When the Screens Go Dark: Rethinking Our Dependence on Digital Systems

By Marc Lindemann
Journal Article | Mar 2 2015 - 3:47pm

Despite its name, the U.S. Army’s Command Post of the Future (“CPOF”) is now more than ten years old. Since CPOF’s introduction, the U.S. Army has fielded multiple upgrades to it and to the digital systems that have constituted the Army Battle Command System (“ABCS”). While this succession of improvements has added functionality to the digital systems themselves, the hidden costs of these sophisticated technologies threaten to undermine the very warfighting functions that they were intended to facilitate. Without proper precautions, the weight of a unit’s digital architecture can crush that unit’s ability to conduct operations. Likewise, emerging cyber and electromagnetic threats that can degrade networked digital systems make excessive dependence on such systems an acute vulnerability. Ever-increasing digital-system complexity requires units to allocate more resources to master ABCS intricacies at the expense of other objectives, such as the conduct of traditional – now often characterized as “degraded” – operations. The less time a unit spends on non-digital training, the more dependent the unit’s operations become on its digital systems. When these systems fail, however, the drawbacks of an increasingly exclusive focus on digital-systems training – and the associated sacrifice of traditional training – become readily apparent. Thus, paradoxically, the more advanced the U.S. Army’s digital systems become, the more U.S. Army leaders will need to consciously and continuously emphasize non-digital fundamentals. The availability of technology is no substitute for the tactical training of Soldiers.

The Costs of Digitization

In 1994, as part of the Force XXI modernization initiative, the U.S. Army designated the 4th Infantry Division (Mechanized) (“4ID”) as its Experimental Force. At Fort Hood, Texas, the 4ID trained on the precursors to many of the digital systems that are present in today’s ABCS, and, in 1999, the U.S. Army hailed the 4ID as its “First Digital Division.” As the 4ID was adapting to these digital systems, the U.S. Army Research Institute for the Behavioral and Social Sciences (“ARI”) simultaneously embarked upon a study entitled, “Managing Force XXI Change: Insights and Lessons Learned in the Army’s First Digital Division,” to chronicle the 4ID’s progress. The ARI researchers noted that the transition to digital systems was not without its difficulties. At least one commander within the 4ID went so far as to ban paper maps from his Tactical Operations Center (“TOC”) to force his Soldiers to rely solely on digital versions. In its March 2002 closing report, the ARI team cited many leaders who gave the digital systems favorable reviews; still, the report featured some prophetic warnings: “Digital leaders and soldiers must be warfighters first. They need to master warfighting basics before they can harness digital tools.” Quoting the 4ID’s COL Ted Kostich, the report also noted: “We need to be careful that we don’t make
our ABCS operators technicians instead of warfighters.”[9]

Since the 2002 ARI Report, ABCS, in the hands of trained operators and supervisors, has effectively reduced the fog of war. For example, a commander and his staff no longer have to depend exclusively on subordinate units calling up their positions over the radio; Force XXI Battle Command Brigade-and-Below/Blue Force Trackers (“FBCB2s/BFTs”) regularly transmit unit locations, displaying corresponding unit icons that move through the battlespace in the Common Operating Picture (“COP”).[10] A swarm of blue icons marching across a CPOF screen is an impressive sight. With the timely influx of situational information, leaders at all levels can integrate and synchronize battlefield activities, making ABCS a significant combat multiplier.[11] Given the success of its digitization, the U.S. Army has committed itself to the further expansion of its systems and networks. As the digital environment becomes more complex, however, today’s leaders must take a hard look at the challenges inherent in their current reliance on these systems.

