2018 Award Winner
USAWC Student Awards Program

Selected for publication in *The Army War College Review*

The Impact of Army Culture on LandWarNet Operations

by

Lieutenant Colonel Jason Hester
United States Army

Under the Direction of:
Colonel Doug Orsi

United States Army War College
Class of 2018

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
01-04-2018	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
The Impact of Army Culture on LandWarNet Operations

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Jason Hester
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Doug Orsi

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College, 122 Forbes Avenue, Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Approved for Public Release. Distribution is Unlimited.

13. SUPPLEMENTARY NOTES
Word Count: 5,981

14. ABSTRACT

The Army relies upon Information Technology and its LandWarNet for virtually all operations. This reliance and the designation of cyberspace as a warfighting domain presents the reality that every soldier is an operator in the domain. The result is a unique and dangerous phenomenon, where the domain is not thoroughly understood by soldiers and leaders alike. Failure to effectively manage this critical resource is at best a lost opportunity to leverage LandWarNet for maximum strategic effect. At worst, it leaves this critical infrastructure unnecessarily vulnerable to failure and/or attack. An assessment of Army culture and signal subculture shows that they must be changed to adapt to the unique management and operation requirements of LandWarNet. The Army should create a culture of more candid assessment within the signal community and its dialogue with mission commanders, increase the value placed upon intellectualism, and increase the value placed on signal strategic planning competencies. Left unchanged, the status quo cultural challenges result in frustration, failed expectations, inefficiencies, flawed planning, and critical performance gaps in the operation of LandWarNet in support of Army forces.

15. SUBJECT TERMS
IT, Cyberspace, Subculture, Anti-Intellectualism, Embedding Mechanisms, Culture Change

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(w/ area code)*
UU	UU	UU	UU	29	

The Impact of Army Culture on LandWarNet Operations

(5,981 words)

Abstract

The Army relies upon Information Technology and its LandWarNet for virtually all operations. This reliance and the designation of cyberspace as a warfighting domain presents the reality that every soldier is an operator in the domain. The result is a unique and dangerous phenomenon, where the domain is not thoroughly understood by soldiers and leaders alike. Failure to effectively manage this critical resource is at best a lost opportunity to leverage LandWarNet for maximum strategic effect. At worst, it leaves this critical infrastructure unnecessarily vulnerable to failure and/or attack. An assessment of Army culture and signal subculture shows that they must be changed to adapt to the unique management and operation requirements of LandWarNet. The Army should create a culture of more candid assessment within the signal community and its dialogue with mission commanders, increase the value placed upon intellectualism, and increase the value placed on signal strategic planning competencies. Left unchanged, the status quo cultural challenges result in frustration, failed expectations, inefficiencies, flawed planning, and critical performance gaps in the operation of LandWarNet in support of Army forces.

The Impact of Army Culture on LandWarNet Operations

> The ultimate objective is to empower Soldiers and decision makers with the information and tools they need to execute their missions as effectively and efficiently as possible. A ready, network-enabled Army is key to winning in a complex world.
>
> —Lieutenant General Robert Ferrell,
> Former Army Chief Information Officer[1]

Information Technology (IT) has become increasingly pervasive in Army operations in past decades. The present-day Army IT infrastructure, termed LandWarNet, represents a critical resource at all echelons.[2] The Army relies upon it for virtually all administrative actions, activity in the operational and strategic spectrums, and even in some degree, the tactical realm. During the evolution of this reliance on LandWarNet, the Department of Defense (DOD) has identified cyberspace as the newest warfighting domain.[3] In doing so, DOD specifically acknowledged the extent to which all Army operations depend upon the domain.

The combination of the Army's heavy reliance on LandWarNet and the designation of cyberspace as a distinct warfighting domain presents the reality that every soldier (or user) is effectively an operator in the domain. In this sense, any user has the potential to impact operations. The impact can be strategic, as seen in the widespread breach of United States (U.S.) military computers originating from malicious code in the flash drive of a single user in 2008.[4] There also remains the ever-present challenge that the technical nature of this space includes terminology, concepts and entire support organizations that typical mission commanders and other senior leaders do not readily understand. The result is an arguably unique and dangerous phenomenon. Every soldier is an operator in a warfighting domain not thoroughly

understood by soldiers and leaders alike. This is unusual in an Army culture that highly values tactical and technical competence within designated lanes of responsibility.

The uniqueness of this scenario warrants a candid assessment of the Army's ability to operate its own networks. Specifically, do existing Army cultural norms best facilitate operation of its LandWarNet? Because a preponderance of Army activity at the strategic and operational level (and even many at the tactical level) relies on the successful operation and overall health of LandWarNet, this question is of clear strategic relevance. Failure to manage this critical resource effectively is at best a failed opportunity to leverage LandWarNet for maximum strategic effect. At worst, it leaves this critical infrastructure unnecessarily vulnerable to failure and/or attack.

This paper will first review the gradual integration of IT into Army activities and the corresponding evolution of organizational and individual responsibilities. An analysis of Army culture relevant to the question follows this historical review, to include cultural aspects of the Army as well as the unique subcultural characteristics of the signal community. Ultimately, this assessment shows that the Army culture overall and the signal community as a subculture must change to adapt to the unique management and operation requirements of LandWarNet and more effectively support all operations. Specifically, the Army should create a culture of more candid assessment within the signal community and its dialogue with mission commanders, increase the value placed upon intellectualism within the Army culture, and increase the value the signal subculture places on strategic planning competencies. Left unchanged, status quo cultural challenges result in frustration, failed expectations, inefficiencies, flawed

planning, and critical performance gaps in the operation of LandWarNet in support of Army forces.

