STRATEGY RESEARCH PROJECT

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

THE SYSTEMS ADMINISTRATOR: STRATEGIC SLUSH IN THE UNIT DEPLOYMENT PROCESS

BY

LTC (P) MICHAEL C. COX
United States Army

19980605 076

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

USAWC CLASS OF 1998

U.S. ARMY WAR COLLEGE, CARLISLE BARRACKS, PA 17013-5050

DTIC QUALITY INSPECTED 4

The Systems Administrator: Strategic Slush in the Unit Deployment Process

by

LTC(P) Michael C. Cox

COL Lynn W. Rolf, Jr.
Project Advisor

The views expressed in this paper are those of the author and do not necessarily reflect the views of the Department of Defense or any of its agencies. This document may not be released for open publication until it has been cleared by the appropriate military service or government agency.

U.S. Army War College
Carlisle Barracks, Pennsylvania 17013

DISTRIBUTION STATEMENT A:
Approved for public release.
Distribution is unlimited.

ABSTRACT

AUTHOR: Michael C. Cox, LTC(P), US Army

TITLE: The Systems Administrator: Strategic Slush in the Unit Deployment Process

FORMAT: "USAWC Strategy Research Project"

DATE: 06 Apr 1998 PAGES: 39 CLASSIFICATION: Unclassified

Computer systems and networks are complex. The military systems are constantly being upgraded to provide those capabilities that will enable the U.S. Army and other services to meet the information dominance needed to defeat adversarial nations and competitors. The Army must rely on the Systems Administrators (SAs), who have the responsibility to control and manage the systems to ensure they work. Yet the SAs are not getting the proper training, management guidance, or command support to meet the demands of these new systems. With no strategic policy to standardize SAs training, no skill identifier to track those who are good SAs, and little understanding of the SAs job, commanders are only beginning to realize they cannot meet the U.S. Army's mission in the 21st century without better trained SAs to manage the technologically complex systems of the future.

TABLE OF CONTENTS

Abstract.....iii

List of Illustrations.....vii

Systems Administrators Are Critical.....1

Computers...critical today.....3

Technology is complex.....6

Systems administrator functions.....8

Systems administrator positions.....13

Strategic Policies for Systems Administrators.....15

No skill identifier.....16

No centrally managed SA technical training.....17

Little command emphasis.....18

Critical nature of the systems administrator.....20

Managers and supervisors of SAs.....21

Conclusions.....24

Recommendations.....25

Endnotes.....27

Bibliography.....31

LIST OF ILLUSTRATIONS

Figure 1. Typical SA Functions.....09

Figure 2. SA's Time, Training, and Command Support.....16

Systems Administrators Are Critical

In the process of shifting the emphasis from a forward based Army to a power projection force with most units based in the United States, military leaders have overlooked a critical piece of the deployment process. Commanders have long been trained and evaluated on their abilities to fight the nations battles. With this new shift in location of the forces, there has not been an equal shift in the training or evaluation of the ability of commanders to get to the battlezone. Units deployed for training at the National Training Center (NTC) are evaluated on how the battles are fought at the NTC, but not on their ability to get to the NTC. When the 25th Infantry Division deployed from Hawaii to take over the mission in Haiti in 1995, the deployment process was delayed at the port. They arrived with equipment that was not the same as the lists of equipment they sent forward for planning purposes.[1] The Unit Movement Officer is responsible for entering the correct data, and the Systems Administrator is responsible for configuring the automated systems to get the proper data to other systems and people for planning purposes.

The thesis of this paper is to show that commanders and managers throughout the military rely extensively on automation, but these leaders have not grasped the importance of the computer systems administrator who

provides a vital service to the commanders in linking the systems together to allow critical information to be passed during deployments. If computers are not configured properly so critical data flows to the planners, a strategic hole in the deployment process is created which may cost the United States the next war.

