Strategy Research Project

The Need for Old School Skills in a New School World

by

Colonel Douglas C. Van Weelden
United States Army

United States Army War College
Class of 2014

REPORT DOCUMENTATION PAGE

Form Approved--OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
15-04-2014	STRATEGY RESEARCH PROJECT	

4. TITLE AND SUBTITLE
The Need for Old School Skills in a New School World

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Douglas C. Van Weelden
United States Army

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Professor Ben Leitzel
The Department of Military Strategy, Planning, and Operations

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: 5,907

14. ABSTRACT

The United States Military has become increasingly dependent upon technology in the recent decades. While the use of technology and automation has improved the its effectiveness, the dependence upon that technology creates a vulnerability that is targeted by adversaries. The cyber domain is relatively new. As such, military technical capabilities are dependent upon it, yet the institution doesn't have the capacity or understanding of how to dominate this domain. U.S. forces must retain the ability to operate absent the technology that makes them so effective. U.S. military and defense strategies currently overlook or undersell this necessity. U.S. military forces need to train to operate in absence of technology. The level and depth to which this training and associated proficiency must be maintained correlates with the level of risk each force faces regarding cyber compromise or digital denial. Until the U.S. military is able to assure cyber dominance or supremacy, it must train service members to fight enemies absent of technology.

15. SUBJECT TERMS
Cyber, Cyberstrategy, Reliance on Technology, Dependence on Technology, Legacy Training

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	33	

USAWC STRATEGY RESEARCH PROJECT

The Need for Old School Skills in a New School World

by

Colonel Douglas C. Van Weelden
United States Army

Professor Ben Leitzel
The Department of Military Strategy, Planning, and Operations
Project Adviser

This manuscript is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

Abstract

Title:	The Need for Old School Skills in a New School World
Report Date:	15 April 2014
Page Count:	33
Word Count:	5,907
Key Terms:	Cyber, Cyberstrategy, Reliance on Technology, Dependence on Technology, Legacy Training
Classification:	Unclassified

The United States Military has become increasingly dependent upon technology in the recent decades. While the use of technology and automation has improved the its effectiveness, the dependence upon that technology creates a vulnerability that is targeted by adversaries. The cyber domain is relatively new. As such, military technical capabilities are dependent upon it, yet the institution doesn't have the capacity or understanding of how to dominate this domain. U.S. forces must retain the ability to operate absent the technology that makes them so effective. U.S. military and defense strategies currently overlook or undersell this necessity. U.S. military forces need to train to operate in absence of technology. The level and depth to which this training and associated proficiency must be maintained correlates with the level of risk each force faces regarding cyber compromise or digital denial. Until the U.S. military is able to assure cyber dominance or supremacy, it must train service members to fight enemies absent of technology.

The Need for Old School Skills in a New School World

Returning to base during a combat general aviation support mission in Afghanistan, the satellite radio in a UH-60 Blackhawk breaks squelch with a transmission from its higher headquarters. The command post is dynamically retasking the flight to perform a pick up for soldiers needing transport to Bagram Air Base. The command post transmits the grid coordinate for pick up, and the copilot immediately enters the data into the on board digital navigation set. With this done, he gives me steering guidance for the flight and an estimated time of arrival at the new destination. The pilot asks his crewmate for additional data for the new destination: what is the elevation of the new location, whose battlespace is it in, and is there any intervening terrain that they need to avoid? Silence follows as the young aviator struggles to find the information using a 1:250,000 scale map that he is unfamiliar with. After a transfer of flight controls, the pilot begins to leverage some “Old School” skills to answer these questions as his copilot keeps the aircraft straight and level following the navigation system’s steering guidance.

The United States Military has become increasingly dependent upon technology in the recent decades. Digital systems and networked technologies have increased the effectiveness, tempo, and lethality of U.S. forces. They have afforded Commanders at all echelons greater situational understanding and the ability to make rapid, effective decisions to defeat the nation’s enemies. While the use of technology and automation has improved the military’s effectiveness, the dependence upon that technology creates a vulnerability that is targeted by adversaries.

The threat to technology and networks is apparent and emerging every day. The cyber domain is relatively new. As such, military technical capabilities are dependent

upon it, yet the U.S. services don't have a capacity or understanding of how to dominate this domain, as one would argue that they do in the air domain. Early in the air domain's exploitation, military forces developed a means to operate in a non-permissive environment. Anti-aircraft systems and air defense tactics were needed in the land and maritime domains. This leads us to the question, how does the military operate in a non-permissive cyber domain while still undertaking combat operations against its enemies? U.S. forces must retain the ability to operate absent the technology that makes them so effective. Commanders must be able to establish situational understanding in absence of computer screens and command and control forces without technology. U.S. military and defense strategies currently overlook or undersell this necessity. U.S. military forces need to train to operate in absence of technology on a routine basis, in order to retain basic warfighting skills and to remain effective. Military personnel must retain the skill to manually perform the tasks that technology performs for them now. The level and depth to which this training and associated proficiency must be maintained correlates with the level of risk each force faces regarding cyber compromise or digital denial. Until the U.S. military is able to assure cyber dominance or cyber supremacy, it must train service members to fight enemies absent of technology.