The Evolution of IT in Army Activities

Army Field Manual (FM) 6-02, *Signal Support to Operations*, provides relevant doctrinal definitions of LandWarNet and cyberspace.

> LandWarNet…is a technical network that encompasses all Army information management systems and information systems that collect, process, store, display, disseminate, and protect information worldwide…LandWarNet is part of, and operates in, the cyberspace domain…Cyberspace is a global domain consisting of the interdependent network of information technology infrastructure and resident data.[5]

Figure 1, also from FM 6-02, provides a graphical representation of LandWarNet as one component of a greater Department of Defense Information Network (DODIN).

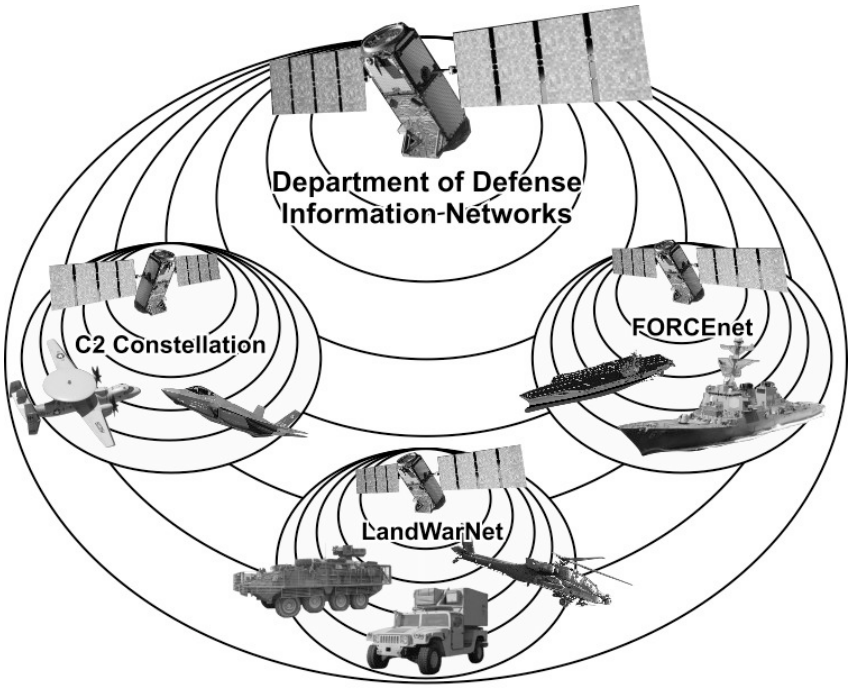

Figure 1. The Department of Defense Information Networks.[6]

Both the excerpt and graphic from FM 6-02 represent the modern doctrinal manifestation of the importance of communication and associated technologies to the military, but communication has always been at the core of military operations. The ability to communicate is critical to the military notion of command and control, and advances in communication methods and technology have played a significant role in the evolution of warfare throughout history. The past several decades have brought remarkable changes to communication technology characterized well by Lieutenant General (Retired) Julius Becton in his 2013 foreword to the aptly named book, *From Pigeons to Tweets:*

> In my lifetime, we have evolved from Morse code transmissions, rudimentary analog telephones and paper spewing teletype machines, to digital communications, globally capable cellular telephones, satellites and fiber optic enabled networks, and the Internet…This unprecedented revolution in Information Technology (IT) posed significant challenges to all aspects of military's business and combat operations--all of which are critically dependent upon rapid, reliable and survivable communications.[7]

Not only have the changes been profound, but remarkably rapid as well, as highlighted by the fact that Becton provides his description of the evolution in communications technology through the lens of a single officer's career.

While Becton's description alludes to the overall importance of communication technology to the Army, nothing about it is particularly surprising. To anyone familiar with the modern military at operational and strategic levels, the reliance on a functional underlying IT infrastructure is obvious. Modern operations centers and command posts down to division and brigade level contain rows upon rows of networked terminals providing leaders and staff a common operating picture and the ability to execute their various staff functions in a digital environment. So great is the reliance on the IT infrastructure that leaders often voice a concern regarding their organization's ability to

function were the network not to be “up.” Despite this concern, practice for such contingencies remains exceedingly rare; an anomaly in a culture which takes pride in contingency preparedness. Ironically, the reliance grows, partially due to an inability to imagine success without it.

In present day, signal soldiers and civilian IT professionals (in institutional support organizations) remain in all formations, yet their role has evolved over time. Beyond the tactical and operational signal elements such as signal battalions and staff S6 and G6 elements, entire enterprise-level commands up to the four-star level exist to operate and defend the IT enterprise across the Army, joint force, and the DOD. These include the Network Enterprise Technology Command (NETCOM), Army Cyber Command (ARCYBER), U.S. Cyber Command, and the Defense Information Systems Agency (DISA).[8] A brief survey of this landscape of relevant signal entities provides an enhanced perspective for the discussion. Keeping in mind that the primary purpose of the IT infrastructure is to provide capabilities to the supported mission commanders and their organizations, this survey begins with those elements closest to the supported mission commander and work up through the Army and DOD enterprise from there.

