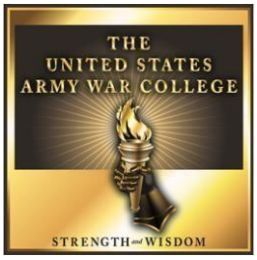
Strategy Research Project

The Forgotten Layer: Infrastructure

by

Lieutenant Colonel Kevin M. MacNeil
United States Army

Under the Direction of:
Colonel Douglas J. Orsi



United States Army War College
Class of 2018

DISTRIBUTION STATEMENT: A
Approved for Public Release
Distribution is Unlimited

The views expressed herein are those of the author(s) and do not necessarily reflect the official policy or position of the Department of the Army, Department of Defense, or the U.S. Government. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

The public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing the burden, to Department of Defense, Washington Headquarters Services, Directorate for Information Operations and Reports (0704-0188), 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to any penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number. **PLEASE DO NOT RETURN YOUR FORM TO THE ABOVE ADDRESS.**

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 Forgotten Layer: Infrastructure

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Lieutenant Colonel Kevin M. MacNeil
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Douglas J. 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.
I understand this document will be included in a research database and available to the public. Author: ☒

13. SUPPLEMENTARY NOTES
Word Count: 5,580

14. ABSTRACT

In 2010 the information technology (IT) industry recognized the transition to cloud computing was driving an increased reliance on data centers and the infrastructure that supports them, specifically power distribution, heating, ventilation, air conditioning, and back-up power. Companies began to use the data center infrastructure management (DCIM) framework, software solutions, and engineering staff to maintain and manage building infrastructure critical to their IT operations and revenue streams. This paper identifies data center consolidation, Army Network Command's responsibility for IT facilities, transition to cloud-based computing, and the fielding of division level Home Station Mission Command Centers as factors driving the Army to the same reliance on data center infrastructure. The analysis describes the DCIM framework and the need for a change in Army culture to one that values IT facility management. It recommends adopting DCIM across the Army IT enterprise. Additional adjustments include adding certified mechanical technicians to the IT facility's staff to establish a facility management working group and a facility certification process as a component the Defense Information Systems Agency's Cyber Operational Readiness Inspection.

15. SUBJECT TERMS
Data Center Infrastructure Management; Power Generation / Efficiency Utilization; Facility Management; IT

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	30	

The Forgotten Layer: Infrastructure

(5,580 words)

Abstract

In 2010 the information technology (IT) industry recognized the transition to cloud computing was driving an increased reliance on data centers and the infrastructure that supports them, specifically power distribution, heating, ventilation, air conditioning, and back-up power. Companies began to use the data center infrastructure management (DCIM) framework, software solutions, and engineering staff to maintain and manage building infrastructure critical to their IT operations and revenue streams. This paper identifies data center consolidation, Army Network Command's responsibility for IT facilities, transition to cloud-based computing, and the fielding of division level Home Station Mission Command Centers as factors driving the Army to the same reliance on data center infrastructure. The analysis describes the DCIM framework and the need for a change in Army culture to one that values IT facility management. It recommends adopting DCIM across the Army IT enterprise. Additional adjustments include adding certified mechanical technicians to the IT facility's staff to establish a facility management working group and a facility certification process as a component the Defense Information Systems Agency's Cyber Operational Readiness Inspection.

The Forgotten Layer: Infrastructure

The fully burdened cost of power is a data center expense that includes the power supplied to the facility, plus the power distribution system and the cooling infrastructure. Vice President and distinguished engineer at Amazon Web Services, James Hamilton, noted in 2008 that this cost dominates all other data center expenses.[1] In December 2016 the Secretary of the Army called for an immediate reduction in information technology (IT) hosting costs. United States (U.S.) Army IT expenses totaled $8.3 billion for 2015, which encompassed manpower, services, products, applications and host facilities.[2] Army IT facilities currently lack the capability to control utility costs and proactively maintain their facility's infrastructure. The Army needs to implement an enterprise level data center infrastructure management framework for managing all of its IT facilities in order to reduce hosting expenses.

This paper explores how the contributing factors of the data center consolidation directive, the transition of IT facilities from Installation Management Command (IMCOM) to the Army Network Command (NETCOM), the transition to cloud-based computing environment, and the fielding of home station mission command centers have increased the Army's reliance on the building infrastructure of mission critical IT facilities. The commercial industry's implementation of the Data Center Infrastructure Management (DCIM) framework is explained and two of the measurable tools used by the industry are described. It then examines recent publications and strategic communication by the Army's Chief Information Officer/G6's, followed by recommendations for creating a culture change in IT facility management across the Army. Finally, post-implementation IT facility management is described.

Background

On December 9, 2016 the Secretary of the Army issued Army Directive 2016-38, *Migration of Army Systems and Applications to Approved Hosting Environments and Consolidation of Data Centers*. It specifically called for a reduction in hosting related costs and a data center infrastructure reduction by 60% from the current baseline.[3] The directive also detailed 570 data centers, processing nodes or computer/server rooms selected for closure before 2025.[4] The directive contains a detailed migration process for applications into the Army Private Cloud-Enterprise or a Defense Information Systems Agency (DISA) enterprise hosting option, provided the application can be virtualized. For those applications that have not yet transitioned to a virtual environment, their owners are left to find new homes for their mission essential IT equipment. Facilities that take on this homeless equipment must understand their current heating, ventilation, and air conditioning (HVAC) power consumption rates and capacity to expand in order to properly assess the requirements of additional incoming equipment. Often this information will require direct involvement from the IMCOM department of public works (DPW) and can require work to rehome electrical runs and increase power and HVAC capacity to certain areas potentially creating friction and priority conflicts between NETCOM and IMCOM.