Military Reliance on Technology

It will be instructive to first examine the depths of technologic dependence built into the military's warfighting machine. It has been argued that technology is the hallmark of the American way of conducting war.[1] It is ingrained into U.S. service cultures and drives how they formulate strategy. What makes present day technologic advances and the military application thereof any different than history? Simply stated, it is the military application of information technologies (IT) to network all elements of the

joint force on the battlefield. Commanders and military forces quickly share situational information, gain an understanding and exploit enemy weakness through rapid application of Commander's intent. Using digitally networked information systems for military application can be viewed as a revolution in military affairs, which is "… generally understood to be changes in military technology, concepts of operation, and military organizations which, over the course of perhaps two to three decades, transform the conduct of war …."[2] Applications of information technologies are changing the very way that the U.S. military fight wars. Historical examples of these revolutions include the invention of the firearm, the airplane and submarine. Use of information technology is so significant to the public's daily lives and now the U.S. military that the Defense Department established a sub-unified command under U.S. Strategic Command called U.S. Cyber Command (USCYBERCOM). Cyberspace has become a domain of its own, discreet from the Air, Land, Sea and Space domains that drove historical military focus and organization. Cyberspace as defined in Joint Publication 1-02, *Department of Defense Dictionary of Military and Associated Terms* is:

> A global domain within the information environment consisting of the interdependent network of information technology infrastructures and resident data, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers.[3]

Cyberspace is broad, and military applications are rife with examples of increasingly dependent capabilities on this new domain.

One of the most prevalent technologies to revolutionize military operations is the use of the Global Positioning System (GPS). GPS has evolved over time from just an aid to navigation to a system that now allows the military to attack targets with precision munitions. Precision Guided Munitions (PGMs) have become a mainstay of munitions

on today's battlefield. Roughly 8 percent of the munitions used in the 1991 OPERATION DESERT SHIELD/DESERT STORM were precision guided, while 68 percent were used in OPERATION IRAQI FREEDOM in 2003.[4] One can only anticipate the use of these munitions to increase in the future. Because of the increased accuracy the public now expects military operations without collateral damage. This could limit the acceptability of imprecise weapons in the future. Political and military leadership can ill afford the use of destructive force that results in the suffering of innocents. The speed and prevalence of today's media can turn an unfortunate incident into an immediate public outcry with strategic significance. The reliance upon GPS continues to grow, but it is not the only technology that the military is becoming increasingly dependent upon.

Digital Command and Control Systems are potentially the hallmark technology of the conflicts in Iraq and Afghanistan.[5] At the time of the United State's invasion of Iraq, the US Army had one digitally enabled Division. The 4th Infantry Division was the Army's test bed for digital enabling. The Division conducted numerous exercises and training events to test and develop digitally networked land forces. The concept held that if a unit could instantaneously share a common understanding of the environment and the commander's intent, it could then mass and exploit the enemy's weaknesses. In essence, seeing more clearly and then deciding and acting more rapidly than an adversary. Upon commencement of ground combat operations digital command and control systems rapidly proliferated the battlespace. Chief among them was a system known as Force XXI Battle Command Brigade and Below (FBCB2) also commonly referred to as Blue Force Tracker (BFT). This system combines geo-referenced position data via satellite based transponders to provide accurate location data for any friendly

units equipped. Over time, this data and this system have been integrated into higher echelon command and control systems, giving Commanders and tactical forces a clear picture of the friendly forces information. The systems also allow operators to input enemy or threat data, assisting with the formulation of enemy situation as well. As the applications and utility of BFT grew, the number of systems on the battlefield increased.[6]

Information technology is integral to the way the U.S. employs military forces. Its capabilities are found at headquarters from tactical through strategic. The reliance on these systems and capabilities might be best proven in the priority and approach that the military gives to it. This is emphasized in the 2010 *Quadrennial Defense Review Report* (QDR):

> There is no exaggerating our dependence on DoD's information networks for command and control of our forces, the intelligence and logistics on which they depend, and the weapons technologies we develop and field. … DoD currently operates more than 15,000 different computer networks across 4,000 military installations around the world. On any given day, there are as many as seven million DoD computers and telecommunications tools in use in 88 countries using thousands of warfighting and support applications.[7]

Clearly the military is reliant upon technology to conduct combat operations. Its incorporation into what is commonly referred to as Net Centric Warfare (NCW) provides military Commanders with an amazing ability to speed up decision cycles and improve the accuracy of decisions made. When combined with a young fighting force, known as "digital natives" who are adept at the employment and use of technology, the results can overwhelm an adversary. As a decisive capability, technological dependence also presents itself as a critical vulnerability.

Threats and Vulnerabilities to Technology

There are multiple aspects inherit in technology that make it vulnerable to loss, manipulation, or disruption. Nations and non-state actors are targeting these vulnerabilities. The information technologies that the military uses are largely constructed on a network model. This network is composed of data processors that generally serve as network nodes. These components are the computers, servers, GPS navigation processors, and other equipment that interface with the digital information. Each node is then connected by some means of data transmission. Most commonly this transmission occurs over physical wire, fiber optic lines, or through the electromagnetic spectrum. Tied into this data transmission component is infrastructure that serves as a means to redirect transmissions, such as terrestrial based routers and satellites. The network, in order to function requires some source of power to run the nodes and power data transmissions. Each component; the power, the nodes, and the transmissions possess vulnerabilities that can threaten high tech military systems.