Mission Commander Staff and IT Resources

Each mission commander throughout the Army formation maintains possession of his/her own IT personnel within their formations. In some cases, this applies to hardware and network infrastructure as well. In operational formations, this applies down to the battalion level and the embedded S6 staff officer and staff. In organizations commanded by a general officer, the nomenclature changes from S6 to G6. According to FM 6-0, Commander and Staff Organization and Operations, the Assistant Chief of Staff, S6/G6 “is the principal staff officer for all matters concerning network operations

(jointly consisting of DODIN Operations and applicable portions of the Defensive Cyberspace Operations), network transport, information services, and spectrum management operations within the unit's area of operations."[9]

Both the reliance on IT to accomplish the mission and the responsibility to provide IT services to lower echelon units tends to increase in larger organizations. It follows that the size, responsibility and technical capabilities of S6/G6 staffs grow as one traverses up the Army's organizational hierarchy. At the lower level, a battalion S6 may focus primarily upon planning and support of tactical communication systems (often primarily radio and satellite communications).[10] In context of the greater LandWarNet, the responsibility of this lower level unit is to "plug in" to the greater enterprise from its dynamic and often-remote physical location. They largely play the role of consumer of the infrastructure. At division and corps level organization, with responsibility to provide access to LandWarNet to subordinate brigade and battalion entities, one finds G6 elements performing some degree of service provider roles.[11] Even so, the services maintained by this level of operational organization are primarily contained to tactical support services within that unit's area of operations.

Commanders for Army institutional support organizations also own a G6 and associated staff. While these organizations tend to rely heavily on standard enterprise IT services (email, internet connectivity, office productivity software, ubiquitous workstations, etc.), outside entities generally provide those services.[12] This is specifically the case for those services provided by NETCOM, ARCYBER, and DISA. In these organizations, the primary roles of the commander's G6 and staff include not providing IT services, but rather serving as an interface with the external service

provider, as well as strategic planning to best leverage IT capabilities tailored to the mission.

Network Enterprise Technology Command (NETCOM)

The NETCOM's mission statement is to "lead global operations for the Army's portion of the DODIN, ensuring freedom of action in cyberspace while denying the same to our adversaries."[13] Network Enterprise Technology Command came into existence for its current purpose in 1997 as 9th Army Signal Command (ASC). In the several years following activation, 9th ASC gradually assumed responsibility for increasingly enterprise-wide signal objectives to include the provision of long-haul communications for major military events, the connection of theater and field commanders with the Pentagon and National Command Authority, and the operation of Theater Network Systems and Operations Centers.[14] The Army re-designated the unit as NETCOM/9th ASC and a Direct Reporting Unit in 2002 as part of an Army department-wide transformation with the mission to "provide technical control and support for the Director of Information Management operations; the operation and management of the Army's total information structure; and the management and defense of the Army frequency spectrum."[15] The NETCOM serves today as the primary IT service provider to the Army enterprise.

As a subordinate headquarters to ARCYBER, NETCOM primarily fulfills one of ARCYBER's three core cyberspace tasks; namely, operation of the Army's portion of the DODIN, LandWarNet.[16] In this role, NETCOM oversees the Army's global IT infrastructure to include the hierarchy of subordinate organizations that execute this role. Two such subordinate organizations relevant to the scope of this paper are the Regional Cyber Centers (RCCs) and Network Enterprise Centers (NECs). Regional

Cyber Centers employ the technical workforce tasked with network operations within a given theater of operations to include security, operations, and maintenance of the theater LandWarNet infrastructure.[17] The theater RCC provides LandWarNet enterprise services downstream to the NECs, which exist at each installation as the IT service provider for each tenant unit. The installation NEC serves as the frontline NETCOM interface to supported organizations for all services.[18] In this way, NETCOM acts as the service provider for Army installations and organizations worldwide.

Army Cyber Command (ARCYBER)

The Army created ARCYBER in 2010 and in 2016 designated it an Army Service Component Command to U.S. Strategic Command. As of January 2017, ARCYBER serves as the higher headquarters of NETCOM. With this current alignment, ARCYBER serves as the Army's primary headquarters to conduct all cyberspace operations, primarily categorized as Offensive Cyber Operations (OCO), Defensive Cyber Operations (DCO), and DODIN operations.[19] While its subordinate NETCOM remains focused on operating LandWarNet and the provision of associated services to the Army's global presence, ARCYBER serves as a headquarters focused primarily on policy as well as OCO and DCO.[20]

Army Chief Information Officer (CIO) / G6

The Army CIO/G6 simultaneously serves dual roles. As the CIO, he or she serves as the principal advisor to the Secretary of the Army on the strategy, policy, and execution of Information Management (IM) and IT for the Army. As the Army Deputy Chief of Staff, G6, he or she provides advice to the Army Chief of Staff for IM/IT and communications issues and their impact on warfighting capabilities from a network functional perspective.[21]

Defense Information Systems Agency (DISA)

Above the Army organizational level, DISA (known as the Defense Communications Agency until 1991) is a combat support agency of the Department of Defense. Defense Information Systems Agency's stated mission is to "provide, operate, and assure command and control, information sharing capabilities, and a globally accessible enterprise information infrastructure in direct support to joint warfighters, national level leaders, and other mission and coalition partners across the full spectrum of operations."[22] Where NETCOM acts as the service provider for the Army, DISA does the same for the greater DOD. The Army's LandWarNet infrastructure and services integrate with the larger DODIN under the responsibility of DISA, and the Army acquires some specific enterprise IT services from DISA (enterprise email is a ready example).[23]

Organizational Roles and Increasing Centralization

Typical Army personnel not directly associated with the signal mission do not generally understand the above organizations and their roles. It is common to hear personnel at all levels refer erroneously to one organization or the other regarding a given IT policy or technical implementation. There are varieties of reasons for this, some discussed below in the context of Army culture. Perhaps one contributor to this lack of understanding is the increasing centralization of IT services across the Army. Users (and mission commanders) are increasingly aware that technical implementations happen elsewhere, but beyond their resident S6 or G6 staff, they cannot "see" what is happening or why. So, in the context of centralizing service, what *is* happening and why?