In addition to calling for data center infrastructure and hosting cost reduction, Army Directive 2016-38 defines the five Army hosting solutions and data centers. The five solutions are Army enterprise data centers, tactical processing nodes, installation service nodes, installation processing nodes, and special purpose processing nodes.[5] Army enterprise data centers are high capacity fixed facilities that can host both local and enterprise level applications. The Army is currently slated to have ten in the United

States and six overseas, though the overseas locations have not yet been determined. Tactical processing nodes are mobile nodes supporting tactical or deployed forces and are exempted from the directive. Installation service nodes contain localized equipment to support the installation with minimal services should it be disconnected, but it does not host applications or process data. Installation processing nodes are fixed data centers supporting a single installation or local area and has all the capabilities of an installation service node plus the ability to host applications and process data. Special purpose processing nodes are fixed data centers supporting special purpose function such as, for example, medical facilities, test ranges, and classrooms or research, development, test and evaluation organizations.[6]

Three of these solutions, Army enterprise data center, installation processing node, and special purpose processing node, are considered data centers by their definition. The installation service node, though not a data center by definition, houses essential equipment supporting the installation, including host-based security servers, security scanners, and emergency services equipment.[7] Facility management and DCIM are needed at all facilities with the exception of the tactical processing nodes.

Contributing Factors

At the conclusion of a recent senior leader visit to the Army's Network Enterprise Center in Hawaii, it was evident the facility suffered from a lack of infrastructure investment in its supporting systems. The facility struggled to maintain complex industrial systems for HVAC, as well as back-up power complicated by unclear responsibilities between NETCOM and IMCOM DPW. As early as 2010 the commercial Information Management industry started to recognize the importance of the data center facility. An article published by *Information Management* in June 2010 citing a biannual

Data Center Users Group survey stated, “Adequate monitoring and management capabilities as respondents’ primary facility/network concern.”[8] Since 2010 data center infrastructure and management has seen exponential growth. In 2016 Grand View Research estimated that the data center cooling market alone will reach $17 billion by 2024.[9] This is one of the contributing factors for industry’s movement to the data center infrastructure management framework.

The contributing factors for the Army were data center consolidation, the functional transition of installation IT management from IMCOM to NETCOM, movement to cloud based distributed computing environments, and the enabling of mission command from home station through the fielding of home station mission command centers in division headquarters.[10] The Army’s reliance on the network for mission command has reached a point where local infrastructure management can have significant mission impact to deployed forces.

In October 2009 the Army’s initiative to establish a global network enterprise moved management and oversight of installation IT service providers from IMCOM to NETCOM and transitioned them into Network Enterprise Centers (NEC).[11] Shifting responsibility for the installation IT service provider to NETCOM had the unintended consequence of breaking the habitual relationship between DPW and the NEC. Installation Management Command retained responsibility for the facility and the systems that support its normal operation. The NETCOM assumed responsibility for the IT equipment within the building; any facility modifications solely supporting technical hardware; and the core mission of providing local network, voice, and data access across the installation.

The same year of the IMCOM to NETCOM transition, Tam Harbert published an article in Computerworld asking what role the IT department should play in controlling a company's energy expenses. She describes an environment where the IT department buys the technology and facilities buys the power.[12] Her environment mirrors the one just created where NETCOM buys the technology and IMCOM provides the power. In the same article, McKinsey and Company called upon "companies to move accountability for facilities operations to the CIO [Chief Information Officer] and to appoint an internal energy czar to better focus on the true cost of data center ownership, which includes both equipment and facilities expenses."[13] This disconnect between facility management and IT service provider creates friction when priorities differ, especially in fiscally constrained environments. For example, preventative maintenance for computer-controlled air conditioning units is a high priority for the IT service provider, but may not warrant the same priority from DPW when compared to power generation upgrades or fresh water pumps for on post housing units. When the IT service provider transitioned from IMCOM to NETCOM it created responsibility stove pipes. This inefficient management of IT facilities will challenge the infrastructure, power requirements, building electrical grids, and cooling capabilities, as services are consolidated in accordance with the Army Directive.[14]

One does not have to venture too far into the cyber, computing, or IT arenas before running into "the cloud," with even the Army piloting a Private Cloud-Enterprise. Cloud computing is a method to deliver services or content over the internet. Defense Information Systems Agency's Enterprise Email is an example of a cloud service that can be accessed through the internet, on a government computer, or mobile device.

Cloud computing enables organizations to consolidate servers into large data centers and provide services from afar.[15] In 2015 LTG Robert Ferrell, then Chief Information Officer/G6 for the Army, issued the service's cloud computing strategy, stating that "the ability to connect to cloud capabilities assures that Army computing and communications resources, authoritative data sources, services and information are available, accessible and safeguarded, from the enterprise to the edge."[16] Cloud computing is often seen as a cure all, however the distributed computing environment is not without risks.

Greg Ferro wrote in his article "Is Networking Infrastructure the Achilles' Heel of Cloud Computing?" that the network is the crux of a connection to the cloud, saying "the success of a public cloud initiative is critically dependent on networking infrastructure."[17] In 2015 Turkish War College Student Osman Ocak did a strength, weakness, opportunities, and threat analysis of cloud computing. In it, he identified the number one weakness to be bandwidth, defined as the ability to move digital information from the end user to the cloud, and the number one threat to be reliability of service providers.[18] Both gentlemen recognize that cloud computing still relies on brick and mortar buildings outfitted with networking equipment. That equipment requires temperature control environments, redundant and stable power, and emergency systems. As the Army transitions to its Private Cloud-Enterprise, there will still be installation processing nodes, special purpose processing nodes, and data centers throughout the world that require facility management to enable mission command, especially with the fielding of Home Station Mission Command Centers (HSMCC).

In 2016 the Army began fielding HSMCCs at division level headquarters. The standardized capabilities included with HSMCC enabled distributed planning, telepresence, communication systems, and command and control. Home Station Mission Command Center “enhances the ability of commanders in garrison to lead forces deployed potentially thousands of miles away.”[19] The HSMCC places even more priority on the installation processing node or data center to provide reliable and redundant network access to the division headquarters. Unforeseen outages due to facility failures at home station can now have immediate impact on division level operations throughout their area of responsibility. Figure 1 is the cyber terrain model for the 25th Infantry Division’s 2017 Warfighter exercise. It clearly depicts every major subordinate command in the division directly connected to the NEC (represented by the blue box). Similarly, in the HSMCC model, the NEC is critical to the division’s warfighting operations.