The vulnerability to network nodes is real and apparent. Data processing hardware and software are vulnerable to manipulation, exploitation, and destruction. Computer code can be manipulated and inserted into a network that can destroy capabilities or create serious disruption. Computer viruses are well known for affecting software. These viruses or malicious code can then be used to extract data from systems or to manipulate the systems processes. A recent example includes the United States' own alleged efforts in developing and employing a virus known as Stuxnet.[8] This virus was used to impact Iran's nuclear program by manipulating computer controlled processes that eventually destroyed a number of atomic centrifuges.

There is also risk of adversaries altering computer hardware to affect a network, and in fact this may be one of the best ways to impact a secure network. This nodal vulnerability concerns manipulation of hardware and devices at the point of manufacture or post-manufacture manipulation. Given the fact that technology advances well ahead of defense acquisition cycles, much of the equipment used by the military is commercial off-the-shelf (COTS) purchased. This limits military acquisition system oversight of the manufacture process and ability to identify affected equipment. There is evidence that counterfeit hardware has already been detected in some of the systems procured by the military.[9] A recent news report alleges that the National Security Agency (NSA) has actually developed a means to intrude into computer systems not connected to the internet. Nefarious individuals can covertly insert a circuit into a device that when manipulated causes the computer system's hardware to communicate via radio signal without the operators awareness or approval. The user interfaces and network nodes are certainly vulnerable and so are the connections between them.[10]

Data transmissions, the links between networked nodes, also present a vulnerability to military technology and networks. There are two primary means for the transmission of electronic data from node to node.[11] One means is via hard line application. These lines can be traditional metal wire or fiber optic. The second means is wireless, via some type of transmission in the electromagnetic spectrum.

Hard line data transmissions are vulnerable to both physical attack as well as intrusion by a potential evil doer. As a physical entity, adversaries can target the destruction of transmission lines with simple means, especially where those lines are inadequately secured. Today's internet transmissions often travel via large undersea

cables that are prone to attack or natural disaster.[12] Potentially more vexing would be if these lines were compromised and spliced into. This would allow an adversary the capacity to potentially manipulate the entire network, reaching far deeper than if the line was simply lost.

The second means of data transmission is potentially the most vulnerable. Transmissions via the electromagnetic spectrum are unsecured (physically) and susceptible to interception and jamming. The transmissions can be secured via encryption, but this does not protect them from interception and jamming. Currently electronic data is transferred between devices using various electromagnetic means and gives networks far reaching and dynamic power. This means is used for GPS communication and long range data transmissions via satellite communications. These transmissions, once released, can be jammed to preclude receipt by other devices. The ability to jam GPS signals is becoming more prevalent and concerning to military users.[13] It has been reported in one instance that Iran may have brought down a U.S. unmanned drone by jamming its GPS signal and hacking its data link connection.[14] The military is pursuing procurement of jam resistant capabilities in light of this threat.[15] A key link of this long range electromagnetic transmission structure is satellites.

Satellites are integral to the GPS system and long range tactical data transmissions where hard lines are unavailable. Satellites also present a vulnerability to the military's technology and network structure as they are susceptible to physical attack or environmental influences. Both China and the United States have demonstrated the capability to eliminate satellites in orbit from earth-based launch platforms.[16] In light of this demonstrated capability, other nations are now pursuing

similar capacity.[17] In addition to direct attacks on satellites, they are becoming increasingly vulnerable to destruction via debris in space or loss due to aging.[18] There can be no doubt that military data transmissions face threats and are vulnerable. Even with protected transmission mechanisms and nodes, there is still a critical element of vulnerability.

Electrical power serves as the locomotive to process and transmit data on information technology networks. Without electricity, information technologies and cyber space fail to exist. The military has built a great deal of protection and redundancy in its power generation and power transmission abilities, but these are not foolproof. One need simply look at the aftermath of any major natural disaster to see the vulnerabilities and shortcomings associated with the production and transmission of electrical power. During the aftermath of Hurricane Sandy, it took an estimated 10-13 days to restore power to 95 percent of customers.[19] The estimates following Hurricane Katrina were much worse. There are military systems under development that can impact electricity, known as electromagnetic pulse (EMP) weapons. Nuclear weapons are known to produce potentially devastating EMP effects that could deny major electrical power use for extended periods of time.[20] The military possesses unit level, small-scale power generation capabilities that would guard against a complete loss of power for technologic applications. However, these capabilities may prove insufficient to powering all nodes and transmissions of a military operational network.

There is a clear reliance by the U.S. military on technology and clear threats to that reliance. The U.S. military and defense cyber strategy to defend the nation’s

military technologic superiority is emerging. Several national defense and military strategic documents address the cyber domain.