As a general trend, improved reliability of the global network and improving technology in the delivery of enterprise services and vulnerability prevention have

enabled a corresponding increase in the centralization of technical activity in administration of LandWarNet. Whereas ten years ago, local NECs and in some cases even organizational S6/G6 staffs, maintained data centers full of servers and network equipment in their physical vicinity, those same services are now provided by NETCOM from centralized locations. Among the leading reasons to centralize in this manner are increased cost efficiencies, reduced “surface area” for cyber-attack, and improved standardization and compliance of vulnerability protection methods.[24]

In more specific terms, the Army is moving in concert with DISA’s initiatives in pursuit of the Joint Information Environment (JIE), a joint, simplified, and standardized security architecture for all services.[25] As described by the DOD CIO in 2015, JIE initiatives will “replace our current individualized and localized security architecture and systems with a set of servers, tools and software that will provide better command and control and more security and do that at a lower cost.”[26] One project that illustrates the scale of these changes is the effort to consolidate hundreds of Internet access points down to just 25 locations, each containing a standardized Joint Regional Security Stack (JRSS), a standard suite of equipment that provides enterprise management and security capabilities.[27] Implementation of JRSS began across the services in 2015 and continues today.[28] While there exists little doubt that this and similar consolidation and centralization initiatives are the right thing to do, they also lead to challenges in the context of Army culture.

Army Culture and Culture Change

Organizational culture refers to the values and behaviors that contribute to the unique social and psychological environment of an organization.[29] Noted psychologist and organizational culture scholar Edgar Schein provides terms and concepts relevant

to this discussion. Beyond the basic definition of organizational culture, Schein describes three distinct levels of culture with varying degrees of visibility at each level, and with interaction between the levels. Figure 2 depicts this concept below.

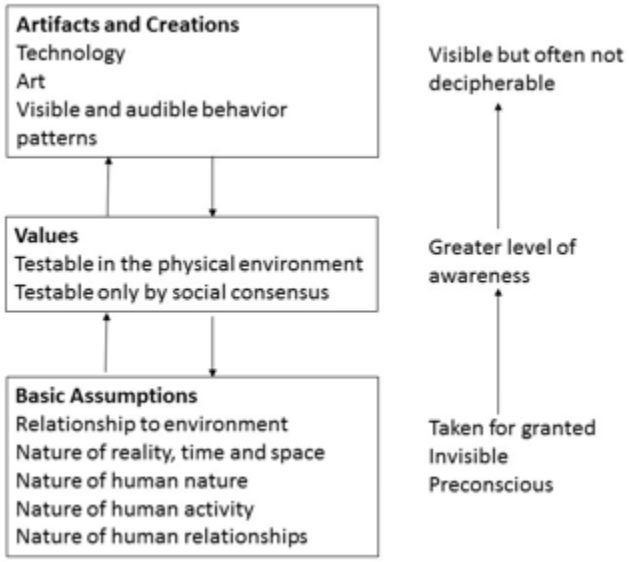

Figure 2. Schein's Model for Levels of Culture and their Interactions.[30]

This work utilizes Schein's concept of the terms *artifacts, values,* and *assumptions* in discussion of organizational culture.

Due to its large size, unique organizational purpose and relative importance to national well-being, the Army has a distinct culture. Because of this, many organizational scholars have examined Army culture over time. The nature of Army business in the provision of national security leads to a performance-oriented culture. The Army highly values both individuals and groups that produce results. Operations typical of combat arms branches of the Army arguably provide the most readily understood and tangible evidence of mission results. A preponderance of senior Army leaders rose through the ranks of the combat arms. Thus, those who developed professionally in environments predominantly focused on the preparation for or

execution of kinetic combat tasks lead the Army. In Schein's terminology, Army culture includes an underlying assumption that tangible results in warfighting-centric tasks demonstrate the highest degree of competence and lead to success. Artifacts of this preference exist in what traits are valued in performance evaluations as well as the high ratio of general officers coming from combat arms.