Systems administrators should manage the critical linkage between the system they administer and other systems. However, they are not getting the proper training, they are not understood by management or commanders, and they are not getting the support they need to provide proper automation management. As the military moves into the 21st century, it will enter an era marked by the absolute requirement to have information superiority or risk losing the war. To take full advantage of the technological revolution or system of systems to provide this information superiority, new operational procedures and organizations are needed.[2] First in the U.S. commitment to prepare for an uncertain future is to "Pursue a focused modernization effort in order to replace aging systems and incorporate cutting-edge technologies into the force to ensure continued U.S. military superiority over time."[3] Systems administrators who have had little training now, are looking to a future of even more complex automation as outlined by strategic leaders today.

Computers...critical today.

Computers have become an absolutely critical part of the business processes in the United States today. Business processes have been established over time in order to standardize and become more efficient. New technology made it possible to enhance the business process and allow workers to produce more for the company. The sequence of developing the automated tools included a business process review just to develop the computer application. This often enhanced the business process: sometimes trimming off unneeded aspects of the process, sometimes combining two or more processes, and sometimes actually adding to the business process just to automate the process but resulting in better records. The US military incorporated the automation capabilities available into its business processes to take advantage of the same efficiencies as other businesses in the US. The military has passed the point where it could fall back on manual procedures.[4] Today the Army is "reinventing its business practices" to further improve efficiencies and provide integrated systems to meet the advanced needs of the future.[5, 6]

Most companies succeeding today have added new capabilities or have taken on new missions to be able to produce more profit. As additional workload is added to the

process and workers are asked to do more with less, automation has been able to partially offset the added work. Automation can provide enhanced tracking of data, can pass specific information to other segments of the workforce, or may pass the completed results of one office to another office entirely which takes that output and creates something else. The military put automation into specific areas to: track requisitions in the logistics area, store information for the intelligence community, calculate the monthly paycheck for personnel, and help in the paperwork generated at the local command. As the Army moves toward the Force XXI concept, it "seeks to exploit the revolutionary and continually advancing changes in technology to offset the reductions in military funding and personnel."[7] In the future the joint service vision is to achieve information superiority with advanced technology such that the military will not have to rely as heavily on massed forces or sequential operations.[8] In the international arena, the U.S. will continue sharing information and intelligence with other nations to counter terrorism, corruption, money laundering activities and help fight drug trafficing.[9]

In recent years US managers have made a determined push to reduce the costs of production, both in the commercial market as well as in the military. This has frequently been

aimed at reducing personnel. With the inclusion of automation, many businesses have reduced middle management and allowed higher management to use automated tools to replace the work done previously by the middle managers. Although some automation shops were set up to run the computers, many offices justified automating their business processes by showing more productivity in the end by fewer workers using the new automation.

The military has also embraced automation to a great extent. In the process, base or installation office locations were affected as well as the battlefield workplaces. Most units today must have automation which can be used either in the office or on the battlefield, so they do not have to change systems when they transition from peace to crisis or war.

Computers have become critical to the business process today, often to a degree that an office cannot function if the systems are down. Military units are no exception. Commanders have embraced automation to assist in the production and correction of the enormous amount of paperwork they must do. Legal offices have automated to track the changes to legal documents used daily. Intelligence systems have been created to help keep track of all the myriad of bits of information used in monitoring potential adversarial nations and competitors.[10] Even one

of the Army's imperatives is modern equipment.[11] According to the President of the United States, "In order to maintain the technological superiority of U.S. forces, we must selectively increase modernization funding to both introduce new systems, and replace aging Cold War-era equipment."[12]

Technology is complex.

Most individuals want to do their job better, and automation has helped them do that. However, many people do not understand some basics about the computers they use. The computer on their desk today is usually linked to others in a Local Area Network (LAN) so information can be passed easily to others who need it. Large computers, often known as mainframe computers, are linked into LANs or sometimes Wide Area Networks (WANs) so those needing a lot of computing power can do the complex part of their processing in the large computer and then finish the rest of the work at their desk computer. Hence, there is an image in the workplace that the computer can do the hard work by simply sending the hard jobs to larger computers and bringing the answers back.