Information demands an audience, and the sheer volume of data available through ABCS can be daunting. [12] The accessibility of information creates a perceived obligation to observe and process it, resulting in a danger of what GEN Martin E. Dempsey, Chairman of the Joint Chiefs of Staff, has termed “paralysis by analysis.”[13] In a TOC, the stream of near-real-time position and spot reports results in constant monitoring to guarantee responsiveness. As more information comes in, a unit assigns more resources to observe the information and analyze its meaning. In addition, though the ABCS provides powerful tools to evaluate, reconfigure, and package data, the crafting of detailed storyboards and CPOF-based update briefs requires time and trained personnel. With more Soldiers becoming necessary to mind and process the data flow, a unit must devote more assets to handle the incoming information.

Yet digital systems cannot do anything if they are not connected properly. What the 2002 ARI report recognized is still true: “[t]he signal battalion has become the Achilles heel of digital operations. Maintaining digital networks and connectivity depends absolutely on signal capabilities. The impact of digital failures during distributed combat operations could be harsh.”[14] Today’s ABCS operators – and even senior leaders[15] – often have to stand aside and wait for signal personnel to painstakingly connect all of the digital systems in a command post or TOC. Many Soldiers defer to signal personnel as the priesthood of the U.S. Army’s digital systems; somehow, after tinkering with wires and pressing various buttons, the signal Soldiers are mysteriously able to elicit functionality. The prospect of digital failure is so unwelcome that commanders may be tempted to keep their command post location static once the signal personnel have established some degree of connectivity and digital capability. Typically, the larger its digital footprint, the more immobile a command post will be. Likewise, the digital logistics and signal support necessary to even push out a tactical command post can seem overwhelming. Each move involves the transport of a multitude of computer equipment, as well as the reconfiguration of digital systems to establish connectivity. Sometimes, too, uniformed signal personnel hit a road block in their efforts, and a digital system is out of the fight until a contractor’s field service representative can arrive. And once the digital systems are functioning, there remains the matter of the proficiency of the people who will be operating them.

In order to use ABCS systems, a unit must allocate sufficient personnel to serve as operators, and each operator requires extensive initial and regular refresher training to keep his skills current. In an era of diminished budgets and multiplying training requirements, finding the resources for such training can be difficult.[16] Moreover, relatively junior operators are not the only ones who need training. A trained, low-level operator may sit in front of a CPOF console, monitoring reports and icon positions, but when it comes time for a staff principal to check his section’s running estimates or to brief a commander using CPOF, that staff member must also know how to use the device. If a staff section relies upon a digital
system, the operators and the principals must be subject matter experts in that system’s use. Unfortunately, the turnover in headquarters personnel – especially junior personnel who will move out to line units – ensures that many digital system operators leave their positions just as they are nearing some level of expertise with their assigned devices.[17]

The rapid succession of upgrades, updates, and other ostensible ABCS improvements results in still more challenges. Military contractors such as General Dynamics and Raytheon repeatedly roll out updates providing additional functionality to the existing digital systems that they produce; sometimes, such as the case with BCS3, the military incorporates entirely new systems into ABCS. Each update may involve additional training for operators and principals.[18] These subsequent versions can also bring what is known as “feature creep”: to distinguish a new version from its predecessors, a digital system’s creator adds functionality. With each version, the “functionalities” of the system multiply, eventually resulting in a system that few Soldiers fully understand and whose primary function is clouded with “gee-whiz” features that are of little practical use.

The steady procession of digital system versions also brings with it a dependence upon an array of contractors to implement these improvements.[19] Operators may undergo an initial 40-hour block of instruction regarding a particular digital system, but there are few operator-level fixes possible when there needs to be an update to the device itself. Operations can slow to a crawl when a digital system goes down and a field service representative has to arrive to install an update. Sometimes a unit will not know that it needs a necessary update until it boots up its system and discovers that the system does not work or cannot “talk” with another system. Military contractors provide valuable services, but there is a problem if uniformed operators and their supervisors do not have the ability to troubleshoot and fix the most basic issues with their “primary weapons systems,” other than by turning off and on the power switch and hoping for the best. Increasing ABCS complexity, the need for communication between digital devices, and a growing emphasis on jointness and interoperability between different services’ systems has resulted in the permanent presence of contractors in waiting. The constant need for these contractors detracts from a command post’s agility and mobility.