Another subtle artifact reflecting this cultural value is the prevalence of successful, influential commanders and leaders who boast of their own supposed low-intellectualism. These leaders take pride in describing themselves as knuckle-dragging, combat proven leaders. Anyone who has served in the Army for even a modest time has seen these leaders. While those observations may be anecdotal, there exists academic literature that identifies this characteristic of Army culture via more thorough examination. Lloyd Matthews describes the history of this cultural attribute in his detailed essay "Anti-Intellectualism in the Army Profession," in which he documents a strong bias towards "doers" versus "thinkers."[31] Among his assertions is that "to express their professional ambition, they feel constrained to suppress, disguise, or ignore their intellectual side…within the system that forces many officers to deny their intellectuality as the price of career success."[32] Though certainly not every leader consciously embraces this phenomenon, the reality is that they have all succeeded in environments that prioritized "doing" over "thinking." This cultural characteristic persists today. As retired Lieutenant General David Barno notes, "Anti-intellectualism in the Army is not new, but it has grown as an unintended consequence of the recent wars."[33]

In the specific context of IT, this cultural artifact persists despite the recent history of increased reliance on the effective management of this technology, a discipline

requiring a degree of complex knowledge. To compensate for a lack of general understanding of the operation and maintenance of enterprise and local IT infrastructure, leaders have simply relied more and more heavily upon their resident technical expertise, the S6 and G6 staffs within their organizations. This approach worked sufficiently, if not ideally, in the era in which S6 and G6 staff maintained administrative control over much of the IT infrastructure and services leveraged by the organization. However, in recent years as the Army moves toward the JIE, it has centralized management of IT services to the enterprise level. The S6 and G6 staffs have little, if any, direct control of implementation and configuration of the infrastructure. Although the local technical staffs of the installation NECs remain within reach of the mission commanders, they have less and less direct administrative control over the technology. Thus, just as mission commanders and leaders have become increasingly reliant on the resident technical knowledge of their supporting S6/G6 staffs, those same staffs increasingly rely on higher enterprise authorities and technicians to execute technical tasks.

Further complicating the scenario is the strong cultural assumption that everything within the physical sphere of control of a mission commander is at the commander's direction. This cultural assumption is historically common in all military organizations for logical reasons. The effective prosecution of armed conflict requires a strong hierarchy and clearly established authority. Military organizations predominantly place this authority with commanders at all levels. It is not surprising that Army culture includes an expectation that commanders provide direction over *all* assets and activities within their sphere of influence. Commanders themselves hold this expectation as well.

However, this is at odds with the increasingly centralized nature of LandWarNet operations.

While NETCOM (typically via their subordinate NECs at each installation) has long owned the local IT infrastructure, mission commanders have still enjoyed significant influence on those activities through their proximity. The S6/G6 staffs most often interacted with NEC staffs to affect the desired influence on behalf of commanders. As the Army moves toward the JIE, local NEC staffs no longer maintain the administrative privileges over network resources and configuration to act directly. When a local mission requirement requires a revised or new capability, often both the S6/G6 staff and the local NEC only serve as intermediaries with the enterprise entities. The enterprise entity could be an RCC, its owning theater signal command or NETCOM staff, ARCYBER, or DISA. Often it requires a combination of all of them to gain the appropriate approval and see it followed by task execution.

The centralization of LandWarNet administration also provides an opportunity to highlight aspects of the signal community subculture within the greater Army culture. To this point, this paper has focused largely on Army culture overall and to a certain degree the subculture of Army leadership. The signal community also has its own distinct subculture. Edgar Schein defines an occupational community as “a group of practitioners, researchers, and teachers who have a common base of knowledge, a common jargon, similar background and training, and a sense of identifying with each other.”[34] This definition certainly applies to the IT community, which in the Army consists of Signal Regiment soldiers and civilians. In his extensive studies on culture within private industry, Schein noted that the organizational IT community demonstrates

consistently similar assumptions.[35] This strengthens the notion that the signal community's subculture within the Army contains distinct characteristics.

One value within the signal subculture is the strong desire to respond with "yes" to every commander expectation. The belief that "no, we can't" is not an acceptable answer stems from a perceived pressure to facilitate every expectation the commander has of the supporting IT infrastructure and services. When the commander expects something from the greater IT apparatus, the supporting signal staff feels great pressure to make it happen. While this is true for any specialty supporting the commander's mission, the signal community arguably feels the pressure more acutely for two reasons. First, as already described, Army leaders generally do not prioritize technical awareness in their own development. One result is that *only* the signal staff in an organization understands the relative feasibility of a leader's IT expectation. A commander may describe requirements for other support disciplines in generally feasible terms based upon the commander's own calibrated sense of understanding. However, the same is often not the case for IT related requirements for which the commander lacks the same calibrated sense. Second, almost all communications and staff activity rely heavily on the IT infrastructure. In many cases, if IT fails, there is no feasible backup plan. This places heavy pressure on the signal staff to accomplish every task and provide 100% availability. This pressure itself is not unhealthy. Critical infrastructure of any type demands high performance and leaders should expect nothing less. However, this insight does help to describe the signal subcultural value that "no" is not an acceptable answer.

The cultural assumptions, values, and artifacts previously discussed combine to create an environment in which mission commanders and leaders establish unrealistic expectations for LandWarNet perceived to be under their control. Further, they expect their own signal staff to execute the related tasks with urgency commensurate with the mission requirement. The requirements often prove unrealistic and the signal staff cannot execute the required tasks without significant assistance from enterprise agencies outside the mission commander's sphere of influence. Perhaps most impactful, in adherence to the cultural value that "no" is never an acceptable answer, signal leadership at all levels essentially guarantees failed expectations by assuring mission commanders that centralized administration processes will retain the responsiveness that mission commanders desire. Frustration, failed expectations, inefficiencies, and flawed planning abound, all largely a result of cultural characteristics misaligned with the requirements to operate LandWarNet.

Culture Change Recommendations

To best create an environment for effective operation of LandWarNet, Army and signal senior leaders must change elements of the culture. The goal of these recommendations is to maximize the Army's ability to leverage the capabilities LandWarNet provides while at the same time minimize the inherent risks.