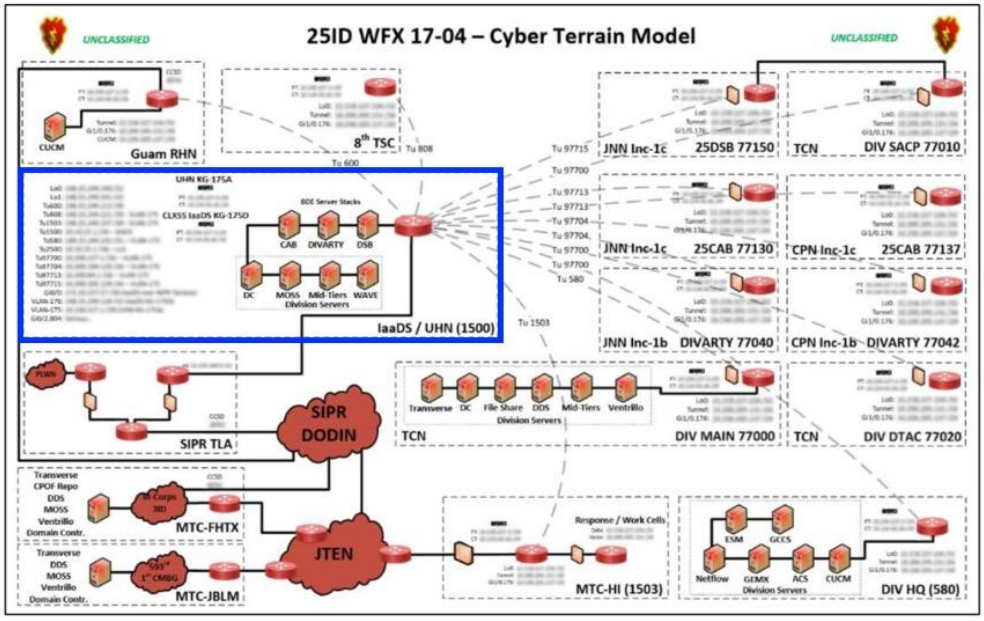


Figure 1. 25th Infantry Divisions Cyber Terrain Model for Warfighter 2017[20]

The IT world is constantly evolving as equipment continues to get smaller, faster, mobile, and more powerful. However, the driving force continues to be the network and access to it. In 2015, LTG Ferrell stated, “The Army Network is a fundamental enabler of mission command. A survivable, simplified and reliable network must support a common operating environment and common user experience throughout training, deployment, all operational phases and at all echelons.”[21] An increased reliance on the network through HSMCC and connection to the Army Private Cloud-Enterprise have stressed an already stretched architecture. The Army’s directed data center consolidation, in addition to dividing responsibilities between IMCOM and NETCOM, has and will continue to have, the unintended consequence that allows IT facility management to slip through gaps and create critical risk through network outages.

As an example of critical outages, Figure 2 is a 30th Signal Battalion/Hawaii NEC slide detailing four major outages in a twelve-month period that affected ongoing U.S. Army-Pacific and 25th Infantry Division operations. The four outages were all facility based and included cooling system failures, power outages, and electrical problems with the fire suppression system. The 30th Signal Battalion staff had no electricians, facility managers, facility engineers, or HVAC specialists. All support was provided by either local contracts or DPW, and in all cases response time was greater than one hour. As emphasis increases for information access from the cloud to the end user, facility management must become a core competency for IT facility owners. The commercial industry has approached this problem using Data Center Infrastructure Management.

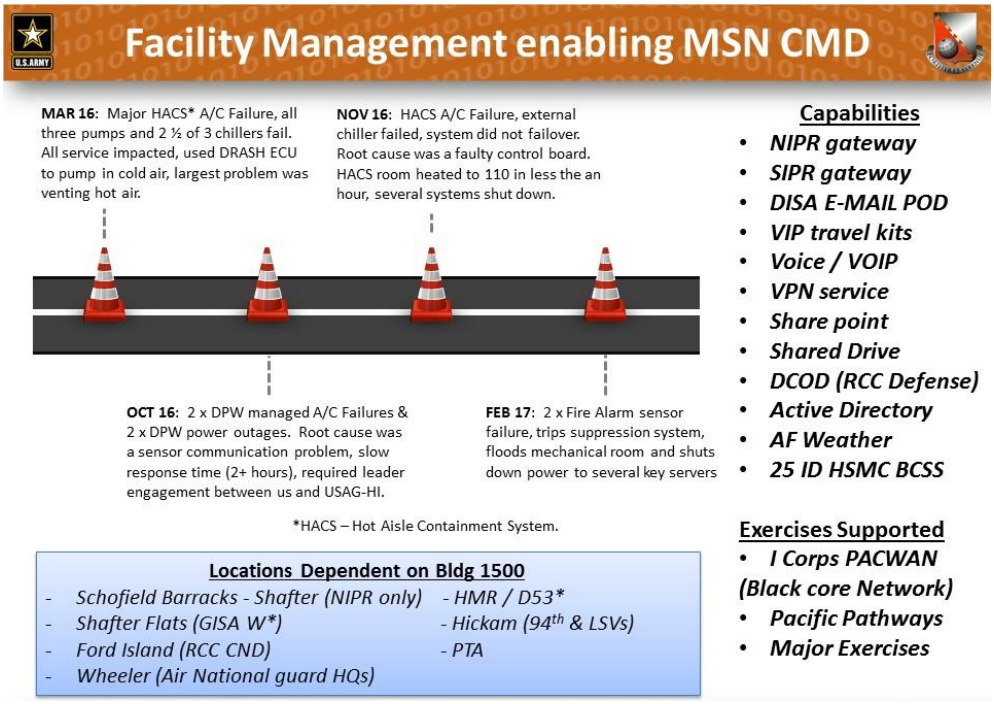


Figure 2. Facility Management Enabling MSN CMD[22]

Data Center Infrastructure Management

In 2010 the IT industry started to focus on monitoring and managing building infrastructure and spawned the DCIM market segment. While often sold as a software product, DCIM is also a solution, or framework, for how to holistically view the data center and its interdependent systems, both IT and facilities based.[23] The top metric in the data center industry is power usage effectiveness. While not perfect, it is effective in grading a data centers' effective use of power.[24] Arguably a more comprehensive metric to evaluate data centers is the Availability, Capacity, and Efficiency (ACE) performance score.[25]

