The New Matrix of War

Digital Dependence in Contested Environments

Capt Keith B. Nordquist, USAF

Disclaimer: The views and opinions expressed or implied in the Journal are those of the authors and should not be construed as carrying the official sanction of the Department of Defense, Air Force, Air Education and Training Command, Air University, or other agencies or departments of the US government. This article may be reproduced in whole or in part without permission. If it is reproduced, the Air and Space Power Journal requests a courtesy line.

> *Do you believe that my being stronger or faster has anything to do with my muscles in this place?*
>
> —Morpheus (Laurence Fishburne), *The Matrix*

Simply being stronger or faster is no longer enough when operations hinge on cyber capabilities, and this dependence exposes vulnerabilities. Since the end of the Cold War, the DOD has proven its strategic advantage across the spectrum of conflict in quantity, quality, and readiness. This kinetic strength is what allies rely upon and enemies fear, equating American dominance to mission assurance.[1] In the digital age, the cyber domain underpins this dominance and preserves the ability to project asymmetric kinetic power worldwide at any time.[2] In kind, adversaries are beginning to acknowledge America's reliance on digital tools in preserving its strategic advantage. As adversaries develop robust digital interference competencies, the conflict moves beyond an exclusively near-peer competition of conventional forces and becomes a comprehensive conglomeration of contested domains. The rhetorical question famously asked by Morpheus in *The Matrix* trilogy captures the essence of this digital dependence and the thoughtfulness it necessitates; strength and speed do not matter within the matrix.[3] The question's import is equally pertinent today; when projecting military muscle requires digital tools, virtual failures affect reality.

The strategic imperative for a new matrix of war is clear—cyber domain operations are the bedrock of American military strength today, and consequently, they are its greatest liability for tomorrow. In particular, those near-peer competitive advantages of the DOD in command and control, deployment and distribution, and weapon system technology exist because of the complementary and enabling nature of cyberspace.[4] Imagine prosecuting an operation at the tactical or strategic level without cyber tools enabling freedom of maneuver—even for just one day. If an adversary disrupts, interrupts, or denies US cyber capabilities, American superiority no longer matters—the DOD cannot employ its strategic advantage. A day without cyber could be catastrophic if the impact is a nullification of a capability to project power. Exercising a holistic vulnerability assessment, the cyber domain is critical to the application of kinetic power. Through reflection and analysis, the DOD must adjust in kind for the increasing risk it encounters when inextricably linking the military enterprise with the digital tools it needs to function.

The implicit charge is to understand and counter possible strategic shock from a cyber attack and appreciate the depth of capabilities that exist in cyberspace. By adjusting military planning cognitive associations, to appreciate the depth of capabilities that exist in cyberspace, the DOD can continue to assure mission success, even during cyber attacks and degraded operations. This change in DOD cognitive association would illustrate how kinetic effects are secondary to digital dominance and inform strategic solutions that deter and defeat cyber domain threats. The future requires constructing an updated, globally integrated strategy that recognizes a superior force attracts digital disruption. Contemplating a day without cyber means acknowledging risk across domains and understanding that conflict transcends physical battlefields, especially as the battlespace becomes more transregional, multidomain, and multidimensional.[5] The new matrix of war in the digital age necessitates concerted transformation, both to appreciate the current calculus of conflict and acknowledge the strategic shock of denied kinetic effect delivery.

Strategic Shock

Disruptive effects to digital tools in the cyber domain ignore the traditional kinetic understandings of conventional warfare. Currently, military planners tend to focus on two incomplete assumptions: (1) contested environments exist in the designated conflict theater, and (2) militaries win wars where kinetic force meets kinetic force.[6]

Assumptions like these fail to adequately address the evolving complexities and connectedness of the new matrix of war. If military planners do not accept that adversaries may achieve strategic outcomes without kinetic power, the US may be susceptible to *strategic shock*.[7] Strategic shock is similar to the principle of shock and awe—instead of overpowering an adversary's physical force to the point of paralysis, one strategically overwhelms their ability to orient themselves in policy or directing forces. In this context, strategic shock is cognitive in nature, encompassing the perceptions, experiences, and psychologies of the opponent.[8] Consequently, to induce strategic shock in an adversary, one must disrupt these cognitive associations.