Recommendation 1: Candor; Costs of Centralization

The signal community, and signal leaders specifically, must be more candid with Army leaders regarding the cost of centralizing the administration of LandWarNet and related IT services. If the degree to which LandWarNet and its administrators provide responsive mission support were the weight on one side of a scale, the counterweight on the opposing side would be cost efficiency and security posture. In this balance of

responsive mission support versus cost efficiency/security posture, the Army has deliberately prioritized cost efficiency/security posture in recent years. The initiatives associated with a move to the JIE reflect that posture. At the same time however, this centralization degrades the ability to provide responsive mission support by placing required administrative control in the hands of remote entities outside the influence of the local mission commander.

This approach represents an arguably prudent solution based on cost/benefit analysis. Given the high costs of IT and increasingly big impact of potential security breaches, one can argue that degraded responsiveness of mission support represents an acceptable cost. It is not within the scope of this paper to argue this point, but rather to recommend changes to address the expectation gap resulting from the approach. If signal leaders who have consciously pushed the scale in the direction of cost efficiency and security posture continue to proclaim that there is no corresponding cost to responsive mission support, the expectation gap will persist.

Signal leaders need to change the subculture. The cultural value placed on promising mission success in all requirements prevents a candid assessment of degraded mission support responsiveness. Signal leaders owe Army senior leaders this candor. Army leadership and mission commanders throughout the Army must understand that we accept degraded mission support as a cost of security assurance. It is a message they will likely accept. Sometimes the answer must be “no” in order to assure an appropriate security posture and fiscal health across the enterprise. More often, the answer can still be “yes,” but with an implementation timeline commensurate

with the ability of centralized enterprise administrators to assess, gain approval for, and implement the change on behalf of mission commanders.

Recommendation 2: Embrace Technology and Intellectualism in General

Army leaders at all levels must embrace technology and dismiss anti-intellectualism across the force. This requires a change to the existing culture in which anti-intellectualism can coexist with career success. The degree to which all Army operations rely upon the IT infrastructure is clear. The reliance is significant enough that the Army must find ways to ensure leaders understand and consider the fundamental requirements to protect and operate it to advantage.

Further, unlike other warfighting domains defined by activities largely within a specific physical dimension (land, air, sea, space), the cyber domain manifests itself in all of them. As there are no limits to the physical reach of cyber operations, they become critical considerations within the sphere of all mission commanders. Stated plainly, cyber is the business of all Army personnel and thus their leaders as well. Technical literacy (not necessarily expertise) is required at all levels and leaders must publicly embrace that obligation to both make effective decisions and set the example for the rest of the force.

Recommendation 3: Signal Strategic Planning Competency

The signal community must focus on the competency of strategic planning. Much of the Army has historically viewed members of the signal community within their reach as the exclusive technical experts and the expectations for the output of signal personnel largely reflect that. The S6 and G6 staffs have focused primarily on technical competencies to make “yes” happen. This is a tempting paradigm for signal personnel to embrace. Particularly within an Army culture that values anti-intellectualism, the

technical competence displayed by signal personnel allows them to stand out. The culture most often rewards them for their technical ability to “make things work.” However, the community’s predominate focus on technical competencies increasingly represents a failure to recognize where it can provide the most impact to the mission and organization.

As the DOD and Army centralize the administration of IT services, resident technical skills within supported organizations provide less value. Increasingly, the value of signal personnel embedded within Army formations comes from an ability to conduct strategic communications planning effectively. While sufficient technical background remains important to plan appropriately, the signal regiment should emphasize the discipline of strategic communications planning beginning with the junior ranks. This would focus the S6/G6 efforts where they can provide the most impact: effective strategic planning for future IT requirements, capabilities, and infrastructure. A thorough understanding of the signal enterprise structure and hierarchy combined with sound strategic planning should result in improved planning lead-time to coordinate for realistic solution implementation by the remote enterprise administrators via processes defined by NETCOM and DISA.

This recommendation provides an ironic contrast to the previous recommendation. While the greater Army needs to place higher value on technical literacy, the signal community needs to emphasize not only technical skills, but also strategic planning. To be clear, signal personnel must remain the technical subject matter experts within their supported organizations, but this should not come at the cost of an energized emphasis on effective strategic planning.

Enacting and Anchoring Change

The above recommendations describe needed changes to both the Army culture and signal subculture. Cultural change is challenging. Not only is the Army culture distinct, it is mature and generally successful. As noted by Gerras, Wong, and Allen, this presents a particular challenge to cultural change initiatives.[36] Culture change in both mature organizations and successful organizations is particularly difficult. The Army is both. The Army is justifiably proud of its culture and considers the culture to have attributed to past successes. Scholars note that the American public's high regard for the military is in part due to its perception as highly performance oriented.[37] Thus, Army personnel are perhaps even more likely than members of other organizations to celebrate underlying assumptions rather than embrace their change.[38]

Other characteristics of Army culture provide additional challenges to change initiatives. Specifically, Cameron and Quinn's Competing Values Model of organizational culture designates the Army as a "hierarchy" culture characterized by a focus on chain-of-command and strict policies and procedures.[39] Cameron and Quinn argue that hierarchy cultures prove difficult to change.[40] The Army's high reliance on ingrained rules leads to less habitual awareness of more dynamic inputs such as an organizational change vision. The Competing Values Model description of Army culture corresponds well with the notion of Power Distance as defined in the Global Leadership and Organizational Behavior Effectiveness Research Program. The identification of the Army's high Power Distance, specifically, further supports and defines the organizational change challenges described by the Competing Values Model.[41] Thus, while change in any organization is challenging, culture change within the Army can

prove particularly difficult. To achieve intended results, then, any recommendations for culture change in the Army should be rooted in a sound approach.