Data center infrastructure management attempts to close the gap between facilities and IT by bringing data from both into a single common operating picture management.[26] Writing for the *American Society of Heating, Refrigeration, and Air-*

Conditioning Engineers' Journal in 2013, Donald Beaty defined DCIM: "The DCIM integrates the stove piped building management systems; IT management systems; power and electrical management; supervisory control and data acquisition systems and computerized maintenance management systems into a consolidated view that enables informed decision making and predictive analysis."[27]

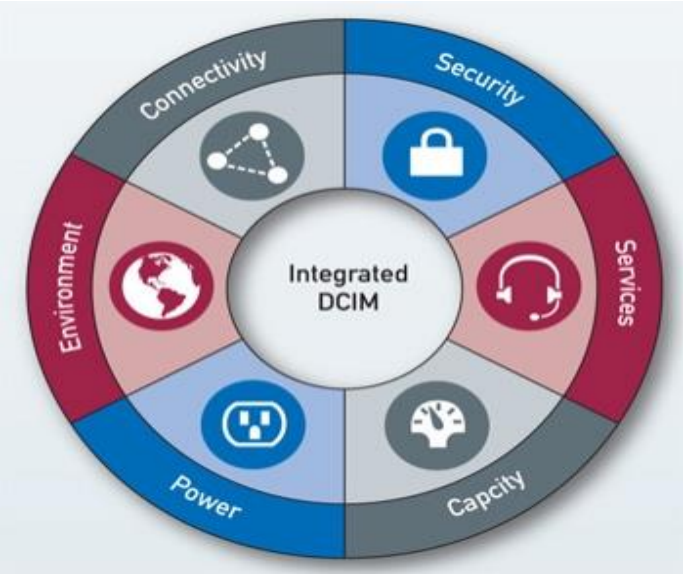


Figure 3. Integrated DCIM Framework[28]

The power usage effectiveness (PUE) metric was introduced in 2007 by The Green Grid to move the data center industry toward energy efficiency. Power usage effectiveness is calculated by dividing the total power consumed in a data center by the amount of power consumed by just the IT equipment. The resulting ratio indicates how much power is considered overhead, such as, for example, power that runs cooling systems or inefficiencies in the distribution chains.[29] A result of one is considered perfect with all facility power directly supporting IT equipment.[30] A result of 1.5 or less is considered efficient.[31] Conversely, a score of 2.5 or greater is considered inefficient with 40% (or greater) of the facilities power consumed by non-IT equipment.[32] The current

industry average, according to Uptime Institute, hovers between 2.0 and 1.7.[33] Power usage effectiveness is not currently measured at Army NECs, and, with responsibility for IT facilities split between IMCOM and NETCOM. it is unlikely the facilities would achieve a 2.5 or lower PUE.

Where PUE singularly focuses on power consumption, the ACE performance score takes a more holistic evaluation of a data center using three critical indicators. The ACE performance score evaluates Availability, Capacity, and Efficiency and considers their interrelationship represented as two triangles, an inner and outer. The inner triangle represents the actual performance at a given point in time for each category. The outer triangle represents the aspirational goal of 100% for each category. Availability tracks the IT service provided, including service provided during power or cooling failures. Capacity is the available assets to install, power, and cool additional IT equipment. Efficiency measures the effectiveness of the cooling systems in chilling IT equipment. Using the ACE performance score, a company can evaluate the three categories and quickly identify when an imbalance exists or risk in one exceeds a set threshold. The ACE performance score is used to inform future investment or risk decisions. In Figure 4, the initial assessment (left triangle) indicated the company had 97% availability but was inefficient (74%) and lacked capacity (86%). Using ACE the company chose to protect Availability and invest equally in Capacity and Efficiency (center triangle). This increased their Capacity but created an ACE performance gap in Efficiency (depicted in light blue) which highlights a known and accepted risk by the company (right triangle).[34]

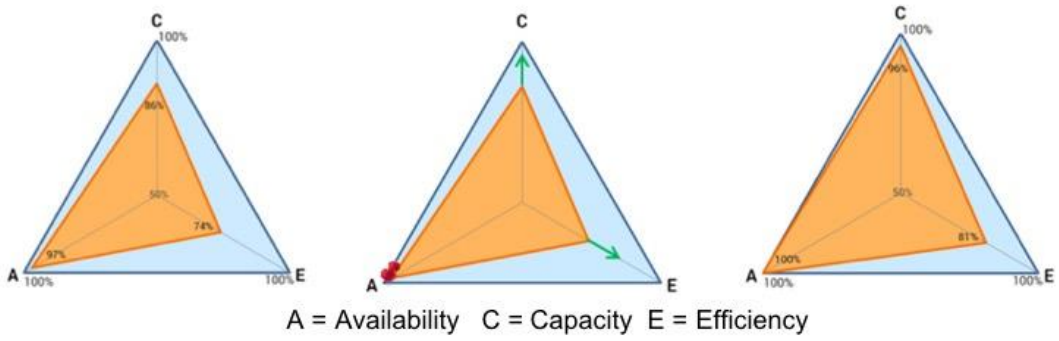


Figure 4. The ACE Performance Score[35]

If left unmanaged, data centers can be financial money pits. Based on hosting costs outlined in the Secretary of the Army's directive, it can be concluded this is the case in the Army.[36] A recent study by the Uptime Institute found that most large data centers produce 3.9 times more cooling capacity than required which translated to over 60% of the cold air supplied is wasted capacity.[37] In 2014 healthcare company Kaiser Permanente was recognized with the Brill Award for Efficient IT by instituting operational efficiency practices at four of their legacy data centers that netted a savings of approximately $10.5 million in electrical utility costs.[38] Strategic communication and a culture change are needed to implement DCIM as a framework and close the IT facility management gap that has developed between IMCOM and NETCOM. Closing this gap will reduce Army IT hosting costs and will increase the reliability and availability of enterprise data centers, installation service nodes, installation processing nodes, and special purpose processing nodes.