Whereas contractor field service representatives and signal Soldiers have seen their stock soar in the past 12 years, analog maps have become a casualty of the U.S. Army’s reliance upon digital systems.[20] Before the advent of ABCS, Soldiers would regularly update a TOC situation map’s acetate overlays. Now, with no way for an analog situation map to compete with the near-real-time data feed from ABCS, making analog updates takes a back seat to monitoring computers. In a conclusion that will resonate with today’s battalion and higher headquarters staff members, the 2002 ARI report remarked that “[t]he division is not manned to conduct operations using both digital and analog (map-and-grease-pencil) systems.”[21] The 4ID’s leaders acknowledged that they had to break with traditional, analog mission command procedures in order to tend the TOC’s digital systems; in the words of one officer, “I don’t have enough people to be inside the TOC working ASAS and then running outside the track and changing the analog stuff on the maps and wingboards.”[22]

Today, training for degraded operations is too often an afterthought. Units struggle so much with setting up, connecting, and operating the latest digital systems that there is little time left to train on how to operate when these systems are not available.[23] The tendency is for units to concentrate on digital training at the expense of analog proficiency, as the skills required for the successful use of ABCS are particularly perishable. As the 2002 ARI report had noted:
Balancing digital training with field craft and tactical training is a challenge unique to the digital division. Because information management skills atrophy more quickly than other skills, units are likely to devote more time to digital training.[24]

These days, in TOCs full of glowing CPOF screens, analog situation maps – when posted – fall into various stages of neglect and obsolescence. Likewise, hard copies of current staff running estimates may be hard to find, as well-meaning leaders attempt to enforce a “paperless TOC” model. The higher the headquarters, the less likely there will be an analog back up of information from subordinate elements. Granted, analog products are inefficient, time-intensive, and relatively limited in terms of the data they display; they are also vital to have on hand when digital systems are not working. Without the presence and regular updating of these analog products, mission failure may be just a power outage or a system crash away.

Regardless of how technologically savvy a commander may be, ABCS provides a sweeping situational awareness that also serves as a tempting opportunity for higher headquarters’ micromanagement, what GEN Dempsey has recognized as “a debilitating inhibitor of trust in the lower echelon of the force.”[25] The packaging of volumes of data into simple icons creates visibility with the suggestion of manipulability. Excessive interference with subordinate unit operations becomes a real danger: if a commander can see something on the screen, then it appears deceptively simple to control it.[26] Some studies have even developed the term “Predator View” for a leader who becomes so caught up with what is on the screen that he fails to see the larger tactical picture.[27] A senior leader who thus becomes enmeshed in the details of an operation at the lowest tactical level is not doing his job and is not allowing his subordinate leaders to do theirs. Digital systems’ invitation to micromanagement also manifests itself in the opposite direction. Although junior leaders do not have to constantly call up to higher headquarters with their positions and give minute-by-minute radio reports of their progress, their FBCB2s/BFTs effectively and automatically provide that stream of information. Junior leaders know that their movements are being tracked and expect higher headquarters to regularly monitor their position and status. This umbilical cord to higher headquarters results in an expectation of constant communication and oversight; moreover, additional guidance is only a free-text message away. This tendency plays out above the small unit level, as well. Digital networks allow for the easy dissemination of Fragmentary Orders (“FRAGORDs”). Without restraint, a flurry of FRAGORDs bombarding a subordinate headquarters’ in-boxes can lead to the same sort of micromanagement problems and initiative-deadening expectations as described above.