The DOD's cognitive depth is rooted in its cyber capabilities, representing the crucial foundation of American military execution. However, DOD resources and energies remain focused on more institutionalized cognitive associations concerning employment—better managed forces, global deployability, and more advanced weapon technologies.[9] Understanding the need for a greater focus on cyber domain security requires a cognitive acceptance that the DOD's depth should be associated with its digital tools, not just its superior capability. Should an adversary attack the DOD's digital dependence without this association, the potential for strategic shock is disastrous. Specifically for the military, an adversary does not need to compete with the DOD's superior capacity, capability, or availability—they need only degrade the ability to employ its advantages to produce strategic effects. More broadly, an enemy can deliver superior effects over a superior force if they disrupt the cognitive depth of their function. A lack of cognitive association to that depth extends the vulnerability and exacerbates the effect. This widens the aperture for understanding DOD risk mitigation, and it expands planning from the frontline to the point of embarkation and from the weapon system to its digital footprint. In particular, those strategic capabilities of the DOD most susceptible to strategic shock without a change in cognitive association are also its employment strengths—command and control (C2), deployment and distribution, and weapon system technology. Each of these strengths needs strategic solutions to deter and prevail in contested environments.

Contested Environments

The contested cyber domain embodies conflict that is no longer exclusive to an abroad, permissive battlefield.[10] Instead, digital tools extend the conflict to the homeland and limit access of the US; one will have to fight to get to the fight in the new matrix of war. C2 is the critical element needed to guide the projection of power from garrison to a conflict area. An examination of the cyber domain needed to enter conflict in a transregional, multidomain context encompasses the tools used for tactical execution, operational guidance, and strategic oversight.[11] Today, the systems to communicate up and down the chain of command are digital, from planning to tasking to executing. Whether through constellations of satellites or cyberspace networks,[12] DOD C2 and communication rely upon tools almost exclusively enabled through the cyber domain to enter an engagement. Designed for decentralized execution,[13] the demands on these digital tools require global awareness and dedicated focus to preserve access. However, each combatant command often employs C2 tools in isolation by centralizing their execution tools, requesting forces, and operating separately from geographic and functional partners. This operating construct represents the DOD's current cognitive association,[14] but it is limited to antiquated and conventional dynamics. The DOD should instead pursue more globally integrated planning for its C2 functions to embrace the comprehensive digital capabilities of its enterprise. Through a worldwide situational awareness, the DOD can cognitively associate C2 with tools that transcend terrestrial designations and authorities. If unaddressed, enforcing parochial C2 relationships in geographic areas of responsibility incurs greater risk of strategic shock.

A critical utility of capable C2 is to manage the deployment and distribution of the military, delivering and sustaining a decisive force to the place of need. Cognitively linking the battlefield to its distribution network expands the contested environment and thrusts logistics into a precarious, strategic center of gravity role.[15] No longer will the DOD be able to operate the global distribution network with impunity as it has for the last 70 years. Today, the end-to-end functionality of the system, from combatant commander request to sourcing and delivery, relies almost completely upon digital tools. The DOD must realistically account for the potential of denied access to these power projection tools so it can disperse the gravity from its logistics cyber dependency. Through cyber perseverance and resilience strategies, the DOD must fight through degradation and preserve the ability to deliver options to joint force commanders. Stove-piped cognitive associations of domain-specific conflict no longer support the global battlespace. Consequently, joint force power projection cannot just be about a capability to effectively and decisively distribute the force; it must also be about its enabling digital network. This multitiered and worldwide view more accurately informs needs and requirements, countering the threat of strategic shock.