John Kotter, noted organizational change thought leader, describes his now well-known eight step process for creating organizational change in his book *Leading Change*.[42] The final stage of Kotter's process for organizational change is anchoring the change in the culture.[43] This is arguably the most critical stage, as successful execution of Kotter's previous seven stages may only result in temporary change if not appropriately anchored in the culture. Leaders cannot anchor enduring change through their individual action alone. Individuals may come and go or eventually shift focus to other areas, so leaders must embed the change in the culture independent of individual personalities.

Edgar Schein identifies the concepts of embedding and reinforcing mechanisms that can serve as the cultural anchors that Kotter describes.[44] Schein distinguished between primary embedding mechanisms and secondary reinforcement mechanisms in his foundational book *Organizational Culture and Leadership*.[45] The embedding mechanisms create what Schein refers to as the underlying assumptions in the culture. The reinforcement mechanisms, while important, primarily serve to reinforce the assumptions created by the embedding mechanisms. A common mistake is to implement secondary reinforcement mechanisms with no corresponding embedding mechanisms.

Thus, focused leaders should enact the recommended culture changes described above with these principles from Schein and Kotter in mind. Importantly, this requires the thoughtful identification of effective embedding mechanisms to ensure

success of Kotter's critical eighth phase to anchor the changes in the culture. One option is find ways to measure the newly valued cultural elements in accordance with the notion that organizations measure what they value. Decades ago, the Army utilized this method in its efforts to prioritize physical fitness by beginning to measure soldier fitness performance on evaluation reports.[46] Regardless of the specific mechanisms employed, identification of them will require creativity and is not a trivial task. However, for reasons already described, any change efforts falling short of this step will likely fail in an organization such as the Army.

Looking Forward

Recent decades have seen rapid integration of IT into Army activities at all levels. In this, the Army is no different from virtually any other enterprise. The striking evolution of technology during the past thirty years has greatly affected all industries and ventures. While many organizations have adapted well, others have not. The scale of potential new capabilities is such to demand that organizations continually assess, adapt, and re-assess their approach to IT management and execution. Because an underlying communication infrastructure supports so much business activity, this applies not just to the technical subject matter experts within the organization but to all personnel and processes.

The Army has room to improve in this regard. Certain aspects of the Army's culture present challenges to the effective operation of this critical infrastructure. Edgar Schein's model of cultural assumptions, values, and artifacts helps to illustrate that certain Army cultural characteristics contribute to flawed planning and failed expectations in the implementation of network-based mission support solutions. Further, despite well-intentioned communications from senior leaders, there remains a cultural

perception that technical matters are the business of “others” and not for the consideration of mission commanders. This conflicts with the simultaneous cultural notion that anything physically located within the influence of a mission commander is at his or her direction; a notion increasingly at odds with reality as management and even physical location of the IT infrastructure becomes more centralized and under the direction of the signal community.

To address these obstacles and most effectively operate and employ LandWarNet, the Army should consciously facilitate the change to the described cultural characteristics. Beyond the identification of recommended changes, Schein’s notion of embedding and reinforcing mechanisms helps to describe the requirement to anchor the changes in the culture effectively, thus accomplishing John Kotter’s eighth phase of organizational change. Specifically, the Army should create a culture of more candid assessment within the signal community and its dialogue with mission commanders to close the gap between expectation and reality in the tradeoff between security assurance and flexible mission support. The Army should also increase the value placed upon intellectualism within the culture, particularly when it comes to the basic tenets of IT planning considerations. Finally, the signal community should simultaneously move to place increased emphasis on IT strategic planning to better support mission commanders.

The Army can implement these changes through a focus on cultural characteristics and their respective impacts. With the needed changes successfully embedded in the culture, Army formations can realize the benefits of improved fiscal efficiency and security posture resulting from the centralized administration of

LandWarNet. Further, they can do so within realistic, predictable solution implementation timelines allowing mission commanders and their staffs to focus on overall mission success rather than IT frustrations.

Endnotes

[1] Office of the Army Chief Information Officer/G6, *Army Network Campaign Plan, Implementation Guidance, Near Term, 2017-2018 (*Washington, DC: U.S. Department of the Army, February 2016), 3.

[2] LandWarNet is not an acronym, but rather a stand-alone term coined by the Army. U.S. Department of the Army, *Mission Command,* Army Doctrine Publication 6-0, C2 (Washington, DC: U.S. Department of the Army, March 12, 2014), 11, http://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/adp6_0.pdf (accessed 14 February, 2018).

[3] John T. Bennett, "Pentagon Declares the Internet a War Domain," July 14, 2011, linked from *The Hill Home Page* at "Policy," http://thehill.com/policy/technology/171531-pentagon-declares-the-internet-a-domain-of-war (accessed January 15, 2018).

[4] Ellen Nakashima, "Defense Official Discloses Cyberattack," August 14, 2010, linked from *The Washington Post Online* at "Politics," http://www.washingtonpost.com/wp-dyn/content/article/2010/08/24/AR2010082406495.html (accessed February 26, 2018).