A Strategy for Implementation

Implementing DCIM will require a shift in culture away from traditional stove pipe lanes of IT management and facility responsibilities. A shift to DCIM answers a call to action put forth in two Army directives. On April 15, 2016, then acting Secretary of the

Army Patrick Murphy issued Army Directive 2016-16 calling for a change in behavior with his campaign “Every Dollar Counts.” His call to action required the Army to be good stewards of taxpayer dollars.[39] Also, as discussed earlier, former Secretary of the Army Eric Fanning called for a reduction in hosting costs in Army Directive 2016-38.[40] Even former Secretary of Defense Robert M. Gates pushed the department to move towards a “more efficient, effective, and cost-conscious way of doing business” in a speech at the Pentagon laying out his four-track approach.[41] Despite a call to action from three senior leaders, little progress has been made in the Army’s IT arena. A change in the Army culture to one that values IT facility management and implements DCIM is needed. An assessment of CIO/G6 strategic communication documents shows the need for a two-part approach addressing the issue. The first is using John Baldoni’s four I’s leadership message model for consistent senior leader messaging regarding DCIM.[42] The second is using John Kotter’s eight-stage process for creating major change too provide a framework for shifting Army culture towards DCIM.[43]

Strategic Communication

A review of current Army CIO/G6 published documents finds a cursory mention of facility management, mostly in the context of moving applications and data to approved enterprise hosting facilities, as in the Army Network Campaign Plan (ANCP) Mid-Term Implementation Guidance for 2018-2022.[44] The *ANCP Near-Term Implementation Guidance* 2016-2018 mentions hosting facilities more than any other document; however, it fails to discuss any kind of facility management and focuses, instead, on server virtualization and consolidation.[45] This oversight stems from the base document.

Published in February 2015, the ANCP's third line of effort (LOE) addresses network throughput and computing infrastructure; however, the objectives and definitions ignore the IT facility. LOE three defines the network in three layers: the global network, the transport network, and the computing infrastructure. The global network is defined as the physical portion of the network for processing and routing data, such as, for example, routers and switches. The transport network is infrastructure that moves data and includes wired and wireless networks, fiber optic cables, and satellite links. The computing infrastructure is used for storing and processing data like the end user device or servers.[46] This definition ignores the facility and building infrastructure required to support IT equipment with power and cooling. The IT facility is a critical network component that enables the desired end state of LOE three, which is "a secure, resilient and versatile global network infrastructure…."[47]

The ANCP details the key stakeholders, partners, customers, work force, policy makers, and community but fails to mention IMCOM, local garrison commands, or DPWs.[48] This omission is the most glaring example of IT providers taking the facility for granted. At a minimum IMCOM should be seen as a partner in the network campaign plan. Without a temperature-controlled environment, stable and consistent power, and on-demand backup power, the Army network will fail to achieve resilience. To effectively change the way IT facilities are managed, their importance must be communicated.

Figure 5. ANCP Key Stakeholders[49]

A recommendation to engage all leaders on the importance of IT facilities and the adoption of DCIM would be to use John Baldoni's four I's leadership message model.[50] In Baldoni's model, Inform, Involve, Ignite and Invite surround the leadership message. Baldoni believes leaders should inform people of the issues and what is required of them, involve others in the messaging and take their inputs, ignite the passions of organization around the message, and invite everyone to participate in the culture change. In surmising his model, Baldoni writes a successful leadership message is dependent on "including these four elements over and over again."[51] A recent example from the U.S. Army Chief of Staff is General Milley's number one priority of READINESS, where he has involved the entire Army, informed the organization of the issues, ignited a passion, and is inviting everyone to get on board.[52] General Miley's number one priority and Baldoni's four I's model present a roadmap for how to clearly communicate the critical importance of the IT facility and necessity to implement DCIM.

Furthermore, DCIM can be directly tied to facilities readiness and support General Milley's number one priority.

Culture Change

In John Kotter's book *Leading Change*, the author details the eight-stage process of creating major change and stresses two key factors. First, make the key assumption that any attempt at major change can be easily derailed for any one of a multitude of reasons.[53] Secondly, sequence is important and it is possible to perform several stages simultaneously; however, skipping phases or advancing quicker in later phases before earlier ones are complete can derail a transformation effort.[54] Kotter's eight stages are: establish a sense of urgency; create the guiding coalition; develop a vision and strategy; communicate the change vision; empower broad-based action; generate short-term wins; consolidate gains and produce more change; and anchor new approaches in the culture.[55] This analysis will focus on four of the stages: sense of urgency, guiding coalition, vision and strategy, and short-term wins.

John Kotter's first stage of change is to create a sense of urgency.[56] Army Directive 2016-38 created this urgency for DCIM when it directed the closure of 570 facilities by 2025, 358 of which were supposed to be complete no later than the end of fiscal year 2018.[57] Kotter states that to increase the level of urgency one has to reduce complacency. Two sources of complacency impacting the implementation of DCIM are the human tendency of denial, specifically for busy or stressed personnel and organizational structures that focus employees to a narrow set of skills.[58] When surrounded by pressing problems or tasks due yesterday, it can be difficult for individuals, managers, and even directors to see the larger problem, thus causing many to enter a state of denial to the existence of a problem.

For DCIM this has impacted local NECs as daily operations and crucial projects (major software upgrades, network transitions, life cycle replacements of network equipment) consume all available working hours. This can lead to a sense of denial towards a service, building power, or cooling systems that are currently working but not efficiently and, in some cases, not being maintained. Couple this sense of denial with organizational stove pipes where employees stay within their cubicles, focused on the task at hand, and potential exists for larger problems to go unnoticed until a failure occurs. The urgency from senior leadership has been established, but to drive it to the lowest levels these sources of complacency must be removed. A guiding coalition is needed to break through the complacency.