In a globally integrated battlespace, DOD weapon systems also depend on digital technologies to operate, and these physical tools are equally susceptible to cyber intrusions. Reliant upon GPS, operating software, and unclassified network acquisition processes,[16] weapon systems are subject to disruption possibilities from development to employment. Moreover, these same weapon systems are subject to attrition and mobilization complications.[17] Failing to consider and plan for cyber domain reliance undermines the survivability and movement of DOD weapon systems, the kinetic equipment needed when prosecuting campaigns. Without addressing how attrition, mobilization, and cyber vulnerabilities converge, the DOD may fail to defend against adversaries when moving resources and employing weapon systems at the speed of war. At worst, a failure to cognitively associate cyber threats with weapon system development may foreshadow fewer available options for joint force commanders, causing the DOD to lose potency when projecting power and lethality. Since losing options costs strategic outcomes, the DOD must address weapon system susceptibility to cyber attack to avoid strategic shock. If not, it could be unprepared to counter the extensive liabilities of the cyber domain.

Strategic Solutions

To deter, deny, degrade, or defeat the threat of strategic shock in C2, deployment and distribution, and weapon system technology, the DOD must holistically address the threat of cyber attack.[18] This requires investigating two broad problem sets with concerted focus: (1) how to preserve American superiority in increasingly contested environments, and (2) how to craft a superior strategy that protects our power projection ability across domains.

These focus areas consider the interdependent impacts of cyberspace problems as the strategic framework to engage the new matrix of war, illustrating the need for a paradigm shift. By balancing superior quantity, quality, and readiness of the force with superior strategy, the DOD can account for its digital dependence, deter aggressive action, and prevail when disrupted. The strategic solutions presented underline the DOD's required cognitive shift in understanding its depth, where superior kinetic effects are secondary to superior posturing with digital tools. Without fundamentally changing its focus to the actual depth of the military's power, it may fail to advance or even preserve its strategic advantage.

The globally deployable and dominant force of the DOD represents an inherent target for adversaries in the cyber domain.[19] Complicating this contested environment, the force is constantly under tension to balance superior quantity, quality, and readiness. Ostensibly, military planners should focus on all three—develop a robust organic capacity of the best technologies, ready to be deployed at a moment's notice.[20] However, budgetary constraints and fluctuating military demands make this difficult, if not impossible, creating a need to inject greater agility and velocity in the execution of military acquisition and operations processes.[21] Cognitively associating a superior force in contested environments with the cyber domain requires the explicit pursuit of gains in force efficiency and globally integrated planning. Using advanced digital tools through the cyber domain, the DOD can prepare for the next high-end conflict by purposefully leveraging existing force quantity, quality, and readiness to generate more capability. Specifically, optimization can preserve a superior force by advancing efficacy in tasking and execution with evolving technologies like automation, machine learning, and algorithmic predictive analysis.[22] This data-driven mindset in managing, enhancing, and deploying a superior force spirals current quantity, quality, and readiness by reducing effort and waste. By making their equilibrium easier to manage and improve in resource-constrained and contested environments, the DOD also capitalizes on its inherent digital depth.

To deter and prevail against cyber attacks in this data-centric community, the DOD must better deny adversary access and promote greater redundancy.[23] Together, they preserve kinetic advantages as cyber assurance strategies. If an enemy is unable to penetrate a hardened network, whether through a securely enabled cloud-based infrastructure or robust authentication protocols from trusted transactions or quantum entanglement, the DOD minimizes vulnerabilities.[24] When the technological cost of entry increases, the eligible pool of capable hostile actors becomes smaller, enabling more tailored and direct address. However, a network barrier limiting access to these most capable adversaries does not disperse vulnerabilities or safeguard functionality. For the DOD to prevail and ensure the utility of its depth, it should move from a link-in-a-chain cyber processing dynamic to a portion-of-a-whole model.[25] Spreading the risk across both a physical and virtual web ensures the capability of a superior force by minimizing exposure and diffusing weaknesses across a network. A web model negates an adversary's ability to totally disrupt operations through the scope and level of effort required to affect them all. Together, synergizing a robust firewall with a dispersed digital footprint preserves the superior force's advantage, especially if called to action in cyber-degraded operating environments.