Another issue that is widely misunderstood is that systems administrators can add demonstration software to office desk computers easily. Often demonstrations show the

flashy exotic state of the art. The concept is that if the demonstrated flashy software could be put on the desk computers at work, then office jobs would be so much easier. Demonstrators push the idea that a disk or compact disk (CD) is all that is needed to easily add these capabilities onto the computer at the office to get the enhanced tools. Frequently these vendors do not describe the complexity of linking this software into the multiple data base files that must be linked for the new software to work. The license to run the software may cost more as well. With as many computers linked as we typically have in a standard office or unit today, just adding the software to the network such that it will benefit those who need it is not easy. It requires careful orchestration to ensure that the new software does not create more problems for another part of the office as it helps one part of the office.

In military units security must be built in as well. Commercial businesses may require security to protect their interests, but typically the military has to have the security so that lives are not lost. Adding the security to an automated system creates another dimension of complexity to an already complicated system. Some automated systems only require passwords to protect the system from unauthorized users. Other systems require very complex tables which identify every element of a data base and who

is authorized to see each field.

Several computer companies have stated that the life cycle of computers today is about 18 months. New computers that are incorporated into a system today at one unit, will soon be outdated. When additional automation is added to the system, the complexity becomes more difficult to fully understand as new technology is linked with old or outdated equipment. Incompatibility among automated management systems was identified as the leading of two major causes for turbulence in the logistics area, not solely relating to systems administrators, but demonstrating the complexities of automation systems today.[13]

Just linking all the computers in one office today is complex. But with the ability to tie them to the internet or wide area networks, the local area networks have the added complexity of the network links and hooks in them. Something that worked on the LAN can be corrupted by something that comes in from the network. The systems administrator is the person to orchestrate linking the complex systems of today.

Systems administrator functions.

So what exactly does a systems administrator do? Figure 1 lists the main functions or duties of a systems administrator. Each duty will be described in more detail

below.

Typical SA Functions

1. Complete Knowledge of Hardware.
2. Complete Knowledge of Software.
3. Orchestrate Physical Changes to System.
4. Control Upgrades to the System.
5. Properly Tune/Link All System Components.
6. Test and Accredit the Functional System.
7. Control Local and External User Access to the System.
8. Control Data Base Administration.
9. Administer Virus Protection.
10. Technically Document Upgrades for Procurement Actions.

Figure 1. Typical SA Functions

An SA must have a thorough knowledge of the system or systems involved. The SA must understand not only the software, but have a good understanding of the hardware, how the two work together, and the uniqueness of each aspect of the system parts. This enables him[14] to control the new parts that are added to the system to ensure they work properly for those intended, and do not preclude the automation that has been established to help another part of the unit or office.

The SA also must protect the systems and the information stored there. To do that, he uses security software to protect the data and control access to the system. Especially in the military, and the same issues apply for any business, those who have access to the system should be able to do their work which entitles them to view

certain things and work in certain areas. They should not have access to other parts of the system such as the payroll. Should someone that is not authorized try to access the system, the security software will deny him access. Security software includes the passwords and the control of them. It also may include specific access codes for each individual on the system to access each data field in the data base. It commonly includes specific software to control passing of data to other nets when an individual accesses those other nets.

There may be several data bases associated with the system on the LAN or connected by communications. Those data bases must be kept usable. This usually includes controlling who has authority to update each field in the data base. Additionally, it may include who has access to read or change each field or the access to it. A data base administrator (DBA) may be assigned to assist the SA, but if the DBA is not available or is not assigned, the SA has that responsibility. The SA specifically has the responsibility to establish user links to get to the data base for each person who should have access.

Commercial off the shelf (COTS) software is regularly purchased by military units and must be loaded onto their systems. Additionally, the versions of the COTS software on the systems are regularly updated by the companies that

produce them. An example of this is the recent upgrade of Microsoft Windows from Windows 95 to Windows 98 or Windows NT. Thus, software is constantly being loaded onto the system to aid in the business process. The SA has the responsibility to load this software so that it still uses all the files previously generated by the workers and that it still works with all the rest of the parts of the systems. The SA must create all the necessary links to the data bases so they work. More recently, the SA must also load new versions of virus protection software. If the SA has not loaded the latest version of the virus protection software, the older version of virus protection software may miss a virus that gets sent into the system from some data transmitted through the internet or LAN. A virus can corrupt not only the individual workstations but could also corrupt data bases, network control software, links to other networks, or even corrupt the ability for the system to start properly.