Kotter's second stage is the creation of a guiding coalition, an empowered and effective team that leads the change effort.[59] For DCIM to work, guiding coalitions would be needed at two levels: Department of the Army (DA) and the local installation level. At the DA level this group would include representation from CIO/G6, Army Cyber Command, NETCOM, DISA, and IMCOM. They would engage with the Assistant Secretary of the Army for Installations, Energy, and Environment to define the roles and responsibilities, capture fiscal requirements, potential savings, and institute metrics, such as PUE or the ACE performance score.[60] Ideally, data generated by the coalition would contribute to the Army Facility Investment Strategy.[61] The local coalition requires representation from the local NEC, DPW facilities team, DPW power generation team, DPW HVAC team, and local contracted expertise. This team should meet routinely to discuss and resolve conflicting maintenance schedules, conduct failure response rehearsals, and schedule major test events. The DA and local guiding coalitions with the

established sense of urgency and a supporting strategy could have an immediate impact across the Army and create lasting change for IT facilities.

John Kotter's third stage is the development of a vision and strategy that are easy to communicate, achievable, focused, and desired.[62] For the implementation of DCIM, the vision needs to describe the facility as an integral part of the network, equating it to the butt stock of a rifle or the wings of an aircraft. According to Kotter, the strategy is how to achieve the vision.[63] The strategy's end state is to make the facility and its supporting systems part of the warfighting network. This includes being resourced and life cycle managed as currently done with other critical network components (switches and servers). To achieve this end state, resources and capital investments regarding IT facilities should be executed in conjunction with the CIO/G6 and organizations running IT facilities. Altering the IT facility's structure to include facility engineers, facility managers, HVAC specialists, and electricians provides vested resident experts to inform investment and life cycle decisions. For smaller installations, one facilities team could support multiple locations; however, for major installations these are critical and must be resident to the IT organization. The means for this strategy include capital investments, personnel costs, budget increase to NETCOM, or an adjustment from IMCOM to NETCOM.

This strategy passes the suitability, acceptability, feasibility, and risk evaluation test. The strategy is suitable as it realigns resources, both money and manpower by conveying the high priority and a vital interest level. The strategy is acceptable to all stakeholders as it streamlines responsibilities and eliminates the friction between NETCOM and IMCOM organizations. The means for the strategy are not readily

available and will require budget restructuring and personnel transitions to support the strategy. The risk for executing this strategy is low; however, given the increasing reliance on the Army network, the risk of not implementing this strategy is high.

In order to build momentum, it is essential to capitalize on early short-term wins. Kotter describes this as the sixth stage of creating major change with the ability to build momentum and convert non-supporters or slow adopters into active assistants in the change effort.[64] Short term wins are easily achievable for DCIM and can be broken into three categories: power bill savings; PUE or ACE score; and obsolete server decommissions. Power bills are currently metered through DPW. A quick data call could collect current bills from all enterprise data centers, installation service nodes, installation processing nodes, and special purpose processing nodes to establish a baseline. On a quarterly basis the facility with the largest power bill reduction, by percentage, could then be recognized and rewarded with a reinvestment of the savings.

In *Leading Change*, Kotter captures the importance of incremental short-term wins to sustain change momentum.[65] The award for power bill reduction could begin immediately, while twelve months later the PUE or ACE performance score award could be deployed. A twelve-month delay will allow time for facility management teams to be hired and training occur. Unlike the power bill award, the PUE or ACE recognition should be tiered and facilities should be recognized and awarded for attaining certain thresholds. For example, if a facility achieves a score below 2.5, moving from ineffective to average range, the facility and management team should be recognized.[66] The long-term award would capture decommissions of unused equipment.

The Uptime Institute's Server Round Up award serves as an excellent template. The institute estimates 30% of a data center's servers are considered "comatose," meaning they are installed, drawing power, and producing heat but are not used. In 2015 Visa and AOL won the award for a combined savings in excess of $10 million. Visa decommissioned over nine thousand servers which enabled them to recoup 3,000 square feet of floor space and reduce their power consumption by 557 kilowatts, with expected savings of $3.2 million in 2016.[67]

Driving change requires mechanisms that enforce it. Edgar Schein provides a model that describes mechanisms as embedding and reinforcing. Embedding mechanisms are assumptions placed into an organization.[68] In their Organizational Culture paper, Gerras, Wong and Allen use the adage "Units do best what the commander checks."[69] Reinforcing mechanisms are those that support embedding mechanisms. Gerras, Wong and Allen describe reinforcing mechanisms as those that focus on organizational systems and procedures.[70] An example embedding and reinforcing mechanism related to a culture that values IT facility management is the embedded recognition program discussed earlier. The power savings, PUE or ACE performance score, and server roundup would reward both units and individuals that demonstrate the value of facility management, efficient systems, and cost savings. The reinforcing mechanism would be organizational systems and procedures that support the recognition program.

To effectively change an organization's culture senior leaders and stakeholders must fully commit to the change, communicate it at every opportunity, and significantly invest both time and resources. Reward programs that capitalize on short-term wins

staggered over a six-to-eighteen-month period will build momentum of culture change. Reinforcing and embedding mechanisms in support of short-term win reward programs will continue to generate momentum and inculcate the culture change. Finally, the CIO/G6 and senior IT leadership needs to embrace the Baldoni four I leadership message model to address IT facility management in published documents, speeches, interviews, and during command visits.

Managing Army IT Facilities in the Future

If the value of the IT facility was recognized and managed with the DCIM framework, there would be three distinct differences from today's environment. The first would equip Army data centers and processing nodes with certified technicians as part of their organic organizations. Second, there would be an established facility management working group chair by the facility owner and supported by external agencies, and, third, a standardized Army facility certification process. These three changes would increase the resiliency of Army data centers and processing nodes while simultaneously making their building systems more efficient and, thus, less costly to operate. The first step to realizing the improved resiliency and efficiency is to have the right experts on the team.

The implementation of DCIM requires that personnel with special skill sets in mechanical, electrical, and plumbing reside on staff at the organization operating the IT facility. This team would vary in numbers based on the size of facility, the supported population, and the scale of the installation but should include a facility manager, facility engineer, HVAC specialist, and electrician. They would perform inspections, preventative maintenance, and testing and oversee all contracted work for the installation's main IT facility and distribution nodes spread across the installation.

