess such a capability based on these developments and the findings of a 2013 cybersecurity review panel.[28]

The automations networks of U.S. Army headquarters organizations now form the backbone of our collective brain. In *The Scientific Way of Warfare,* Antoine Bousquet lands squarely on the problem this creates. In our enthusiasm for the potential of networks and information, he warns that we become "utterly dependent" on such capabilities.[29] In essence, the tools by which we collaborate and make decisions in our tactical headquarters have created a fatal vulnerability by merging product and process.

Consider how the Army now conducts the operations process in a division headquarters. The staff forms into working groups or planning teams, often dispersed via the network. Even if they convene in person, the staff captures each step of the planning process in a digital medium of some kind. Briefings to the commander may take place around an analog map, but nearly all orders dissemination occurs through digital media. As operations progress, fragmentary orders go out by e-mail, annexes get posted to portals, and dozens of other supporting products get posted in various digital commons.

Given the risk of concentrating the entire staff and commanders of a division at a single targetable location, even rehearsals may take place not around a terrain model but with leaders huddled around monitors in their headquarters tents. In each case, a capable adversary might plausibly penetrate the operations process.

Once inside our cyberperimeter, the possibilities are as diverse as they are unsettling. An enemy could choose to disrupt planning and executing by shutting down the network, or it could covertly capture plans from within the network and adapt its own operations to increase the odds of success. Worse still, the enemy could develop the ability to corrupt our mission command system by altering or planting false data or information into our network. Considering that both China's and Russia's operating concepts revolve around creating ambiguity, challenging the clarity of planning operations is a likely pursuit of their operations.

As we have already seen, these are not hypothetical capabilities—the technology already exists to realize those ends. The point is not that we ought to live in fear that all our plans are known to the enemy but rather that we cannot assume the impenetrability of our networks or the absolute secrecy of our decision making. This provokes the question, what are the prospects of victory without our accustomed informational advantages?

Preparing for Information Dystopia

Sobering as these possibilities may be, we need not panic. Divining the operating concept behind the threat clarifies our problem. To prepare for potential wars to come requires developing and strengthening two divergent competencies: resilience in our information networks and, simultaneously, the ability to plan, prepare, execute, and assess "in the dark" in the event networks are disabled or fatally compromised.

During the 3rd Infantry Division's October 2016 Warfighter Exercise, even after the enemy gained access to our networks and enjoyed the ability to adapt its scheme of maneuver to defeat our own, the division succeeded. We met with success not through any act of prescience but rather through a plan that permitted subordinate brigade combat teams the flexibility to respond to battlefield circumstances. Let us unpack the

Sgts. 1st Class Richard Miller (*left*) and Brian Rowcotsky of the U.S. Army Cyber Protection Brigade discuss the response to a simulated cyber attack on the 1st Brigade Combat Team, 82nd Airborne Division, with Staff Sgt. Frederick Roquemore (*standing*), a cyber network defender with the 1/82nd, during the unit's rotation 6 November 2015 at the Joint Readiness Training Center at Fort Polk, Louisiana. (Photo by Bill Roche)

possibility of mitigating these developments regarding network integrity.

Coming to grips with the penetrable operations process requires, above all, that the mind be made ready for a new norm. The idea that it could happen should not be a far-off possibility. From Robert E. Lee's saddle, the hazard of an intercepted order, though not necessarily common, was a known possibility. Telegraph wires could be cut or tapped by either side, and couriers killed or captured.[30] Neither the Federal nor the Confederate armies possessed a decisive advantage in information security. The simple recognition of this condition meant that all commanders needed to be mindful of indicators that their plans were known to the enemy, or that their own orders had failed to reach subordinates.