Going Forward

The U.S. Army’s current path, with its emphasis on joint and multinational operations[28], will ultimately require the integration and interoperability of other services’ and various nations’ digital systems.[29] In the foreseeable future, the digital architecture will become more, not less, complicated, as the U.S. Army attempts to digitally connect headquarters, Soldiers, and vehicles[30] across services and across nations. Every step closer to this goal involves the investment of additional funds, personnel, and training resources, along with the consequent opportunity cost in traditional tactical training. Today, facing budget cuts, some military leaders are promoting digital systems as a means of cutting training and personnel. LTG Susan Lawrence, the U.S. Army’s Chief Information Officer/G-6, announced on 27 June 2013, “I’m convinced that, as we draw down, if we get this network modernized right, it will enable us to be that smaller, better-trained, more capable expeditionary Army.”[31] When hearing these arguments, it is important to remember that digital systems and networks were a means to an end, not an end unto themselves.
The U.S. Army cannot pin all of its hopes upon its digital systems; such thinking is dangerously akin to treating the network as the country’s Maginot Line. The U.S. Army is rightly investing in the creation of cyber warriors to protect against and repel attacks to its digital systems. Protecting the digital dominance that we have obtained goes hand in hand with the use of these systems. Merely attempting to harden our digital systems – increasing our defenses – is not enough, however. The U.S. Army must train for situations in which its digital systems, by accident or design, are not functional.

In trying to refocus on the operations that digital systems were designed to facilitate, the concept of decentralization provides a useful prism through which leaders can view the demands of current and future digital complexity. Recent Unified Land Operations and Mission Command doctrine has reaffirmed the significance of decentralization and expanded its applicability. There is an inherent conflict between networking and decentralization, however. The more an organization is networked, the more reliant it becomes on the center – the hub or the brain – of the network. It is important to remember that the U.S. Army originally embarked upon its networking program in order to facilitate point-to-point control between commanders and subordinates.

Disciplined initiative is the key to non-digital operations in a military force that now prioritizes networked, digital operations. In a threat environment where even the most useful digital system may be knocked out of the fight, there needs to be a back-to-basics approach that will enable units to continue to fight effectively in the absence of their digital systems and digital guidance from higher headquarters. Every commander should be able to shut off the TOC’s power, slipping the digital leash, and have confidence that his or her unit can continue to function. Junior leaders and staff sections should be able to anticipate the problems inherent in digital-system failure and know what to do without a major disruption in TOC operations. ADRP 6-0’s non-digital solutions – “establishing trust, creating shared understanding, or providing a clear intent using mission orders” – are significant. More significant, however, and more measurable is the degree of Soldiers’ basic proficiency in their warfighting tasks.

**Conclusion**

Although this paper does not and cannot advocate the abandonment of the U.S. Army’s existing digital systems, the U.S Army’s dependence on digital systems is very much on its leaders’ minds today. These systems have repeatedly demonstrated the potential to make the U.S. Army a much more efficient and lethal fighting force. Before his retirement, however, GEN Robert W. Cone, then Commanding General, U.S. Army Training and Doctrine Command, gave digital systems an ultimatum: “Why do we want this piece of technology? If it does not dramatically improve training efficiency, we need the strength to walk away.” Right now, the military is poised to increase digital training requirements in pursuit of inter-service operations, multinational activities, and the expansion of the network to include all Soldiers and vehicles. Leaders at every level must understand their dependence on digital systems, successfully manage their units’ use of these systems, and promote decentralized initiative in support of clearly defined and mutually understood tactical goals. In the end, Soldiers must have tactical knowledge that transcends anything displayed on a computer monitor. Soldiers, not our digital systems, are what will win our future conflicts.

**End Notes**


[7] “Forceful steps may be needed to jump-start digitization. For example, a brigade commander in the 4ID banned the use of paper maps in command posts to force leaders and soldiers to use the new digital systems. The commander later credited that step for much of his unit's digitization success.” Ibid., 29.

[8] Ibid., 32.

“Commanders rely on technical networks to communicate information and control forces. Technical networks facilitate information flow by connecting information users and information producers and enable effective and efficient information flow. Technical networks help shape and influence operations by getting information to decisionmakers, with adequate context, enabling them to make better decisions. They also assist commanders in projecting their decisions across the force.” ADRP 6-0, 3-28.