With a complex system, the SA must be able to tune the various parts to work properly together. This is accomplished by loading proper LAN commands into the software to allow various workers to access the system in short time segments on a priority basis. Should one individual cause a large document to be printed, the controlling task in the computer which prints documents to a

specific printer would store a copy of the document for printing. Then it would send a part of the document to the printer because the printer may not have enough memory to load the entire document at one time. While the printer is busy printing part of the document, the task releases the main computer processing power to do other things until the printer needs some more data to print. With the computer properly tuned, everyone has some time on the main computer as necessary to download data and to send data across the LAN or internet.

An SA also frequently has the responsibility to procure software that is needed for the system. This may include meeting with the president of the company, the commanding officer on the post or base, and working with the financial advisors to determine what is needed or wanted and is affordable by the higher authorities. Once the software is purchased there may be training that is required to load the software separate from the training needed to operate or use the software. The SA must properly load the new software and get it operational for those users that need it. Since few in the unit understand the system as well as the SA does, he is usually involved in describing the software needing to be purchased.

An SA must also coordinate upgrades to the system. This may be in conjunction with regularly scheduled

maintenance downtimes, or it may be scheduling time to shut the computer network down on the base at a time it will not greatly impact the mission. Frequently the downtime is used to perform other maintenance as well. Some software or hardware can be loaded or connected to the system with the system running, but other times the system has to be shut down to all the customers for the new equipment or capabilities to be properly added to the system.

Any new aspect or capability of the system is under the jurisdiction of the SA for testing to ensure it works properly. Testing can be as simple as sending a document to the newly added printer and checking to see if it prints. On the other hand, testing can include a very detailed test plan which calls for complex test data to be loaded at hundreds of terminals on a specified test schedule, and the results compared to specific expected outputs. Frequently the printouts of the operations of the system must be analyzed before the test can be certified as a success. This usually must happen before users can use the system for what it was designed to do. All testing must be under the supervision of the SA so he can monitor and ensure the system functions as it should.

Systems administrator positions.

The systems administrator position is a job that

frequently gets listed as an additional duty. The SA position in the English Department at West Point, up to as recent as 1996, was an additional duty with responsibilities for over 50 terminals.[15] The person selected may have had some previous computer experience, or may not have. Most of the time, the commander selects someone who may be thought of as a computer geek--someone who has learned a bit about computers regardless of his other skills or his military occupational specialty (MOS). If there is not a person in the command that has had some computer experience, then the next most likely person to get the additional duty will be the signal officer because of his communications experience.

Usually an SA has many tasks to do. Unfortunately, the SA tasks are commonly listed as an afterthought with all the other tasks that must be done--a reflection on the command that they do not understand the importance of the SA duties.

Writing the job description with enough details to get the position permanently established has not happened in most units or at many installations. Since Table of Organizational and Equipment (TOE) units are established primarily to support the warfighting commanders in chief (CINCs), this would be a critical position if the commanders knew how important the job is. Unfortunately, most commanders rely on the computers but just know they must work. The link to the SA has not been made in their minds

yet. Units with a Table of Distribution and Allowance (TDA) have some flexibility in establishing a wider spectrum of specialties, and in some cases, even hiring contractors to do specific functions.

Strategic Policies for Systems Administrators

There are virtually no strategic policies for SAs. With other military systems, such as wheeled vehicles, tracked vehicles, electronics, or medical equipment, there is always a mechanic or trained operator to care for the equipment. This technician is responsible for properly maintaining the system, helping the common operators of the system, and sending the equipment to higher level repair shops for maintenance as required to keep the system properly functioning. Although automation has achieved higher numbers of systems throughout the military units than any other system, there are no systems mechanics established yet to aid the common users. This paper will explore job skill identifiers, training, and command emphasis as they relate to the critical position systems administrators hold in a unit or on base.