The Protection Strategy

With a demonstrated reliance on technology and the emerging threats, the military has taken action to address the vulnerability of this capability in strategic documents and guidance. First and foremost, emphasis is being placed upon and a capacity built to defend the networks. The second aspect of the military's strategy for retaining technological capacity is through redundancy of capability. The military is working diligently to build protection capabilities and to ensure operations continue with minimal interference should network defense fail. The Defense Department's QDR and Defense Strategic Guidance documents, along with the Chairman of the Joint Chiefs of Staff's National Military Strategy and the USCYBERCOM's strategy all account for the reliance on cyberspace and the threats to that reliance.

The Defense Department's 2010 QDR recognizes the importance and reliance upon cyber and technologic capabilities. This strategic document addresses four steps the department is taking in order to strengthen cyberspace capabilities. The steps are: developing a comprehensive approach to DoD operations in cyberspace, developing greater cyberspace expertise and awareness, centralizing command of cyberspace operations, and enhancing partnerships with other agencies and governments.[21] These actions are moving the military closer to the goal of cyber dominance or control. The QDR recognizes however, that there is operational risk associated with not being able to defend its systems in cyberspace. The mitigation to this risk is that "… DoD mission-critical systems and networks must perform and be resilient in the face of cyberspace

attacks."[22] The document's discussion regarding the operational risk in essence cedes failure in the event of a digitally denied environment.

The updated 2012 Defense Strategic Guidance, *Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense* updates defense strategy from the 2010 QDR. This document is designed to realign defense strategy in light of operations winding down in Iraq and Afghanistan, as well as constraining fiscal and budgetary realities. In this guidance, the Defense Department iterates the importance of the cyber domain to military operations.[23] It further states the importance of defending the networks and cyber capabilities, but does not address the need for capabilities in light of digital denial.

Following the publication of the 2010 QDR, but prior to the most recent Defense Strategic Guidance of 2012, the Chairman of the Joint Chiefs of Staff published the 2011 National Military Strategy. In this document, then Chairman Admiral Mullen addressed the significance of the cyber domain to military operations and the threats posed. While the strategy states, "We must grow capabilities that enable operations when a common domain is unusable or inaccessible;"[24] it is intended to convey the need for cross domain synergies. While specifically addressing cyberspace the strategy states that given a large scale intrusion or debilitating attack the military must, "… provide a broad range of options to ensure access to and use of the cyberspace domain …."[25] Thus, the ability to conduct combat operations in a digitally denied environment is alluded to, but not specifically addressed. Providing options to ensure access may not be available with present day capability, making this aspect of the military strategy unsuitable.

In July 2011 the Department of Defense published its *Strategy for Operating in Cyberspace*. In this document it poses the employment of new defense operating concepts to defend networks and systems. There are essentially four concepts to achieve this goal: enhancing cyber hygiene, deterring and mitigating insider threats, employing an active cyber defense capability, and developing new defense operating concepts and computing architectures.[26] The USCYBERCOM Commander, dovetailing with this DoD strategy, expounded on his Command's efforts in testimony to Congress in March of 2013. He stated that working together with the NSA the Cyber Command forces are creating: a defensible cyber architecture; global situational awareness and a common operating picture of the cyber domain; a concept for operating in cyberspace; a trained and ready force to operate in the domain; and capacity to take action in the domain when authorized.[27] He further elaborated on each of these priorities, but in essence spoke about the necessity to develop a defensible network and then monitor activities in the domain and respond to threats with a dedicated force trained and enabled to do so.

In order to further assure continuity of operations in cyberspace, the military has recognized the need to create network resiliency and redundancy. The second line of effort is returning a disabled network to operational status with minimal disruption or having the capacity to operate on a separate network. The Defense Department's Strategy for Operating in Cyberspace acknowledges:

> In the case of a contingency involving network failure or significant compromise, DoD must be able to remain operationally effective by isolating and neutralizing the impact, using redundant capacity, or shifting its operations from one system to another. Multiple networks can add diversity, resiliency, and mission assurance to cyberspace operations.[28]

Having a system with the ability to regenerate quickly, or having a backup system certainly lowers the impact on that system. The issue at hand is the gap between a strategy focusing on network defense and redundancy and the need to conduct combat operations in light of a failure to defend or provide redundant networks. The immaturity of these strategies and associated capabilities required to execute them, along with the illustrated vulnerabilities to the military's technology creates a gap for which the U.S. military must be prepared to address.

Addressing the Strategy/Vulnerability Gap

It is clear that the U.S. military is moving boldly forth with an ever increased reliance on technology and operations in the cyber domain. The Defense Department is developing strategies designed to protect its friendly freedom of action. These strategies are immature and do not address the vulnerability of or need to operate in a cyber denied environment. Nation states and non state actors around the globe are developing and procuring means to deny the U.S. military its use of technological overmatch. If successful, military forces must still perform warfighting tasks and functions to achieve strategic end states and defend national interests. Performing these tasks in "Old School" fashion may be easier said than done. Legacy skills, or performing tasks in an "analog mode" is currently unrealistic.