“Information becomes a force multiplier when it provides a capability that, when added to and employed by a combat force, significantly increases the combat potential of that force and enhances the probability of successful mission accomplishment.” AR 25-1, 1-7.

“Electronic means of communication have increased the access to and speed of finding information. However, they also have increased the volume of information and the potential for misinformation. Successful commanders are mindful of this when they configure their mission command system. Commanders determine information requirements and set information priorities. They avoid requesting too much information, which decreases the staff’s chances of obtaining the right information.” ADRP 6-0, 2-83.


Leibrecht et al., 40.

“In the military, concepts such as Information Operations and Network Centric Warfare rely on complex information systems that utilize global computer networks. Until 2009, most requirements and decisions on network security and capability were made by communications experts, especially in the military. However, as dependence on this vulnerable network increases, commanders must be directly involved because of the great operational impact of network failure or degradation. There is concern that many senior leaders are being thrust into an area for which they are poorly equipped due to lack of cyberspace education or experience.” William Waddell with David Smith, James Shufelt, and COL Jeffrey Caton, “Cyberspace Operations: What Senior Leaders Need to Know About Cyberspace,” Center for Strategic Leadership Study 1-11, March 2011, 1, available at <http://www.csl.army.mil/usacsl/publications/CSLStudy_1_11_CompleteReportWithCovers.pdf> (14 May 2014).

“While advances in the science of human learning and training help us train soldiers faster, the truth is that it can barely keep up with the expanding list of training requirements.” GEN Robert W. Cone, “Building the New Culture of Training.” Military Review, January-February 2013, 14, available at <http://tboc.army.mil/MilitaryReview_20130228_art005.pdf>


For example: AFATDS, Raytheon; AMDWS, Northrup Grumman; FBCB2, Northrup Grumman; BCS3, Boeing subsidiary Tapestry; CPOF, General Dynamics; and TAIS, General Dynamics.

Hard copies of field manuals have also fallen victim to digitization. Too often, though, leaders will put copies of U.S. Army publications on disc and then, when the power goes out, are unable to access the necessary reference material.

Leibrecht et al., 40.

Ibid. (quoting COL Bob Cone, 02 March 2001).


Leibrecht et al., 41.

Dempsey, 7.


“The long-term goal is to integrate these [Mission Command Training Program (‘MCTP’)] corps and division multi-echelon [Warfighter Exercises] with Global Combatant Command exercises. This will
increase the Joint-Interagency-Intergovernmental-Multinational component and provide high-payoff training opportunities for Special Operations Forces, multinational partners, and our United Action Joint partners that enable operational level headquarters to tie tactical capabilities to regional or national strategies. . . . Tied to this are plans for NATO partners to participate habitually in future U.S. corps and division WFXs. Overall, MCTP’s transformed exercise architecture and OCT initiatives will ensure operational level HQs can train in a much more relevant, realistic, and complex environment than previously possible, with all the required enablers to fully train commanders and staffs.” COL Michael Barbee, “The CTC Program: Leading the March into the Future,” Military Review, July-August 2013, 21 available at <http://usacac.army.mil/cac2/cac-t/Repository/MilitaryReview_20130831_art006.pdf> (14 May 2014).

[29]. “The term ‘network-enabled capabilities’ requires some explanation. The term means the use of network technologies and information technology assets to facilitate cooperation and information sharing. This can lead to a build-up of complex and ad hoc multinational environments, referred to as network-enabled capabilities or network enabled operations. Network enabled capabilities have the potential for increasing military effects through improved use of information technology systems.” van Burken, 40.