A critical task for this team is forming the nucleus of a facility working group that would meet routinely and build relationships with DPW, service vendors, maintenance contractors, utility providers, and suppliers. This working group would develop a maintenance schedule and tasks and create written procedures for preventive, predictive, and reactive situations.[71] The culminating event for this working group would be a yearly “pull the plug” test that would sever the utility supplied power. This test would validate all facility systems, including uninterruptable power supply, automatic transfer systems for power distribution and cooling, generators, the fuel supply, and validate the backup power capacity against the demand from the facility.[72]

Finally, a “pull the plug” test would be a critical component of a DISA or Army Cyber Command established facility accreditation process much like the tiered system used by the Uptime Institute.[73] This accreditation would be in conjunction with DISA’s new Command Cyber Operational Readiness Inspection and be a recurring event for the facility every two or three years.[74] The results from a facilities accreditation process would inform decisions regarding limited resources and clearly articulate risk to the facility leadership and mission critical customers.

Conclusion

This analysis has shown how the data center consolidation directive, the transition of IT facilities from IMCOM to NETCOM, the move to cloud-based computing environment, and fielding of home station mission command centers have dramatically increased the Army’s reliance on the building infrastructure of mission critical IT facilities. This dependency necessitates a culture change and the implementation of the commercial industry’s solution of the DCIM framework. The implementation of DCIM starts with consistent communication that identifies the IT facility as a critical component

of the Army network. To change the culture surrounding the management of IT facilities, leaders must recognize the sense of urgency, build guiding coalitions at the department and local levels, develop the vision and strategy, and then sustain the momentum through short-term wins and award recognition spaced out over eighteen months from inception. A future after DCIM implementation achieves the directed Army goal of reducing hosting costs and guarantees a resilient network with robust and reliable infrastructure.[75] As the CIO/G6 LTG Farrell said, a network that provides information as the point of need enables Soldiers "to make informed, more effective decisions as they perform the missions of the future."[76]

Endnotes

[1] James Hamilton, "Cost of Power in Large-Scale Data Centers," *Perspectives* blog entry posted November 30, 2008, https://perspectives.mvdirona.com/2008/11/cost-of-power-in-large-scale-data-centers (accessed January 9, 2018).

[2] Secretary of the Army, Army Directive 2016-38, *Migration of Army Systems and Applications to Approved Hosting Environments and Consolidation of Data Centers* (Washington, DC: Secretary of the Army, December 9, 2016), enc 2, 2, http://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/AD2016-38_Final.pdf (accessed October 21, 2017).

[3] Ibid.

[4] Ibid., 1.

[5] Ibid., enc 2, 3-4.

[6] Ibid., enc 2, 4.

[7] Ibid.

[8] Valerie Valentine, "Infrastructure Monitoring and Management Tops List of Data Center User Issues," June 2, 2010, https://www.information-management.com/news/infrastructure-monitoring-and-management-tops-list-of-data-center-user-issues?reconf=1 (accessed December 30, 2017).

[9] Grand View Research, "Data Center Cooling Market Analysis by Product (Air Conditioners, Precision Air Conditioning, Chillers, Air Handling Units), by Application (Telecom & IT, Retail, Healthcare, BFSI, Energy), and Segment Forecasts to 2024," July 2016,

http://www.grandviewresearch.com/industry-analysis/data-center-cooling-market (accessed December 30, 2017).

[10] George Seffers, "Mission Command from Afar," *Signal Magazine Online* (October 1, 2016): https://www.afcea.org/content/article-mission-command-afar (accessed December 29, 2017).

[11] Fort Jackson Leader Staff, "IT Organization Changes Affiliation, Name," October 8, 2009, linked from the *Army Home Page*, https://www.army.mil/article/28493/it_organization_changes_affiliation_name (accessed December 30, 2017).

[12] Tam Harbert, "Power Struggle," *Computerworld*, March 2, 2009, 26.

[13] Ibid.

[14] Secretary of the Army, Army Directive 2016-38, enc 2, 6.

[15] Tech Target, "Cloud Computing," July 2017, linked from the *TechTarget Home Page*, http://searchcloudcomputing.techtarget.com/definition/cloud-computing (accessed January 20, 2018).

[16] Office of the Army Chief Information Officer/G-6, *Army Cloud Computing Strategy*, (Washington, DC: U.S. Department of the Army, March 2015), 1.

[17] Greg Ferro, "Is Networking Infrastructure the Achilles' Heel of Cloud Computing?" February 2014, http://searchcloudcomputing.techtarget.com/feature/Is-networking-infrastructure-the-Achilles-heel-of-cloud-computing (accessed January 2, 2018).

[18] Osman Ocak, "SWOT Analysis of Cloud Computing," *International Journal of Advances in Computer Science and Cloud Computing Online* 3, no. 1 (May 2015): 62, http://www.worldresearchlibrary.org/up_proc/pdf/23-142951527728-31.pdf (accessed December 30, 2017).

[19] Seffers, "Mission Command from Afar."

[20] Brian M. Jorgenson, *25ID Warfighter 17-04 – Cyber Defense Overview*, White paper (Schofield Barracks, HI: 25ID, May 9, 2017).

[21] Robert Ferrell, "Enabling the Army Network for a Complex World," October 2, 2015, linked from the *Army Home Page,* https://www.army.mil/article/156585/enabling_the_army_network_for_a_complex_world (accessed December 29, 2017).

[22] Kevin MacNeil, "Facility Management enabling MSN CMD," briefing slide to U.S. Army Pacific Commander, GEN Brown, Wheeler Army Airfield, HI: 30th Signal Battalion, March 21, 2017.

[23] Donald L. Beaty and David Quirk, "Managing Infrastructure," *Ashrae Journal* 57, no. 6 (June 2015): 82, in ProQuest (accessed December 20, 2017).

[24] Donald L. Beaty, "Data Center Energy Metric," *Ashrae Journal* 55, no. 1 (January 2013): 61, in ProQuest (accessed December 20, 2017).

[25] Akhil Docca, Dave King, and Steve Davies, “Five Reasons Your Data Center’s Availability, Capacity and Efficiency Are Being Compromised,” March 26, 2014, 2-3, https://www.futurefacilities.com/resources/whitepapers/five-reasons-your-data-center-s-availability-capacity-and-efficiency-are-being-compromised (accessed December 20, 2017).