U.S. forces have been training and developing tactics, techniques, and procedures (TTPs) on digitally enhanced and networked systems for over a decade. As U.S. forces become reliant on these systems, and continue to reinforce their capabilities and power, there is evidence to suggest that their ability to perform those tasks in "analog mode" has eroded. It was with relative frequency during combat missions in Afghanistan that copilots were unable to navigate without the aid of the GPS. Further,

these aviators failed to recognize when the GPS malfunctioned, which was usually due to a system error and not enemy action. This was troubling because the system would continue to provide erroneous navigation information that could have impacted mission success. Similar issues have been identified in studies of civilian aviation.

The Federal Aviation Administration (FAA) conducted a study, published in September 2013 regarding the dangers of commercial pilots becoming increasingly reliant upon on board flight management systems. The report investigated several aviation accidents over recent years and tied significant findings to pilots' reliance on the integrated aircraft technology. First, the study found that pilots' increased reliance and use of on board automated flight management systems eroded their basic flight skills.[29] It found further that in 60% of the accidents studied, inappropriate manual flight skills were a factor in the incident. This has far reaching impact to the U.S. military's perceived ability to transition combat operations from digital to "analog mode" without disruption or impact to the mission. The FAA study further found that pilots who became reliant upon these digital onboard systems in many cases, failed to recognize when the system was failing or providing erroneous data.[30] This is consistent with observations of military aviators and also could have serious impact on a major combat scenario. If an adversary were able to access and manipulate friendly command and control systems, would it be recognized prior to being exploited? An adversary could potentially create an artificial current operating picture that causes U.S. commanders to become confused, make inappropriate decisions, and in worst case scenarios, lead to the defeat of friendly forces.

The loss of “analog mode” capabilities and skills can be analyzed using behavioral and learning theory. There is a long held saying in common vernacular, “use it or lose it.” A lot of study and research has gone into how humans learn skills and tasks, then subsequently retain those skills and tasks for later recall. The level and depth to which a person learns a task or skill initially will play heavily into how well that skill is recalled at some later date.[31] Further, after initially learning a skill or task, the ability to recall becomes more difficult as the time of disuse increases.[32] The ability to perform tasks and skills in “analog mode” is directly attributed to how well the skill was initially learned and how often it is performed or practiced. Drawing on the example of the copilots in Afghanistan, it is likely that these pilots were not trained to the level and degree needed to recall manual navigation skills. Further, they were not required to perform those skills on a recurring basis. Pilots traditionally developed their skills in a relatively analog environment regarding aerial navigation. They were exposed to a two week long low level navigation course during Initial Entry Rotary Wing Training. Their primary responsibilities as a newly assigned aviator in the operational force included the navigation function for missions. This level of initial training followed by rigorous reinforcement training afforded them better recall of that skill, even though they too were becoming reliant upon the GPS navigation capability. Today’s Army Aviators receive a quick introduction to analog navigation in initial entry training, and once assigned to units rarely navigate in this manner.[33] Given the GPS capability, and the need to train on its operation and functions, navigating by pilotage and dead reckoning (“analog mode”) is usually only trained once a year by aviators, and subsequently evaluated once a

year.[34] These training requirements are developed and overseen through the Aviation proponent under the Army's Training and Doctrine Command (TRADOC).

Army Aviation determines these training event and iteration requirements via its Center of Excellence (USAACE) under TRADOC.[35] USAACE's Directorate of Training and Doctrine (DOTD) receives input to training requirements and demands in multiple ways. There are the trainers at the schoolhouse, subject matter experts, representatives from the Directorate of Evaluations and Standardization, and Commanders in the field providing input on training demands from the current operating environment. TRADOC strategic capabilities assessments based upon approved futures scenarios provide input on training demands from the future operating environment. From these inputs, the DOTD develops course material and training requirements that are ultimately approved by the Aviation proponent Commanding General. It is a relatively holistic approach to identifying training demands and developing the training doctrine.

The system is designed to identify training requirements that fulfill strategic capabilities. Like other aspects of military's overall defense management construct, decisions to add a trained capability will generally come with an additional fiscal burden, unless offset by a reduction in other training requirements. One reason for the shift away from "analog mode" training time and emphasis could be this fiscal tension and the benefit provided by digital capability. In order to keep overall training costs from rising, "analog mode" training is sacrificed to support additional digital systems training. These issues highlight a further dilemma regarding learning and retention that challenges the future fighting force.

The millennial generation, also known as the digital natives, is the cohort of the future fighting force. This group of 18-29 year olds has grown up entirely surrounded by technology, and as a result is very adept at the use, implementation, and exploitation of technologic capabilities.[36] This is and continues to be a boon to the military as it moves forward to leverage technology to overmatch future adversaries. The potential also exists however, that this demonstrated aptitude and reliance on technology could make the military more vulnerable in a digitally denied environment. This cohort is less well versed in “analog mode” operations due to their digital foundation and the transformation of U.S. education and training systems to accommodate the digital learning environment.[37] Given what is known about task recall, and it being a function of the depth of initial learning, this group may not possess the ability to rapidly adapt to “analog mode” operations in a digitally denied environment. The millennial generation represents the tip of the spear of the U.S. military. They are the personnel who are responsible for receiving, processing, interpreting, and disseminating information within the military command structure. In essence, they are the executing element of the Commander’s mission command function. If unable to transition effectively to an “analog mode” of operation when needed, the results could be disastrous to U.S. forces and the execution of warfighting tasks and missions. There is recent evidence to support that the current force lacks capability in transitioning to and executing warfighting tasks and functions in “analog mode”.

