(Photo by Lawrence Torres III, U.S. Army)

Master Sgt. Charlie Sanders (left) and Capt. Lashon Bush, 2nd Signal Brigade, work on a mission event synchronization list in the Joint Cyber Control Center during Operation Deuce Lightning at Grafenwoehr, Germany on 23 February 2011. A team of more than sixty U.S. and German soldiers and airmen took part in the exercise to assess the 2nd Signal Brigade's ability to provide network support.

The Relevance of Culture

Recognizing the Importance of Innovation in Cyberspace Operations

Lt. Gen. Edward C. Cardon, U.S. Army

Col. David P. McHenry, U.S. Army

Lt. Col. Christopher Cline, U.S. Army

At the October 2015 Association of the United States Army annual meeting and exposition in Washington, D.C., Army Captains Brent Chapman, Matt Hutchinson, and Erick Waage demonstrated a "cyber rifle" tool they developed in ten hours using $150 in spare parts. This tool remotely disabled an unmanned aerial vehicle.[1] Shortly after the demonstration, the captains, all assigned to the Army

Cyber Institute at West Point, New York, wrote in *War on the Rocks* that the U.S military needed an open innovation process. They opined the existing military acquisition processes are no match for current and future cyberspace threats, which create the need for the military to rapidly field innovative responses.[2]

We are in the midst of a sea change in the conduct of warfare. In the past, commanders used information to shape operations. Today, we are witnessing how information and operating environments are overlapping and, in some cases, are one and the same. In Ukraine, Russia dominated the electromagnetic spectrum, disrupting Ukrainian military communications, geolocating Ukrainian battalions with unmanned aerial vehicles, and then destroying those battalions with devastating artillery strikes.[3] Russians also shut down Ukrainian power-distributor computers and attacked phone lines to prevent customers from reporting outages.[4]

Perhaps even more important, adversaries are using social media more effectively than U.S. forces to shape public perceptions and facilitate military operations. For example, the Russian government's social media dominance has shaped what information is available to Russian citizens and where they are getting information. Similarly, the Islamic State leverages social media as a strategic weapon to shape the public narrative and to recruit and finance. Such growing use of electronic warfare, cyber warfare, and information operations in hybrid war predicates the need for valuing innovation in cyberspace operations.

The U.S. Army is losing ground daily by not leveraging the innovations of our adversaries and those of the civilian sector. The Army cyberspace community, like most, is witnessing the need for paradigm shifts in how leaders think about, advantage, and foster innovation. There is a need to relook how the Army innovates internally while leveraging industry in new ways to innovate using external solutions. The old models are outdated, and what one sees in cyberspace makes these paradigm shifts an imperative for the entire military.

As Chapman, Hutchinson, and Waage demonstrate, the Army possesses the talent that can provide the pathway to innovation. Leaders must use this internal talent to grow a culture of innovation that will ensure current and future mission success. To address the challenges of complex and continually evolving information and operating environments, we must examine many of our own paradigms for how we address innovation across the force.

Innovation Defined

In November 2014, then Secretary of Defense Chuck Hagel announced the Defense Innovation Initiative to highlight the Department of Defense's (DOD's) need to adopt innovative practices and means of operating in increasingly contested environments. Hagel noted, "We are entering an era where American dominance in key warfighting domains is eroding, and we must find new and creative ways to sustain, and in some areas expand, our advantages even as we deal with more limited resources."[5] Current Secretary of Defense Ash Carter has sustained the momentum. DOD continues to expand cooperative efforts with Silicon Valley through initiatives such as Defense Innovation Unit–Experimental (DIUx) that seek to build and strengthen relationships with new and existing innovators.[6] In doing so, the secretary highlights that many military innovations can and should come from our industry partners.

In many ways, innovation has become a nebulous term that describes all things new from automobiles to mattresses. Innovation is simply anything novel and useful that one implements. Geoffrey A. Moore describes *application innovation* as "creating differentiation by finding and exploiting a new application or use for an existing technology."[7] Meanwhile, Elaine Dundon speaks of "the profitable implementation of strategic creativity."[8] For cyberspace operations, we offer the following definition of innovation: the implementation and integration of new concepts, processes, and material that enhance mission capability. Organizations can enhance innovation through collaboration, flexibility, creativity, and resourcing.

Innovation in Cyberspace

The mercurial nature of cyberspace presents a number of novel challenges to the warfighter. A constant influx of emerging technologies, practices, and techniques define the information and operating environments. The time between acquisition and obsolescence adds to this complexity. Threats come from highly capable and resourced nation-state actors, terrorist and criminal organizations and individuals, and hacktivists. The cost barriers to entry continue to decline for adversaries: a successful hack only has to be right once; a capable defense has to be right 100 percent of the time.

Unlike in conventional war, the United States does not have a monopoly on the means to conduct cyberspace operations. This requires the military community to assess honestly its strengths and vulnerabilities when it comes to offense and defense. The Army needs to approach the information environment with the recognition that innovative solutions may be both external and internal.