That does not mean we should eschew the multiplicative power of our networked systems but rather train to avoid dependency upon them. The mind can grow accustomed, perhaps addicted, to clarity or certainty that can be artificial or temporary. In *Certain Victory: The US Army in the Gulf War*, Gen. Robert H. Scales describes the unfulfilled hunger for precision intelligence and unfailing communications that many commanders had grown dependent upon during their service in Europe.[31] How fascinating that when weather and distance induced lapses in communication, the intent-based orders of Maj. Gen. Frederick M. Franks Jr. allowed the Seventh Corps to continue planning and executing by "grease pencil and acetate."[32]

With such historical precedents in mind, a severe cyberattack or network collapse must become an anticipated event—as likely as indirect fire in the security

area. Furthermore, the cognitive and procedural adjustment from network-enabled planning to pure analog will not happen of its own accord but requires that leaders act and staff reorganize.

Transition from a computer network-centric to a traditional hand-driven process calls for different responsibilities, outputs, and communication media. The physical act of planning and executing relies upon different agents. Agility, in part, will be the speed at which a staff can reorient on an analog process and then back to a full network-enabled capability without loss of potency.

Those who design exercises and training bear the responsibility of placing stress on these processes. Training the operations process "unplugged," as it were, helps the members of the staff survive this turbulence and retain staff cohesion and functionality. They can better understand the difference between product and process while supporting the commander's decision making. In sum, when buffeted by unreliable networks, we may fall back on sound training, but training and warfighting must proceed from a sturdy and tested operating philosophy—in our case, mission command.

We may be comforted that our forebears successfully coped with the uncertain information environment long before us. During Napoleon's 1809 Danube Campaign, Napoleon's Army of the Danube, and the Army of Italy, under his stepson, Eugene, advanced on Vienna on two distinct axes separated by the Italian Alps. A weeklong ride kept both commanders in the dark as to the success or failure of the other. Eugene blundered into his first engagements but rediscovered his confidence and dealt Archduke John a decisive defeat.[33] He then fought his way into Austria to join Napoleon's forces against Archduke Charles based on little more than an operational approach described to him by dispatches from his commander before departing.[34] I propose that rather than greater information security or dominance, our endeavors must engender a more authentic exercise of mission command.

During our division exercise, I overheard the wry remark by a senior officer, "I know the enemy doesn't know what we're going to do because I don't know what we're going to do." The comment frames a final point worth considering. If the enemy penetrates our mission command system, detailed operational and deception plans become liabilities. The wider the commander's range of options, the more difficult to counter them. Deception has value, but for tactical and operational headquarters, returns may not merit large investment. Retired Brig. Gen. Huba Wass de Czege echoes this sentiment in describing a personal epiphany as a brigade commander at the National Training Center: "Creating ambiguity is a lot more important than trying to create deception."[35] Creating ambiguity does not imply not planning but rather means avoiding patterns and keeping every option available for the longest possible time. In practical terms, this manifests as the use of decision-point tactics. Decision-point tactics respect Helmuth von Moltke's dictum that "one does well to order no more than is absolutely necessary" while putting to good use the planning capacity of the staff.[36]

Concluding Thoughts: Peace with Uncertainty

Martin van Creveld's study *Command in War* delves into the nature of the operations process and finds the American "pathology of information" during the Vietnam War nearly enough to "make one despair of human reason."[37] His critique stings but rings true. Then and now, technological capabilities seduce us into dependency on a fickle mistress. The "quest for certainty," he assures us, is an errant one, and the weight of evidence supports his claim.[38]

Our decision-making processes must prostrate themselves to uncertainty rather than attempt to abolish it. The pursuit of ambiguity and confusion forms the logic of our adversaries' military response to U.S. superiority in traditional warfighting. The Chinese and Russian operating concepts put cross-domain operations at their core and scale from the strategic to the tactical. Cybercombat figures largely into their all-encompassing vision of warfare, and the capability to penetrate military networks already exists. The cognitive aspect of the operations process need not change, but we must prepare for the likelihood that our digital couriers may be intercepted or worse. Columnist Sebastian Bae captures the essence of our times, asserting that victory will go to "those who effectively leverage information to confuse, deceive, and control the adversary."[39] The discovery of Special Order 191 may or may not have changed the course of

the American Civil War, but the potential seems clear even to amateur historians. We would do well to heed the spirit of our own times and prepare our staffs and commanders for a contested information environment where even our decision-making process may not remain hidden from the enemy. ■

Notes

Epigraph. James Shirley, "The Last Conqueror," in *Palgrave's Golden Treasury of the Best Songs and Lyrical Poems in the English Language*, ed. Francis Turner (London: J. M. Dent, 1906), 70. Shirley's poem points to the breadth of death's devices and suggests, as I do, that the greatest hazards are often the least obvious.