A small sample of systems administrators is listed here in figure 2 showing how many years each individual has served as an SA, how much training they received for the

position, and the support they received from the command. Particularly note the brevity of the training.

Name	Time as SA	Tng Received	Cmd Spt
James[16]	4 yrs	2 weeks	Personality driven
Johanson[17]	8 yrs	2 weeks	Understands only concept
Luebke[18]	3 yrs	self taught	Only a crisis gets $
Sum[19]	8 Yrs	1 week school	Personality dependent
Woods[20]	2 yrs	6 weeks school	Midlevel improving

Figure 2. SA's Time, Training, and Command Support

No skill identifier.

One of the first places to check concerning policies must be with the enlisted, officer, or civilian personnel systems. The ability to effectively manage personnel is based upon tracking them in the systems and dividing requirements to them based upon their individual progress through their career skills. However, there is no special identifier in either the military or civilian personnel tracking systems to identify a person that has the skills of a systems administrator. The Warrant Officer skill 251 was originally identified as an SA, but those positions have systematically and almost completely been eliminated from military units. The officer skill 53 deals with automation management, but unless the individual has personally sought

out special training, the 53 specialty does not contain the technical training necessary to be an SA. With no skill identifier for trained personnel, each time a person moves to another assignment, he will be assigned to the primary MOS skill for which he is in the military or civilian support of the government. If the previous assignment was particularly rewarding, or if that individual especially enjoyed working on computers, he may step forward and try to get a similar assignment at the new station outside the primary reason for which he moved there. But with no use of the MOS established for this purpose and no skill identifier for those who have worked in this area before, anyone who may have had significant training as an SA will not be known to the gaining commander.

No centrally managed SA technical training.

Each systems administrator must gain the systems knowledge by attending schools that teach those specific skills needed. For COTS software, this almost always requires an individual to go to civilian schools, or schools run by contractors. Automation programs frequently have SA courses taught as a part of the training available for the system. However, this training is not centrally managed by the Army, nor are specific standards established for each system. Even schools centrally managed for training users,

as in transportation at Fort Eustis, or military intelligence at Fort Huachuca, do not train SAs.

Systems administrators have to go to schools that teach about the operating system on the computers they deal with in order to understand those techniques necessary to tune them. With each application teaching only those skills necessary to fine tune that specific application, an SA frequently does not get the necessary overall skills to make the conglomeration of applications and the network of systems into the most efficient tool for the users.

Training time is critical for an SA. As each new application is procured, there needs to be some time for the SA to acquire the SA level training. However, with few SAs, a unit cannot spare the time for an SA to go temporary duty (TDY) to get all the training desired. The timing of the SA training may not match the schedule the SA can work into his schedule. And although there are requirements for the unit to complete its mission, there is little emphasis from the higher command levels for the commander to specifically send the SA to training. The complexities and critical nature of automation, though available as additional classes, is not part of the core of the US Army War College ciriculum.[21]

Little command emphasis.

A typical example of the lack of attention given to

systems administrators is the evaluations given commanders for sea emergency deployment readiness exercises (SEDREs). There is an evaluation for the commander on whether he departs the post on schedule, but no mention of the correctness of the data required to be entered for the transport of the unit from the post to the port. Documented evidence shows that typically the data received at the port is only about 25% accurate, causing considerable delay in loading the ships, and extra charges for the ships delay in the port.[22] In the logistics world, inaccurate data "led to loss of visibility of those personnel and equipment which were not processed correctly; the loss of visibility caused users and logisticians alike to lose confidence in the systems that were supposed to prevent such outcomes."[23] It is not the systems administrators responsibility to enter the transportation data, but the unit movement officer (UMO) needs to get the data correctly entered so it can be processed properly. If the SA did not get the system correctly set up or tuned, whatever data that may have been entered may have been corrupted or not sent forward correctly to those who needed it. Correct transportation data has become absolutely critical with the shift in emphasis from a forward deployed military to a power projection military force.[24]

In Europe a unit had been trained on a system, but with

the SA leaving on a permanent change of station due to an emergency medical problem, the system could not be accessed for about 6 months because no one knew the password. The knowledge of who to contact and how to use the system was lost as the previous SA departed the unit.[25]

Critical nature of the systems administrator.