The U.S. Army is transitioning its forces from its decade long deployment cycles in OPERATIONS IRAQI FREEDOM and ENDURING FREEDOM. Given the demand for forces and capabilities in those two operations, the Army focused on training and

preparation for those conflicts. These combat zones served as a rich laboratory to test and improve the military's use of technology and operate in the cyber domain to leverage against adversaries. However, there were few if any challenges to the U.S. military's superiority in the cyber domain. The transition from this wartime stance and training model is shifting and the Army recognizes the need to focus on the full spectrum of potential conflicts. The Army's training centers began training cycles to address full spectrum capabilities and are conducting what are now being called Decisive Action Training Environment (DATE) training rotations.[38] Army Brigade Combat Teams encounter the rigors of a full spectrum environment in an immature theater of operations. The units are facing cyber warfare during these rotations, mostly being challenged with cyber intrusion and network defensive tasks.[39] While the training does not inject a threat induced digital denial component, the units are denied digital capability as a result of the theater immaturity and forcible entry requirements. The units are deploying into an environment where established networks and cyber capabilities do not exist. As forces enter an immature theater, or find themselves maneuvering against enemy forces, they have to operate in absence of some of their mission command enabling technology. In immature theaters, networks need to be established or expanded to accommodate a maneuvering force. These units are finding that they are not adequately trained to perform necessary mission command tasks in "analog mode"; this is especially true for their younger, less experienced members.[40] As Army units move away from operating in fixed based, established command posts and into those that are more mobile in nature, the need to train "analog mode" operations is becoming more apparent.

Clearly the need for “analog mode” capability exists. Until the day comes where the United States is capable of gaining and maintaining cyber domain superiority, as it accomplished in the air domain, it must retain the ability to fight and win in a digitally denied environment. Actions taken by the military henceforth will assure the ability to fight and win, thereby assuring the Nation’s security.

Recommendations

Given the military’s vulnerability to the denial of technology, it must take action to ensure it ability to fight and win against any and all future adversaries. There are steps that can be taken to ensure success in the full spectrum of potential conflicts. The U.S. military cannot give up on the incredible capability that technological solutions afford. It also cannot stop performing warfighting tasks and functions when those systems are denied.

First and foremost, the military must continue to explore the cyber domain and work toward dominating it when necessary. To ensure the military’s ability to leverage technology over adversaries, it must develop strategies, tactics, and forces designed to fight, win, and dominate in the cyber domain. Clearly the current military strategic documents reflect that desired end state. The U.S. military is currently short of that end state, and while that does not mean it should abandon these goals, it does mean that it must address the lingering vulnerability gap. The national defense and military strategies must highlight and iterate the need to retain capability when denied use of the cyber domain, and not just the need to defend domain access. Adding this emphasis in strategic documents will highlight the need for “analog mode” capabilities in U.S. forces. The way in which the services address this gap is dependent on several variables.

The first variable is addressing the organization's risk to digital denial and the need for "analog mode" capabilities. Each of the military services and the individual organizations within them need to assess the nature of their vulnerability in light of the potential threat of digital denial. It is possible that certain echelons of forces are at low to no risk of mission failure in a digitally denied environment. Certainly an infantry platoon should be able to perform its warfighting functions to fire and maneuver on enemy forces, even absent digital enhancement. The brigade-level or joint task force-level headquarters above that infantry platoon may be significantly challenged to accomplish their necessary functions in that same environment if not trained to do so in an "analog mode". Each organization will have a different vulnerability or risk of failure under digitally denied conditions. Leaders should direct a risk assessment to determine the level and degree of focus each unit should take to train and maintain an analog capability to conduct combat operations.

The second variable is determining individual levels of learning and retention of "analog mode" tasks. Units should conduct organizational risk assessments to determine the need for analog capability. Before commanders can determine training requirements, they will need to further assess the individual proficiency levels within their units. The demographic composition of the organization will be a strong determinant into the amount of training required and the frequency of refresher training.

Fundamentally, the answer lays in the commander's assessment. Each commander must assess their unit's capability to operate in a digitally denied environment and assess the required level of proficiency based on the unit's mission. If the need and the required level of proficiency are high, more time and intensity will be

required to achieve and sustain that level. Younger organizations with a lower base of knowledge and proficiency in “analog mode” will require more intense training initially, and more frequent reinforcement to sustain the capability. There will admittedly be the challenge of training to dominate adversaries with technological overmatch while retaining the ability to dominate in a digitally denied environment. Military commanders must strike the necessary balance of training between digital and analog skills based upon risk and readiness imperatives.