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

A soldier assigned to the 780th Military Intelligence Brigade on Fort Meade, Maryland, sets up low-level voice intercept equipment 21 October 2015 during a cyber integration exercise on Joint Base Lewis-McChord, Washington.

While military innovation always played a role in the advancement of warfighting, institutional headquarters often struggled to incorporate and support tactical innovations. In many instances, this results in looking outward for innovations and adopting them for internal use through a top-down approach. Within the military, leaders tend to favor the initiatives of a select few at the top, often regardless of expertise, rather than those of the population at large. However, the DOD needs innovations introduced by individuals—a bottom-up approach—to maintain the initiative in dynamic information and operating environments.

To affect operations, the cyberspace community must challenge the military norms and become a community with the resources, embraced values, and behavior that promote an innovative mindset and ability to evolve. A culture of innovation views new thinking and experimentation that address operational, procedural, technical, and other challenges influencing cyberspace operations as the norm.

The Innovation Imperative

Addressing cyberspace challenges by responding to the innovation imperative requires leaders to adopt a culture that fosters and rewards innovative practices. Without leader emphasis, innovation initiatives will fail. Retired Gen. Stanley McChrystal recounts in *Team of Teams* how he realized that he needed a different leadership style to defeat a highly adaptable enemy. Rather than serve as a "chess master" and drive outcomes through top-driven decision-making, McChrystal took on the role of a "gardener" and focused on shaping the ecosystem.[9] McChrystal describes how he shaped culture by example and continuously driving the narrative.[10] Like McChrystal, to shape a culture that propels

(Photo courtesy of U.S. Army)

A soldier with the 780th Military Intelligence Brigade conducts cyber support operations through improvised use of commercial, off-the-shelf equipment 24 January 2016 during a training rotation for the 2nd Stryker Brigade Combat Team, 2nd Infantry Division, at the National Training Center, Fort Irwin, California.

cyberspace operations forward, leaders must value empowerment, collaboration, and adaptability.

Good ideas are not reserved to a particular rank or stature. The "gardener" leadership direction McChrystal took relied on trust throughout the command and mirrored several tenets of mission command by recognizing the importance of empowering agile and adaptive leaders.[11]

Like a gardener, leaders can set the conditions by watering and weeding, but they cannot make the plant grow. Leaders must inspire creativity, idea generation and sharing, and initiative in their subordinates while encouraging them to take risks based on their ideas.[12] Leaders must avoid impediments to creativity simply out of fear of taking risks based on others' novel ideas. It is not enough for leaders to proclaim that the workforce should share ideas and not fear failure. Leaders must ensure that systems and resources are in place to enable idea sharing and to underwrite some failures.[13]

A crowdsourcing website together with challenge-based innovation offers a way to enable idea sharing. Members of a command can share and vote for ideas. Leadership can then select and implement those they deem likely to enhance operations. Leaders must be active participants. At U.S. Army Cyber Command and Second Army, crowdsourcing is one way to show innovation as congruent with the organization's mission. Team members are also able to pitch their ideas directly to the command's leadership through a *Shark Tank*-style resource-investment panel.[14]

While a need exists to take advantage of internal innovation, there is an equal requirement to look outward to build innovative proficiencies. There is a need to learn from others' innovation. The cyberspace community must continue developing relationships with academia and industry to expand innovation opportunities. We need these outside perspectives and partner activities as we continue to confront unforeseen challenges in cyberspace. The Army's proposed *engagement warfighting function* reinforces that future operational challenges are too numerous and complex for U.S military and civilian agencies to address alone.[15]

Government and industry are acknowledging the importance of Silicon Valley and the startup community in not going it alone. For example, the March 2016 appointment of Google Chief Executive Officer Eric Schmidt to head the Defense Innovation Advisory Board, the appointment of tech entrepreneur Chris Lynch to head the Pentagon's Defense Digital Service, and the establishment of DIUx coopt the talent and knowledge of Silicon Valley to serve the DOD.[16] U.S. Army Cyber Command

and Second Army launched the Silicon Valley Innovation Pilot program and participate in Stanford University's *Hacking4Defense* program.[17] Proctor and Gamble's Connect and Develop program offers an example from industry. That program allows the company to collaborate with organizations and individuals around the world to systematically search for technologies, packages, and products it can improve, scale up, and market on its own or together with other companies.[18]

Cyberspace's volatile nature and its rapid turnover of technology and practices require a flexible and adaptable cyber force. As the Army addresses ongoing and future operational challenges, cyberspace operations' role will increase at all levels of warfare. Cyberspace is becoming inextricably linked to land dominance. As evidenced in Ukraine, tactical applications of cyber effects will become the norm, with cyber capabilities integrating with maneuver and mission command. We must learn from ongoing conflicts that highlight the emerging challenges of cyberspace operations, information operations, and electronic warfare. We must then apply these lessons in our policies and doctrine, and at our combat training centers.

Many in industry, along with McChrystal, have learned the futility of five-year strategic plans in dynamic environments accentuated with uncertainty. To combat this, they seek adaptive advantage. Units such as the 780th Military Intelligence Brigade and the U.S. Army Cyber Protection Brigade—where teams are at the forefront of our ongoing cyberspace operations—are already making strides. Their continual integration into combat training center rotations is allowing cyber teams to act on change while experimenting rapidly not only with equipment and services but also with models, processes, and strategies.