[32]. “Commanders enable adaptive forces through flexibility, collaborative planning, and decentralized execution. They use mission command to achieve maximum flexibility and foster individual initiative.” ADP 3-0, Unified Land Operations, 10 October 2011, 7, available at <http://usarmy.vo.llnwd.net/e2/rv5_downloads/info/references/ADP_3-0_ULO_Oct_2011_APD.pdf> (14 May 2014); see also Dempsey, 3-4 (“Smaller, lighter forces operating in an environment of increased uncertainty, complexity and competitiveness will require freedom of action to develop the situation and rapidly exploit opportunities. Decentralization will occur beyond current comfort levels and habits of practice.”); ADRP 6-0, 2-86.


[34]. Recent training simulations, such as that with the 2nd Brigade Combat Team, 82nd Airborne Division, in October 2012 at the Joint Readiness Training Center at Fort Polk, Louisiana, have involved “significant communications challenges involving either austere and immature infrastructures or sophisticated area-denial electronic and cyber attack from our adversaries.” Flynn and Richardson, 40. In addition, these challenges have forced units undergoing evaluation to “practice the skills needed when communications are degraded, and then navigate through the challenges of establishing digital connectivity across [multiple] battalion task forces—all under free-play enemy action, including electronic jamming and military cyber attack.” Ibid.

[35]. “Successful commanders understand that networks may be degraded during operations. They
develop methods and measures to mitigate the impact of degraded networks. This may be through exploiting the potential of technology or through establishing trust, creating shared understanding, or providing a clear intent using mission orders.” ADRP 6-0, 3-48.

[36]. Ibid.

[37]. At an 18 June 2013 symposium at Fort Leavenworth, Kansas, BG James E. Rainey, director of the Mission Command Center of Excellence, announced the new Army Mission Command Strategy. Rainey received the question whether “units were relying too much on technology in order to execute Mission Command,” he and replied that “units have to plan on the possibility that the enemy will have the capability of temporarily neutralizing our technological systems.” In particular, he commented, “Mission Command set us up for success when we temporarily lose those systems.” Another symposium participant, Maj. Gen. Jeffrey L. Bailey, deputy chief of staff, G-3, U.S. Army Forces Command, indicated that the U.S. Army was “requiring units to operate in degraded technological environments to ensure units are not becoming overly reliant on technology.” LTC Jeff Allen, “Leaders Discuss Mission Command Strategy,” Combined Arms Center, 27 June 2013, available at <http://www.ftleavenworthlamp.com/article/20130627/NEWS/130629309> (14 May 2013).

[38]. “Information systems — especially when integrated into a coherent, reliable network — enable extensive information sharing, collaborative planning, execution, and assessment that promote shared understanding.” ADRP 6-0, 3-49.

[39]. Cone, 15.

[40]. “The truth is that the most agile, adaptive, intelligent system on the battlefield or anywhere else in our Army is a human being. We will spend billions of dollars researching how to improve the network, but it will mean little if we don’t focus our energies on command climates and environments that develop the human foundation—trust, initiative, dialogue and freedom of action within intent—that will allow mission command to thrive throughout our Army and our institutions to become as agile as our operating forces.” COL Tom Guthrie, “Mission Command: Do We Have the Stomach for What is Really Required?” Army, June 2012, 28.

About the Author

Marc Lindemann

Major Marc Lindemann is currently serving as Battalion Executive Officer for the 1-258th Field Artillery Battalion of the New York Army National Guard, as well as a Principal Assistant District Attorney in the Suffolk County District Attorney’s Office. He deployed to Central Iraq in 2005-2006 as a platoon leader in the 4th Infantry Division. Major Lindemann received his bachelor’s and master’s degrees in history at Yale University and holds a J.D. from Harvard Law School. The views and opinions expressed here are the author’s alone and do not necessarily reflect those of the U.S. Army, Department of Defense, or any U.S. government agency.

Links:

Copyright © 2015, Small Wars Foundation.

Select uses allowed by Creative Commons BY-NC-SA 3.0 license per our Terms of Use.
Please help us support the Small Wars Community.