Conclusion

While sounding incredibly intuitive, U.S. military strategy and doctrine appear to overlook the need for forces to operate in an “analog mode” of operation. The strategy addresses the need for operating in degraded environments, but appears to wishfully think that digital denial is not a realistic possibility. The U.S. military has become increasingly reliant upon technology as it leverages this technology to overmatch adversaries. Those adversaries recognize their reliance, and are effectively developing, and have developed means to deny digital capabilities and the ability to leverage that technology. As the U.S. military moves further away from the mature theaters of combat operations that it has operated in over the last decade, the weaknesses associated with atrophied skills in the “analog mode” of operation are becoming apparent. Until the U.S. military achieves the capability to assure cyber dominance and superiority, its forces must retain “analog mode” capabilities to fight and win on the battlefields of the future. Old school skills are perishable and still needed in this new school world.

Endnotes

[1] Thomas G. Mahnken, *Technology and the American Way of War Since 1945* (New York: Columbia University Press, 2008), 1-2.

[2] Andrew Marshall, “Introduction,” in *The Revolution in Military Affairs: Warfare in the Information Age,* ed. Keith Thomas (Canberra, Australia: Australian Defence Studies Centre, 1997), 3.

[3] U.S. Joint Chiefs of Staff, *Department of Defense Dictionary of Military and Associated Terms,* Joint Publication 1-02 (Washington, DC: U.S. Joint Chiefs of Staff, November 8, 2010), 64, http://www.dtic.mil/doctrine/new_pubs/jp1_02.pdf (accessed January 11, 2014).

[4] Mahnken, *Technology and the American Way of War Since 1945,* 209.

[5] Gregory Fontenot, E.J. Degan, and David Tohn, *On Point: The United States Army in Operation Iraqi Freedom* (Ft. Leavenworth, KS: Combat Studies Institute Press, 2004), 416.

[6] James Conatser and Thane St Clair. "Blue Force Tracking - Combat Proven." *Armor* 112, no. 5 (Sep, 2003): 20-3, http://search.proquest.com/docview/205342302?accountid=4444 (accessed February 20, 2014).

[7] Robert M. Gates, *Quadrennial Defense Review* (Washington, DC: U.S. Department of Defense, February 2010), 37, http://www.defense.gov/qdr/images/QDR_as_of_12Feb10_1000.pdf (accessed January 12, 2014).

[8] Chris Demchak, “Hacking the Next War”, *American Interest* (September/October 2012), http://www.the-american-interest.com/articles/2012/8/10/hacking-the-next-war (accessed January 14, 2014).

[9] William J. Lynn III, "Defending a New Domain." *Foreign Affairs* 89, no. 5 (Sep, 2010): 97-108, http://search.proquest.com/docview/749414296?accountid=4444 (accessed January 14, 2014).

[10] David E. Sanger, Thomas Shanker, “N.S.A. Devises Radio Pathway Into Computers,” *The New York Times*, January 14, 2014, http://www.nytimes.com/2014/01/15/us/nsa-effort-pries-open-computers-not-connected-to-internet.html?_r=0 (accessed January 16, 2014).

[11] Certainly this statement discounts the possibility of transmission via portable data storage. This is discounted as the time and physical proximity required for this type of transfer would render the process obsolete. The nodes would in this case be unconnected, and therefore not networked.

[12] "Indian Ocean Cable Suffers Outage." *Ocean News & Technology* 17, no. 4 (May 2011): 62, http://search.proquest.com/docview/868192867?accountid=4444 (accessed January 23, 2014).

[13] "Out of Sight; GPS Jamming." *The Economist*, Jul 27, 2013. 51, http://search.proquest.com/docview/1413237761?accountid=4444 (accessed January 10, 2014).

[14] Charles A Barton III, "Global Positioning System is a Single Point of Failure." *Signal* 67, no. 2 (10, 2012): 59-62, http://search.proquest.com/docview/1318557307?accountid=4444 (accessed January 10, 2014).

[15] "Raytheon to Produce Military GPS Anti-Jamming Antenna System," *Satellite Today*, February 27, 2009, http://www.lexisnexis.com.ezproxy.usawcpubs.org/hottopics/lnacademic/?verb=sr&csi=277894&sr=HLEAD(Raytheon%20to%20Produce%20Military%20GPS%20Anti-Jamming%20Antenna%20System)%20and%20date%20is%202009 (accessed January 23, 2014).

[16] Barton, "Global Positioning System", 59-62.

[17] Ibid.

[18] Richard Crowther, "Space Junk--Protecting Space for Future Generations," *Science* 296, no. 5571 (May 17, 2002): 1241-2, http://search.proquest.com/docview/213575325?accountid=4444 (accessed January 23, 2014).

[19] Jonathan Fahey, "Power Outages After Hurricane Sandy Weren't Unusually Long After All," November 16, 2012, http://www.dailyfinance.com/2012/11/16/power-outages-after-hurricane-sandy-werent-unusually-long-after (accessed January 14, 2014).

[20] R. J. Woolsey, "The Ultimate Cyberthreat: Nuclear EMP Attack." *Hampton Roads International Security Quarterly* (July 1, 2013): 22, http://search.proquest.com/docview/1373225743?accountid=4444 (accessed January 14, 2014).

[21] Gates, *Quadrennial Defense Review*, 38.

[22] Ibid., 91.