With an emphasis from the computer demonstrators that the systems are easy to set up, and a mentality that PCs are simple to operate, there is a trend to think networks are simple to operate efficiently. While there are many more tools today than in the past that can ease the burden of the SA, the job is not easy. In the early days of the United States military, the job of the horse trainer was difficult. He had to break the horses before they could be effectively harnessed to do the will of the soldiers. Not every soldier could break horses, but once the horses were broken, it was much easier for every soldier to master the skills necessary to use the horses in significantly benefiting the entire unit. Just as the horse trainer worked in the western expansion of the frontier in the 1800s, so today the SA has the responsibility to harness the capabilities of the computers of today. If the SA effectively manages the computers, they can be utilized by the average military individual going into the 21st century to achieve the

information dominance required.[26]

Some managers strongly suggest the SA job should be contracted out to the experts. This could be considered similar to the push in the military during the early 1980s to contract out those non core capabilities of the military, such as the cooks and doctors. Most installations went to centralized mess facilities and contracted out the management of them to include the cooks. Yet when units went to the battlefield, they still needed to eat. While Brown and Root could be contracted to prepare meals in crisis areas or have the food prepared in the rear areas and hauled to the front, some cooks are still needed. Doctors can be contracted at the installation area, but when the need to go to war takes place, lives are lost in the battle area if doctors are not available to care for the wounded at that time and in that area. Similarly, systems administrators must be available in the area to keep a system up and functioning during the battle when fluctuations in power or environment may cause the system to need retuning. The cost of contractors in a danger zone is usually increased by a minimum of 50% and is rarely under $150K per person per year.[27]

Managers and supervisors of SAs.

The attitudes of managers of the systems administrator

have a lot to do with how the SA works in the unit or office. If the attitude is one of understanding the job of the SA or each element of the unit, the commander will usually support the SA in the appropriate level of training and functioning of his job. However, many commanders or office supervisors concentrate on the aspects of the position that they enjoy, those aspects of the position that helps them look good in front of their boss, or those aspects of the position that seem to always have problems. The SA job frequently gets left out of those reviews, because the SA job is complex to explain to a boss and because what an SA does is not something easy to articulate. Hence, the SA gets lip service when it comes to support of the function, and told he cannot leave for training due to responsibilities to keep the system up and running.

Does a manager understand the job of an SA? Usually the manager does not. Since the SA job is quite technical and specialized for the particular computer equipment involved, the manager regularly tells the SA to "do a good job" but could not really tell if the SA was doing a good job or not. The computers could be up and operating well, but the SA may have been responsible for upgrading the software and did not apply the upgrade package.

Another problem that plagues managers is getting support for the automation budget. Because automation costs

are high, someone who did a poor job of setting up the equipment may have departed the area leaving the critical upgrade to someone new. That may require a new person to approach the command with a substantial expense to make the system functional. Just as the new system is coming on-line, new technology may come out which requires the software or hardware to be upgraded in order to stay under the maintenance contract. This process of keeping up with a very rapidly advancing and expanding technology while reducing personnel and improving efficiencies makes the automation managers job complex while trying to keep with the military's five year planning cycle.[28] Since that area may be short of personnel in a downsizing environment and the civilian counterpart gets paid two to ten times as much for the same job, it is difficult to get and keep good automation managers today.[29] In ten years or so, the SA job will be easier because midlevel managers will have grown up in an automated era unlike today's midlevel managers some of whom fear the technology. Command support is often also given based upon how well the managers up the chain of command understand automation, most of whom have not grown up with computers.