The evolving construct of contested environments presents a unique opportunity to strategically assess the cyber assumptions in military strategy and recognize how enemies seek asymmetric or unconventional advantages.[26] In particular, crafting a broader strategy matrix that acknowledges how C2 deployment and distribution, and weapon system technologies are contested through the cyber domain allow for a more global and comprehensive understanding of military operations. A broader strategy matrix also counters the potential for strategic shock by grounding the cognitive associations of the DOD within its digital dependence. With an organizational mindset that focuses on mission assurance in a cyber-enabled and potentially degraded environment, the DOD can not only promote the evolution of digital capabilities but also protect current, critical cyber functions from a disadvantage. It is empowered to transform with the evolved battlespace, blurring the lines between domains and systems through strategic planning to assure the mission.[27]

As cyber becomes more multidomain in execution and function through globally integrated planning, the DOD must also address roles and responsibilities, authorities, and dynamic prioritization in relation to the cyber threat.[28] Specifically, it must explore operational models that support its digital depth, leveraging current and future cyber tools to protect advantages, deny adversary access, and prevail against hostile action. Additionally, these operational models need to address the cognitive tension between employing kinetic advantages and enabling them. The DOD cannot accept losing capability or forces in unacceptable numbers along this digital employment connection but may be susceptible to such losses with planning constrained to domain-specific outcomes.

To prevent strategic shock from stove-piped cognitive associations, strategic risk must continuously address the possibility of interference in those digital tools that connect the military planner to the warfighter, the cyber thread that connects all levels of the DOD.[29] The military should also reassess strategic risk with a global perspective, to redress the permissive geographic assumptions that have permeated conflict since the Second World War, centered on the belief that the US can operate at will. Future conflicts will not be limited to a single combatant command, so cognitive associations require adjustment to view kinetic effects as products of robust and global cybersecurity. Moreover, contested environments make the binary relationship between peace and war murkier due to persistent adversarial action in the cyber domain. Digital tools are constantly at risk, so preventing strategic shock requires relentless advocacy. As with preserving a superior force, DOD planners should focus on how the military enterprise is more resilient without linked or linear processes, spreading resources out into a web to promote survivability. The DOD's digital dependence cannot prevail with a sequential chain model and single points of failure.

A New Matrix

The cyber domain threats of tomorrow require understanding strategic shock today. Of note, the new matrix of war does not seek to supplant or undermine the importance of a superior force, whether through its C2, deployment and distribution, or weapon system technology. Instead, it merely acknowledges the DOD's digital dependence to employ these advantages, embracing a cognitive association between military depth, cyber domain capability, and strategic shock vulnerabilities. Much like the mythical Morpheus is the Greek god of dreams, the fictional character from *The Matrix* challenges military planners to see reality differently and appreciate virtual vulnerabilities. The DOD's reliance on cyber tools is like a dream, both incorporeal yet subject to influence, manipulation, and disruption. Without understanding how adversaries pursue asymmetric advantages against superior forces, the DOD cannot fully appreciate the risk it accepts through its digital dependence.

Projecting power into contested environments requires continuously examining DOD depth and thinking through operating without cyber capabilities as well. Success now requires highlighting key digital functions the military must have to operate, where cyber vulnerabilities need tactical and strategic awareness of permissiveness and freedom of maneuver. Empowered by a comprehensive discussion of global integration and interconnectedness, the American kinetic power advantage is only part of this equation for military planners. The DOD must understand how mission assurance to deliver kinetic effects is a product of securely operating in the cyber domain. To divest the two is to force an analog solution onto a digital age's problems, or as Morpheus might quip, to stay in Wonderland. The US cannot afford delusion and must acknowledge how emboldened adversaries will seek to disrupt our advantages, attacking the military's cyber depth and not necessarily its conventional forces to achieve strategic effects. Strength and speed alone do not matter within the new matrix of war.

Further discussion, research, and policy are required to move beyond the limitations of the current cognitive association. To overcome paralysis and prepare for the unexpectedness of future contested conflicts, the DOD must relentlessly pursue solutions to deter cyber threats, prevail against them, and preclude suffering from strategic shock. The new matrix urgently requires better global integration, superior cyber security and resilience, and optimized dominance with fewer resources, demanding more investment into digital tools that promote efficiency and less focus on geographic authorities. The DOD can pioneer this future out of necessity, but only as fast as it can cognitively accept its digital dependence. If the US fails to institutionally associate power projection with the digital tools it requires, the DOD may not prevail in a day without cyber. ✪

Notes

[1] Michael O. Wheeler, "The Changing Requirements of Assurance and Extended Deterrence," *Institute for Defense Analyses*, July 2010, iii–iv, http://www.dtic.mil/docs/citations/ADA550264.