[23] Leon E. Panetta, *Sustaining U.S. Global Leadership: Priorities for the 21st Century Defense* (Washington, DC: U.S. Department of Defense, January 2012), 5, http://www.defense.gov/news/Defense_Strategic_Guidance.pdf (accessed January 12, 2014).

[24] Admiral Michael G. Mullen, *The National Military Strategy of the United States of America,* (Washington, DC: Office of the Chairman of the Joint Chiefs of Staff, February 2011), 9, http://www.army.mil/info/references/docs/NMS%20FEB%202011.pdf (accessed February 23, 2014).

[25] Ibid., 10.

[26] Leon E. Panetta, *Department of Defense Strategy for Operating in Cyberspace* (Washington, DC: U.S. Department of Defense, July 2011), 6, http://www.defense.gov/news/d20110714cyber.pdf (accessed January 11, 2014).

[27] *Senate Armed Services Committee Hearing*. Testimony by Keith Alexander, Commander, U.S. Cyber Command, Lanham: Federal Information & News Dispatch, (March 12, 2013), http://search.proquest.com/docview/1316575988?accountid=4444 (accessed January 11, 2014).

[28] Panetta, *Department of Defense Strategy for Operating in Cyberspace,* 6.

[29] Federal Aviation Administration, *Operational Use of Flight Path Management Systems: Final Report of the Performance-based Operations Aviation Rulemaking Committee/Commercial Aviation Safety Team Flight Deck Automation Working Group* (Washington, DC: Federal Aviation Administration, September 5, 2013), 31-33, http://www.faa.gov/about/office_org/headquarters_offices/avs/offices/afs/afs400/parc/parc_reco/media/2013/130908_PARC_FltDAWG_Final_Report_Recommendations.pdf (accessed January 10, 2014)

[30] Ibid., 36-44.

[31] Ben Leonard, "Literature Review on Skill Fade," *Human Factors Integration Defence Technology Centre,* May 25, 2007, 5, http://www.hfidtc.com/research/training/training-reports/phase-2/2-10-3-2-skill-fade.pdf (accessed January 15, 2014).

[32] Ibid., 4.

[33] Aviators are trained in a block titled Basic Warfighting Skills (BWS). This is a 19 flight period/20 flight hour block of instruction where aviators are taught analog mode of navigation in conjunction with a myriad other tasks. While a longer period of time than the author's personal training experience, the author's two week block was focused on analog mode navigation. The author's point regarding insufficient depth of initial learning is valid in light of the competing tasks learned/performed. See: U.S. Army Aviation Center of Excellence, *INITIAL ENTRY ROTARY WING AVR (COMMON CORE): Flight Training Guide* (Fort Rucker, AL: USAACOE, March 5, 2013), 21, https://www.us.army.mil/suite/doc/39528786 (accessed January 23, 2014).

[34] U.S. Department of the Army, *Aircrew Training Manual, Utility Helicopter, H-60 Series,* Training Circular 3-04.33 (TC1-237) (Washington, DC: U.S. Department of the Army, May 10, 2013), Chapter 2, Training.

[35] Information regarding detailed processes of training development found in: U.S. Army Aviation Center of Excellence, *Training Development (TD),* USAACE Regulation 350-70 (Fort Rucker, AL: U.S. Army Aviation Center of Excellence, March 9, 2012), https://www.us.army.mil/suite/doc/39674105 (accessed February 24, 2014); U. S. Army Training and Doctrine Command, *Force Development: United States Army Training and Doctrine Command Standard Scenarios for Capabilities Development*, TRADOC Regulation 71-4 (Fort Eustis, VA: Headquarters U. S. Army Training and Doctrine Command, February 12, 2014), http://www.tradoc.army.mil/tpubs/regs/TR71-4.pdf (accessed February 24, 2014); and U. S. Army Training and Doctrine Command, *Training: Army Learning Policy and Systems*, TRADOC Regulation 350-70 (Fort Eustis, VA: Headquarters U. S. Army Training and Doctrine Command, December 6, 2011), http://www.tradoc.army.mil/tpubs/regs/TR350-70.pdf (accessed February 24, 2014).

[36] Paul Taylor and Scott Keeter, eds., *Millennials: A Portrait of Generation Next: Confident. Connected. Open to Change* (Washington, DC: Pew Research Center, February 2010), http://pewsocialtrends.org/files/2010/10/millennials-confident-connected-open-to-change.pdf (accessed January 23, 2014).

[37] Martin Nikirk, "Teaching Millennial Students," *The Education Digest* 77, no. 9 (May 2012): 41-4, http://search.proquest.com/docview/1010398596?accountid=4444 (accessed January 23, 2014).

[38] Dennis Steele, "Decisive-Action Training Rotations: 'Old School without Going Back in Time'," *Army* 63, no. 2 (February 2013): 26-37, http://search.proquest.com/docview/1282532092?accountid=4444 (accessed January 23, 2014).

[39] Ibid.

[40] Curtis A. Buzzard, "MAP BOARDS TO CPOF," *Infantry* 100, no. 2 (April 2011): 10-3, http://search.proquest.com/docview/892471864?accountid=4444 (accessed January 16, 2014).