1. Francis Winthrop Palfrey, *The Antietam and Fredericksburg* (New York: Charles Scribner's Sons, 1910), 21–23.
2. William Allan, *Stonewall Jackson, Robert E. Lee, and the Army of Northern Virginia, 1862* (New York: Da Capo Press, 1995), 243.
3. Department of Defense, Defense Science Board, *Task Force Report: Resilient Military Systems and the Advanced Cyber Threat*, (Washington, DC: Office of the Under Secretary of Defense for Acquisition, Technology and Logistics, January 2013), 17, accessed 28 December 2016, http://purl.fdlp.gov/GPO/gpo60252.
4. Army Doctrine Reference Publication (ADRP) 5-0, *The Operations Process* (Washington, DC: Government Publishing Office [GPO], 2012), 1-1.
5. S. L. A. Marshall, *Men Against Fire: The Problem of Battle Command* (Norman, OK: University of Oklahoma Press, 1947), 85.
6. Ibid.
7. ADRP 5-0, *The Operations Process*, 1-2.
8. ADRP 6-0, *Mission Command* (Washington, DC: GPO, 2012), 3-8.
9. Ibid., 1-5.
10. Dietrich Dorner, *The Logic of Failure* (Cambridge, MA: Perseus Books, 1997), 75.
11. Carl von Clausewitz, *On War,* eds. and trans. Michael Eliot Howard and Peter Paret (Princeton, NY: Princeton University Press, 1976), 154.
12. Antoine J. Bousqet, *The Scientific Way of Warfare: Order and Chaos on the Battlefields of Modernity* (New York: Columbia University Press, 2009), 232; Astrid Stuth Ceballos, Cristina L Garafola, and David C. Gombert, *War with China: Thinking Through the Unthinkable* (Santa Monica, CA: RAND Corporation, 2016), 14, accessed 6 January 2017, http://www.rand.org/content/dam/rand/pubs/research_reports/RR1100/RR1140/RAND_RR1140.pdf.
13. Conrad C. Crane, "The Lure of Strike," *Parameters* 43, no. 2 (Summer 2013), accessed 23 December 2016, http://strategicstudiesinstitute.army.mil/pubs/parameters/issues/Summer_2013/1_Crane_SpecialCommentary.pdf.
14. Angus Goldberg, "Bespredel and the Conduct of Russian Hybrid Operations," *Small Wars Journal* website, 26 October 2016, accessed 28 December 2016, http://smallwarsjournal.com/jrnl/art/bespredel-and-the-conduct-of-russian-%E2%80%9Chybrid-operations%E2%80%9D; Timothy Thomas, *The Three Faces of the Cyber Dragon* (Fort Leavenworth, KS: Foreign Military Studies Office, 2012), accessed 5 January 2017, http://fmso.leavenworth.army.mil/EPubs/Epubs/3Faces%20of%20the%20Dragon.pdf.
15. Liang Qiao, Al Santoli, and Xiangsui Wang, *Unrestricted Warfare: China's Master Plan to Destroy America,* trans. Central Intelligence Agency (Panama City, Panama: Pan American Publishing, 2002), 77.
16. *The Science of Military Strategy* remains accessible only to Chinese linguists, but Chinese experts from Jamestown Foundation have made available their yeoman's work of translation and analysis. See Joe McReynolds, "China's Evolving Perspectives on Network Warfare: Lessons from the Science of Military Strategy," *China Brief* 15, no. 8 (Washington, DC: Jamestown Foundation, 16 April 2015), accessed 5 January 2017, https://jamestown.org/program/chinas-evolving-perspectives-on-network-warfare-lessons-from-the-science-of-military-strategy/.
17. Mingda Qiu, "China's Science of Military Strategy Cross-Domain Concepts in the 2013 Edition," Cross-Domain Deterrence Project Working Paper (La Jolla, CA: University of California San Diego, September 2015), 17–20, accessed 28 December 2016, http://deterrence.ucsd.edu/_files/Chinas%20Science%20of%20Military%20Strategy%20Cross-Domain%20Concepts%20in%20the%202013%20Edition%20Qiu2015.pdf.
18. Eric Heginbotham et al., *The U.S.-China Military Scorecard: Forces, Geography, and the Evolving Balance of Power, 1996-2017* (Santa Monica, CA: RAND Corporation, 2015), 276, accessed 1 January 2017, http://www.rand.org/content/dam/rand/pubs/research_reports/RR300/RR392/RAND_RR392.pdf.
19. Angus Goldberg, "Bespredel and the Conduct of Russian Hybrid Operations."
20. Sebastian Bae, "Cyber Warfare: Chinese and Russian Lessons For US Cyber Doctrine," Georgetown Security Studies Review website (blog), 7 May 2015, accessed 28 December 2016, http://georgetownsecuritystudiesreview.org/2015/05/07/cyber-warfare-chinese-and-russian-lessons-for-us-cyber-doctrine/.
21. Shaheen Ghori and Azhar Unwala, "Brandishing the Cybered Bear: Information War and the Russia-Ukraine Conflict," *Military Cyber Affairs* 1, no. 1 (2015): 6–7, accessed 23 December 2016, http://scholarcommons.usf.edu/cgi/viewcontent.cgi?article=1001&context=mca.
22. Ibid., 2
23. John Arquilla, "Cyberwar is Already Upon Us," *Foreign Policy,* 27 February 2012, accessed 28 December 2016, http://foreignpolicy.com/2012/02/27/cyberwar-is-already-upon-us/?wp_login_redirect=0.
24. Ibid.
25. Fred M. Kaplan, *Dark Territory: The Secret History of Cyber War* (New York: Simon and Schuster, 2016), 160.
26. David Petraeus, "How We Won in Iraq," *Foreign Policy*, 29 October 2013, accessed 28 December 2016, http://foreignpolicy.com/2013/10/29/how-we-won-in-iraq/.
27. Sydney Freedburg, "Wireless Hacking in Flight: Air Forces Demops Cyber EC-130," *Breaking Defense*, 15 September 2015, accessed 28 December 2016, http://breakingdefense.