[5] Headquarters, Department of the Army, *Signal Support to Operations,* Field Manual 6-02 (Washington, DC: Headquarters, Department of the Army, January 22, 2014), 1-1, http://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/fm6_02.pdf (accessed February 14, 2018).

[6] Ibid., 3-2.

[7] Clarence McKnight, Jr. and Hank Cox, *From Pigeons to Tweets, The Dramatic Revolution in Military Communications* (Palisades, NY: History Publishing Company, 2013), 11.

[8] Department of the Army, *Signal Support to Operations,* 2-10 – 2-16.

[9] Headquarters, Department of the Army, *Command and Staff Organization and Operations,* Field Manual 6-0 (Washington, DC: Headquarters, Department of the Army, April 22, 2016), 2-12, http://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/ARN7501_FM_6-0_Incl_C2_FINAL_WEB.pdf (accessed January 15, 2018).

[10] Department of the Army, *Signal Support to Operations,* 2-2 – 2-3.

[11] Ibid., 2-3 – 2-4.

[12] Ibid., 2-13 – 2-15.

[13] *U.S. Army Network Enterprise Technology Command Home Page*, http://www.netcom.army.mil/ (accessed January 15, 2018).

[14] Network Enterprise Technology Command, "Brief History of the United States Army network Enterprise Technology Command and the 9th Army Signal Command," linked from the *U.S. Army Network Enterprise Technology Command Home Page* at "History," http://www.netcom.army.mil/about/history.aspx (accessed January 15, 2018).

[15] Ibid.

[16] Department of the Army, *Signal Support to Operations,* 2-12.

[17] Ibid., 2-16.

[18] Ibid., 2-15.

[19] No Author, "U.S. Army Cyber Command," linked from the *U.S. Army Cyber Command Home Page* at "History," http://www.arcyber.army.mil/Organization/History/ (accessed January 15, 2018).

[20] Ibid., 2-11.

[21] Department of Command, Leadership, and Management, *How the Army Runs: A Senior Leader Reference Handbook,* 2015-2016 (Carlisle Barracks, PA: U.S. Army War College, 2015), 15-1.

[22] *Defense Information Systems Agency Home Page*, http://www.disa.mil/about (accessed January 15, 2018).

[23] Department of the Army, *Signal Support to Operations,* 3-1.

[24] Defense Information Systems Agency, *Enabling the Joint Information Environment (JIE): Shaping the Enterprise for the Conflicts of Tomorrow* (Fort Meade, MD: Defense Information Systems Agency, 2014), 10, https://www.disa.mil/~/media/Files/DISA/About/JIE101_000.pdf (accessed January 15, 2018).

[25] Ibid., 1.

[26] Cheryl Pellerin, "DoD CIO Details Information Technology Priorities," Feb 26, 2015, linked from the *U.S. Department of Defense Home Page* at "News," https://www.defense.gov/News/Article/Article/604182/ (accessed January 15, 2018).

[27] Defense Information Systems Agency, "Joint Regional Security Stacks (JRSS)," linked from the *Defense Information Systems Agency Home Page* at "Initiatives," https://www.disa.mil/Initiatives/JRSS (accessed January 15, 2018).

[28] Sydney Freedberg Jr., "Carter Visit Highlights Cybersecurity," May 31, 2016, linked from the *Breaking Defense Home Page* at "Intel & Cyber," https://breakingdefense.com/2016/05/carter-visit-highlights-armys-cybersecurity/ (accessed January 15, 2018).

[29] Business Dictionary, “Organizational Culture,” linked from the *Business Dictionary Home Page*, http://www.businessdictionary.com/definition/organizational-culture.html (accessed October 17, 2017).

[30] Edgar Schein, *Organizational Culture and Leadership* (San Francisco: Jossey-Bass, 1986), 14.

[31] Lloyd J. Matthews, “Anti-Intellectualism in the Army Profession,” Chapter 3 in Don M. Snider and Lloyd J. Matthews, eds., *The Future of the Army Profession*, 2nd ed. (New York: McGraw-Hill, 2005) 61-92.

[32] Ibid., 77.

[33] David Barno and Nora Bensahel, “Six Ways to Fix the Army’s Culture,” September 6, 2016, linked from the *War on the Rocks Home Page* at "Special Series-Strategic Outpost,” https://warontherocks.com/2016/09/six-ways-to-fix-the-armys-culture/ (accessed January 15, 2018).

[34] Edgar Schein, *Organizational Culture and Leadership,* 2nd ed. (San Francisco: Jossey-Bass, 1992), 278.

[35] Ibid.

[36] Stephen J. Gerras, Leonard Wong, and Charles D. Allen, *Organizational Culture: Applying a Hybrid Model to the U.S. Army*, Research Paper (Carlisle Barracks, PA: U.S. Army War College, November 2008), 17.

[37] Ibid., 11.

[38] Ibid., 17.

[39] Ibid., 3-4.

[40] Ibid., 15-16.

[41] Ibid., 14-15.

[42] John P. Kotter, *Leading Change* (Boston: Harvard Business School Press, 1996), 21.

[43] Ibid., 21.

[44] Gerras, Wong, Allen, *Organizational Culture*, 17.

[45] Schein, *Organizational Culture and Leadership,* 223.

[46] Gerras, Wong, Allen, *Organizational Culture,* 18.