[26] Mark Harris, “Bridging the Gap Between IT and Facilities,” June 8, 2010, http://www.datacenterknowledge.com/archives/2010/06/08/bridging-the-gap-between-it-and-facilities (accessed December 22, 2017).

[27] Julia Geva, “DCIM: Where the Physical and Virtual Can Meet,” *Cabling Installation and Maintenance Magazine Online* (September 1, 2012): http://www.cablinginstall.com/articles/print/volumne-20/issue-9/features/dcim-where-the-physical-and-virtual-can-meet.html (accessed December 31, 2017).

[28] Ibid.

[29] Beaty, “Data Center Energy Metric,” 88.

[30] *42U*, “What is PUE / DCiE? How to Calculate, What to Measure,” linked from the *42U Home Page*, http://www.42u.com/measurement/pue-dcie.htm (accessed December 31, 2017).

[31] Ibid.

[32] Ibid.

[33] Uptime Institute, “2014 Data Center Survey Results,” June 4, 2014, *YouTube,* video file, https://www.youtube.com/watch?v=ZCRSeu60fxl (accessed December 30, 2017).

[34] Data for this paragraph was obtained from: Docca, “Five Reasons your Data Center’s Availability, Capacity and Efficiency Are Being Compromised,” 10.

[35] Ibid.

[36] Secretary of the Army, Army Directive 2016-38, 1.

[37] Matt Stansberry and Julian Kudritzki, “A Holistic Approach to Reducing Cost and Resource Consumption,” linked from the *Uptime Institute Home Page,* https://journal.uptimeinstitute.com/holistic-approach-reducing-cost-resource-consumption (accessed December 22, 2017), 8.

[38] Ibid.

[39] Secretary of the Army, Army Directive 2016-16, *Changing Management Behavior: Every Dollar Counts (*Washington, DC: Secretary of the Army, April 15, 2016), 1, https://www.army.mil/e2/c/downloads/441522.pdf (accessed October 17, 2017).

[40] Secretary of the Army, Army Directive 2016-38, enc 2, 1.

[41] Robert M. Gates, “Statement on Department Efficiencies Initiative,” public speech, Pentagon, Washington, DC, August 9, 2010, http://archive.defense.gov/speeches/speech.aspx?speechid=1496 (accessed October 17, 2017).

[42] John Baldoni, *Great Communication Secrets of Great Leaders* (New York, NY: McGraw-Hill, 2003), 32.

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

[44] Office of the Army Chief Information Officer/G-6, *Army Network Campaign Plan Implementation Guidance Mid-Term 2018-22* (Washington, DC: U.S. Department of the Army, n.d.), 1-2.

[45] Office of the Army Chief Information Officer/G-6, *Army Network Campaign Plan Implementation Guidance Near-Term 2017-2018* (Washington, DC: U.S. Department of the Army, n.d.), 1-7.

[46] Office of the Army Chief Information Officer/G-6, *Army Network Campaign Plan* (Washington, DC: U.S. Department of the Army, February 2015), 15.

[47] Ibid.

[48] Ibid., 11.

[49] Ibid.

[50] Baldoni, *Great Communication Secrets of Great Leaders*, 32.

[51] Ibid., 33.

[52] Timothy Hale, "CSA Milley: 'Readiness is my No. 1 priority,'" April 27, 2016, linked from the *Army Home Page*, https://www.army.mil/article/166838/csa_milley_readiness_is_my_no_1_priority (accessed October 18, 2017).

[53] Kotter, *Leading Change*, 20.

[54] Ibid., 23.

[55] Ibid., 21.

[56] Ibid.

[57] Secretary of the Army, Army Directive 2016-38, *Migration of Army Systems and Applications to Approved Hosting Environments and Consolidation of Data Centers (*Washington, DC: Secretary of the Army, December 9, 2016), enc 2, 2, http://armypubs.army.mil/epubs/DR_pubs/DR_a/pdf/web/AD2016-38_Final.pdf (accessed October 21, 2017).

[58] Kotter, *Leading Change*, 40.

[59] Ibid., 57.

[60] U.S. Army War College, *2015-2016 How the Army Runs, A Senior Leader Reference Handbook* (Carlisle, PA: U.S. Army War College, 2015), 16-2.

[61] Ibid., 16-13.

[62] Kotter, *Leading Change*, 72.

[63] Ibid., 71.

[64] Ibid., 123.

[65] Ibid., 120.

[66] *42U*, "What is PUE / DCiE? How to Calculate, What to Measure."

[67] Information in this paragraph came from the same source, see Uptime Institute, "Server Roundup Winners," linked from the *Uptime Institute Home Page,* https://uptimeinstitute.com/component/content/article/9-training-events/348-server-roundup-winners?Itemid=101 (accessed January 2, 2018).

[68] 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.

[69] Ibid.

[70] Ibid., 20.

[71] Fred Dickerman, "Building a Data Center Facilities Management Team from Scratch," linked from the *Uptime Institute Home* Page*,* https://journal.uptimeinstitute.com/building-data-center-facilities-management-team-scratch (accessed October 25, 2017), 2.

[72] DatacenterDynamics, "Pulling the Plug," July 4, 2006, linked from the *Datacenter Dynamics Home Page*, http://archive.datacenterdynamics.com/focus/archive/2006/07/pulling-plug (accessed January 1, 2018).

[73] Uptime Institute, "Uptime Institute Tier Certification's Value to the Multi-Tenant Data Center Market," November 29, 2011, *Uptime Institute YouTube Channel*, video file, https://www.youtube.com/watch?v=1Yli4flldp8 (accessed January 2, 2018).

[74] Signal Staff, "DISA Cyber Program Focuses on Operational Risk," March 29, 2017, linked from the *SIGNAL Home Page* at "The Cyber Edge," https://www.afcea.org/content/disa-cyber-program-focuses-operational-risk (accessed January 2, 2018).

[75] Secretary of the Army, Army Directive 2016-38, enc 2, 1.

[76] Office of the Army Chief Information Officer, *Army Network Campaign Plan*, 6.