[2] Maj Gen Richard Weber, USAF, and Col Mark E. Ware, USAF, "Cyberspace Mission Assurance: A New Paradigm for Operations in Cyberspace," *High Frontier* 6, no. 4, (August 2010): 3–7, http://www.dtic.mil/docs/citations/ADA549792.

[3] "Question Asked by Morpheus," *The Matrix*, directed by Lana Wachowski and Lilly Wachowski (1999; Burbank, CA: Warner Home Video, 1999), DVD.

[4] Col Clinton J. Ancker III, USA, Retired, and Lt Col Michael Flynn, USA, Retired, "Exercising Command and Control in an Era of Persistent Conflict," *army.mil*, 3 May 2010, https://www.army.mil/article/38412/exercising-command-and-control-in-an-era-of-persistent-conflict/; Eric Peltz and Marc Robbins, "Leveraging Complementary Distribution Channels for an Effective, Efficient Global Supply Chain," *RAND Corporation*, 2007, vii–x, http://www.dtic.mil/docs/citations/ADA473027; US Government Accountability Office (GAO), *Defense Acquisitions: Assessments of Selected Weapon Programs*, Report to Congressional Committees (Washington, DC: US GAO, March 2017), 5–6, http://www.dtic.mil/docs/citations/AD1032079; and Joshua T. Hartman, "Exploring the Complementary Nature of Cyber and Space Operations," *High Frontier* 6, no. 4 (August 2010): 31–34, http://www.dtic.mil/docs/citations/ADA549792.

[5] Jim Garamone, "Dunford: Command, Control Must 'Keep Pace' in 21st Century," *DoD News, Defense Media Activity*, 4 January 2016, https://www.defense.gov/News/Article/Article/639844/dunford-command-control-must-keep-pace-in-21st-century/.

[6] Joint Chiefs of Staff, "The Joint Force in a Contested and Disordered World," *The Joint Operating Environment 2035*, 14 July 2016, ii–iii, http://www.dtic.mil/docs/citations/AD1012885; and Maj Paul J. Blakesley, British Army, "Operational Shock and Complexity Theory," monograph (Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, 26 May 2005), 69–71, http://www.dtic.mil/docs/citations/ADA437516.

[7] Col Peter J. Lane, USA, "Strategic Shock: Managing the Strategic Gap," strategy research project (Carlisle Barracks, PA: Army War College, March 2013), 1–5, http://www.dtic.mil/docs/citations/ADA589203.

[8] Maj Anthony L. Marston, USA, "The Efficacy of Cognitive Shock," monograph, (Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, May 2015), 33–35, http://www.dtic.mil/get-tr-doc/pdf?AD=AD1001654.

[9] Lt Col Thomas M. Jordan, USA, "Versatility and Balance: Maintaining a Full Spectrum Force for the 21st Century," this is capped in original document Strategy Research Project, (Carlisle Barracks, PA:

Army War College, 6 April 1998), 22–24, http://www.dtic.mil/docs/citations/ADA343362; Lt Col Russell F. Miller, USA, "Developing and Retaining Information Warriors: An Imperative to Achieve Information Superiority," Strategy Research Project, (Carlisle Barracks, PA: Army War College, 29 February 2000), 2–3, http://www.dtic.mil/docs/citations/ADA377713; and Justin A. Thompson, "Improving Department of Defense Global Distribution Performance Through Network Analysis," (master's thesis, Monterey, CA: Naval Postgraduate School, June 2016), 41–42, http://www.dtic.mil/docs/citations/AD1026843.

10. Peter C. Mastro, "So Near and Yet So Far: Choices and Consequences of the Stand-In and Stand-Off Approach," (master's thesis, Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, 1 June 2015), 121–25, http://www.dtic.mil/docs/citations/AD1015800.

11. CDR Lawrence Rice, USN, "Technology's Impact on Command and Control: How Much Does the Operational Commander Need?," final report (Monterey, CA: Naval Postgraduate School, 19 May 1997), 13–14, http://www.dtic.mil/docs/citations/ADA328120.