The "cyber rifle" tool fabrication demonstrates that empowered individuals working collaboratively will find adaptable solutions to operational problems. Commanders must emplace a network of systems and processes to facilitate the ingenuity of these rapid innovations as they lead to adaptation. Organizing for adaptation is how we will take advantage of the emergent characteristics of cyberspace. Empowered cyber teams are the answer to adapting to this operational challenge.

Conclusion

The increasing overlap of information and operating environments requires the Army to rethink how it addresses innovation to address the Army's operational challenges. Paradigms are shifting. Future dominance on land depends largely on how successful we are in cyberspace operations. To ensure dominance, leaders must prioritize innovation and create the conditions where innovation can thrive. The Army must reframe how it leverages external innovation while also fostering the promise of internal innovators in the force. The Army must make these changes if we are to remain relevant and ready to face our adversaries in both the land and cyber domain. ■

Biographies

Lt. Gen. Edward C. Cardon, U.S. Army, is the commanding general of U.S. Army Cyber Command and Second Army. He holds a bachelor's degree from the U.S. Military Academy, and master's degrees from the National War College and the U.S. Naval Command and Staff College. His previous assignments include commanding general of the 2nd Infantry Division; deputy commandant of the U.S. Army Command and General Staff College; and deputy commanding general (support) for 3rd Infantry Division.

Col. David P. McHenry, U.S. Army, is the G5 of U.S. Army Cyber Command and Second Army. He holds a BA from the University of Northern Colorado and two MAs from the School of Advanced Military Studies, Fort Leavenworth, Kansas. He has served in the Pentagon and deployed to Iraq.

Lt. Col. Christopher Cline, U.S. Army, is an Army strategist assigned to U.S. Army Cyber Command and Second Army. He holds a BS from the U.S. Military Academy, an MPhil from the U.S. Air Force Air University School of Advanced Air and Space Studies, and an MIA from Texas A&M University. His previous assignments include strategic planner for Eighth Army and regional commander at the Directorate of Admissions at West Point. ***Cline is the principal author of this article.***

Notes

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

2. Ibid.

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

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

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

6. Maureen Schumann, "Defense Innovation Unit–Experimental (DIUx): Silicon Valley," fact sheet, n.d., accessed 17 May 2016, http://www.defenseinnovationmarketplace.mil/resources/2015828_DIUx-FactSheet.pdf.

7. Geoffrey A. Moore, "Darwin's Dictionary," Dealing with Darwin website, accessed 17 May 2016, http://www.dealingwithdarwin.com/theBook/darwinDictionary.php#Innovationtypes.

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

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

10. Ibid.

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

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

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

14. "Shark Tank," ABC website, accessed 17 May 2016, http://abc.go.com/shows/shark-tank. *Shark Tank* is a television show that features "people from all walks of life" pitching entrepreneurial ideas to a panel of "tough, self-made, multi-millionaire, and billionaire tycoons" with a goal of securing their investment.

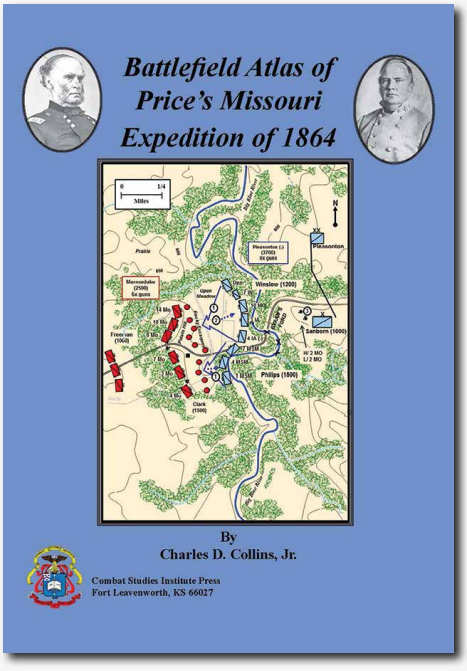
15. U.S. Army Training and Doctrine Command (TRADOC) Pamphlet 525-8-5, *The U.S. Army Functional Concept for Engagement* (Fort Eustis, VA: TRADOC, 24 February 2014), 10.

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

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

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

MR We Recommend



The Combat Studies Institute announces publication of *Battlefield Atlas of Price's Missouri Expedition of 1864* by Charles D. Collins Jr. It is a faithful rendering in maps of official records pertaining to the Price Expedition, the last great Confederate effort west of the Mississippi to turn the tide of the Civil War. However, it also incorporates original research that corrects some historical inaccuracies pertaining to the series of events in the expedition. As such, it is the best available tool to facilitate an understanding of the raid, especially as an aid for those who may have the opportunity to walk the ground of the major engagements.

http://usacac.army.mil/sites/default/files/documents/cace/CSI/CSIPubs/Prices_Missouri_Expedition_web.pdf