com/2015/09/wireless-hacking-in-flight-air-force-demos-cyber-ec-130/.

28. Defense Science Board, *Task Force Report*, 5.

29. Bousquet, *The Scientific Way of Warfare*, 222.

30. Robert S. Lanier, Francis Trevelyan Miller, and Henry Wysham Lanier, *The Photographic History of the Civil War,* vol. 8 (New York: The Review of Reviews, 1911), 288 and 362.

31. Robert H. Scales, *Certain Victory: The US Army in the Gulf War* (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 1994), 375.

32. Ibid.

33. Robert M. Epstein, *Napoleon's Last Victory and the Emergence of Modern War* (Lawrence, KS: University Press of Kansas, 1994), 49, 85, 95, and 128.

34. Ibid.

35. Huba Wass de Czega, "Carousel of Deception," in *66 Stories of Mission Command*, eds. Adela Frame and James W. Lussier (Fort Leavenworth, KS: U.S. Army Command and General Staff College Press, 2000), 27.

36. Helmuth von Moltke, *Moltke on the Art of War: Selected Writings*, ed. Daniel J. Hughes (Novato, CA: Presidio Press, 1993), 184.

37. Martin Van Creveld, *Command in War* (Cambridge, MA: Harvard University Press, 1985), 260.

38. Ibid., 264.

39. Bae, "Cyber Warfare."