12. Dan Shen, Genshe Chen, Jose B. Cruz Jr., Erik Blasch, and Martin Kruger, "Adapting C2 to the 21st Century: Game Theoretic Solutions to Cyber Attack and Network Defense Problems," conference paper (Rockville, MD: 12th International Command and Control Research and Technology Symposium, June 2007), 1–2, 16, http://www.dtic.mil/docs/citations/ADA481265; and Brig Gen Kurt S. Story, USA, and Peter M. Stauffer, "Delivering It to the Soldier," *High Frontier* 6, no. 4 (August 2010): 16–19, http://www.dtic.mil/docs/citations/ADA549792.

13. Lt Col Robert C. Johnson, USA, "Fighting with Fires: Decentralize Control to Increase Responsiveness," monograph, (Fort Leavenworth, KS: US Army Command and General Staff College School of Advanced Military Studies, 2001), 37–41, http://www.dtic.mil/docs/citations/ADA403795.

14. Maj Richard McGlamory, USAF, "Defense or Diplomacy? Geographic Combatant Commands," (master's thesis, School of Advanced Air and Space Studies, Air University, Maxwell, AFB, 1 June 2011), 55–56, http://www.dtic.mil/docs/citations/AD1019397.

15. Thomas Lorenzen, "The Edge of Chaos: Emergent Factors in the Information Environment," *The Strategy Bridge*, 9 May 2017, https://thestrategybridge.org/the-bridge/2017/5/9/the-edge-of-chaos-emergent-factors-in-the-information-environment; and Maj Gen Arnold Punaro, USMC, Retired, Bill Phillips, John O'Connor, and Capt Garrett Campbell, USN, "Logistics as a Competitive War Advantage," technical report (Washington, DC: Defense Business Board, 20 October 2016), 2–5, http://www.dtic.mil/docs/citations/AD1020304.

16. Marc A. Thibault, Jr., "GPS: Public Utility or Software Platform?," technical report (Monterey, CA: Naval Postgraduate School, 1 September 2016), 57–62, http://www.dtic.mil/docs/citations/AD1030085; John B. Dickens and Dean R. Dukes, "Innovative Decentralized Decision-Making Enabling Capability on Mobile Edge Devices," technical report (Monterey, CA: Naval Postgraduate School, 1 September 2015), 85–88, http://www.dtic.mil/docs/citations/AD1008918; and Col Robert L. Tremaine, USAF, Retired, "Demonstrating Cyberspace Superiority in an Acquisition World," *High Frontier* 6, no. 4 (August 2010): 62–65, http://www.dtic.mil/docs/citations/ADA549792.

17. J. B. Bartholomess, Jr., "The Issue of Attrition," journal article (Carlisle Barracks, PA: Army War College, Spring 2010), 17–18, http://www.dtic.mil/docs/citations/ADA522310; and Maj Christopher G. Williams, USA, "Fielding a Division Staff in the Modern Day," technical report (Fort Leavenworth, KS: Army Command and General Staff College, 10 June 2016, 58–61, http://www.dtic.mil/docs/citations/AD1020377.

18. Martin Libicki and Lt Gen Robert Elder, USAF, Retired, "Mission Assurance in the Face of Cyber Attacks," *High Frontier* 6, no. 4 (August 2010): 24–27, http://www.dtic.mil/docs/citations/ADA549792.

19. Lt Col William D. Bryant, USAF, "Cyberspace Superiority: Dominating the Digital Frontier," (thesis, Maxwell AFB, AL, School of Advanced Air and Space Studies: January 2014), 47–48, http://www.dtic.mil/docs/citations/ADA622182.

20. Laura J. Junor, "Managing Military Readiness," *Strategic Perspectives*, 23 Institute for National Strategic Studies, (Washington, DC: National Defense University, February 2017), 1, http://www.dtic.mil/docs/citations/AD1030355.

21. Chad DeStefano, Kurt Lachevet, and Joseph Carozzoni, "Distributed Planning in a Mixed-Initiative Environment: Collaborative Technologies for Network Centric Operations," conference paper (Rome, NY: Air Force Research Laboratory, October 2007), 20, http://www.dtic.mil/docs/citations/ADA489219.

22. George K. Baah, Thomas Hobson, Hamad Okhravi, Shannon C. Roberts, William W. Streilein, and Sophia C. Yuditskaya, "A Study of Gaps in Cyber Defense Automation," Technical Report no. 1194

(Lexington, MA: Massachusetts Institute of Technology, Lincoln Laboratory, 13 October 2016), 39–40, http://www.dtic.mil/docs/citations/AD1021685; Liang Xiong, "On Learning from Collective Data," (doctoral thesis, Carnegie Mellon University, Machine Learning Department, December 2013), 142–43, http://www.dtic.mil/docs/citations/ADA598234; and L. Richard Moore Jr., "Cognitive Model Exploration and Optimization: A New Challenge for Computational Science," conference paper (Mesa, AZ: Lockheed Martin Systems Management, Air Force Research Laboratory, Warfighter Readiness Research Laboratory, 24 March 2010), 160, http://www.dtic.mil/docs/citations/ADA553672.

23. Lt Col Shane H. Connary, USAF, "Computer Network Operations Command and Control: A New Perspective," final report (Monterey, CA: *Naval War College*, 22 October 2009), 1–3, http://www.dtic.mil/docs/citations/ADA513948.

24. Matthew Presley, "Beyond Data Services: Cloud Processing for Net-Centric Information Distribution," *High Frontier* 6, no. 4, August 2010: 57–61, http://www.dtic.mil/docs/citations/ADA549792; Andrew Miller and Rob Jansen, "Shadow-Bitcoin: Scalable Simulation via Direct Execution of Multithreaded Applications," research report (Monterey, CA: Naval Research Laboratory, 10 August 2015), 6, https://www.nrl.navy.mil/itd/chacs/sites/www.nrl.navy.mil.itd.chacs/files/pdfs/15-1231-1593.pdf; and Rodney Van Meter, "Security of Quantum Repeater Network Operation," final report (Fujsawa, Japan: Keio University, 3 October 2016), 3–5, http://www.dtic.mil/docs/citations/AD1019872.

25. Lt Gen Charles Croom, USAF, Retired, "The Cyber Kill Chain: A Foundation for a New Cyber Security Strategy," *High Frontier* 6, no. 4 (August 2010): 52–56, http://www.dtic.mil/docs/citations/ADA549792.

26. Barry R. Schneider, "Asymmetric Rivals: The Enemy Next Time," *The War Next Time: Countering Rogue States and Terrorist Armed with Chemical and Biological Weapons, 2nd edition,* ed. Schneider and Jim A. Davis (Maxwell AFB, AL: USAF Counterproliferation Center, April 2004), 1, https://www.hsdl.org/?view&did=446550.

27. Lt Col Patrick J. Obruba, USAF, "Breaking Stovepipes: Bridging Gaps in Air Force Industrial Control Systems Management to Enable Multi-Domain Mission Assurance," technical report (Maxwell AFB, AL: Air War College, 16 February 2016), iv–1, http://www.dtic.mil/docs/citations/AD1037194.

28. Michael J. McNerney, "Department of Defense and Security Cooperation: Improving Prioritization, Authorities, and Evaluations," technical report (Santa Monica, CA: RAND Office of External Affairs, 9 March 2016), 3–4, http://www.dtic.mil/docs/citations/AD1014435.

29. Maj Michael D. Pritchett, USAF, "Cyber Mission Assurance: A Guide to Reducing the Uncertainties of Operating in a Contested Cyber Environment" (master's thesis, Wright Patterson AFB, OH: Air Force Institute of Technology, 14 June 2012), 39–41, http://www.dtic.mil/docs/citations/ADA563712.

Capt Keith B. Nordquist, USAF

Captain Nordquist (BA, USAFA; MA, Embry-Riddle Aeronautical University) earned his commission in 2008 as a distinguished graduate. He is a strategic initiatives officer with the Commander's Action Group, US Transportation Command at Scott AFB, Illinois. Before his current position, he completed two assignments as a C-5 instructor aircraft commander and served in training, safety, inspection, flight command, and executive officer positions at squadron, wing, and major command levels.