If the main tasks of an individual are articulately expressed on an evaluation worksheet by a midlevel manager who does not understand automation, the tasks associated

with the SAs job may be expressed in a generic or oversimplified way. The other tasks will probably be better understood by the supervisor, and will likely be graded as more important. This leads many systems administrators to be graded on tasks mostly unrelated to the most critical aspect of their position. Managers of the future must be aware of each of the critical aspects of their units, understand the complexities of each system, and be capable of employing skilled midlevel managers to fully orchestrate the advanced systems necessary to defeat adversaries.[30, 31]

Conclusions.

Although automation is critical to the efficient operation of units today, many systems managers and upper management do not fully understand or appreciate the complex nature of the systems they manage. As the complexity of the technology continues to advance, systems administrators must be increasingly available to properly administer the complex computers that are linked together, for military units to rapidly deploy and have the information dominance they need to maximize what they do best on the battlefield.[32] The systems administrators position needs to be properly established and to be filled by someone who understands the complexity of the automation network, who gets the training and support of the commander, and gets tracked through the

personnel systems to enable better utilization of these critical skills.

Slush, a mixture of snow and water, is very slippery. It frequently causes vehicles to slide off roads. Yet the phrase to "grease the process" has reference to making something slippery so it will go through the bureaucracy faster. Systems administrators can be the strategic slush to help critical information flow through the automated systems faster and better, or they can cause the information to slide off track. This all leads to a requirement to have better policies at the strategic or national level to improve this area of the military. Other nations are rapidly incorporating the technology that is available. If the US military does not better establish policies to manage automation, other nations may gain the advantage and exploit or attack US systems in the future wars.[33, 34]

Recommendations.

The joint staff needs to establish a policy at each of the military services setting standards for systems administrator training similar to the way user or operator training has standards. The joint staff should establish the standards so equal standards are set among all services and so systems can be utilized jointly rather than the

stovepipe type systems of the past.

The military service chiefs each need to push to establish a skill identifier to track SA skills in the military and civilian personnel systems of today. Additional skill identifiers are currently used for this type of situation in the military personnel systems. One could be established for the systems administrator skills. The civilian personnel system could adopt something similar to this.

The Army staff must begin to establish deployment evaluation criteria for division, brigade, and battalion commanders based upon the entire missions they may be called upon to execute in crises or war. This must include correct deployment planning information sent through the automated systems for the air or sea ports to move the units to the battle area.

The unified commanders in chief need to place more emphasis on lower commanders and staffs understanding the process of getting to the battle so the military can better do its power projection job when it gets there.

text word count 5,708

Endnotes

[1]In personal discussions with Herb Kaskoff, the program manager of the Worldwide Port System (WPS), the planning data that came from the units showed only about 25% accurate planning information.

[2]Institute for National Strategic Studies of National Defense University, Strategic Assessment 1996 Instruments of U.S. Power. National Defense University Press, 220-221.

[3]William S. Cohen, Report of the Quadrennial Defense Review (May 1997), 14.

[4]MSGT Narin Sum USA, Systems Administrator, interview by author, 18 Feb 1998, Carlisle, PA.

[5]GEN John M. Shalikashvili USA, Joint Vision 2010, 26.

[6]GEN Dennis J. Reimer USA, Army Vision 2010, 12.

[7]LtGen Kenneth A. Minihan USAF, National Cryptologic Strategy for the 21st Century, (June 1996), 14.

[8]Shalikashvili, 17-19.

[9]William J. Clinton, A National Security Strategy for a New Century, (Washington D.C.: The White House, May 1997), 10.

[10]Minihan, 4.

[11]The Honorable Togo D. West and General Dennis J. Reimer, A Statement on the Posture of the United States Army Fiscal Year 1998, (Washington D.C.: February 1997), 5.

[12]Clinton, 13.

[13]LTC Yves J. Fontaine USA, "Strategic Logistics for Intervention Forces," Parameters, Vol XXVII, No 4, (Carlisle, PA: US Army War College, Sep 23, 1997), 44.

[14]Any reference to he or him will be considered to refer to her or hers as well. There is no intent to distinguish genders in this paper.

[15]MAJ Stephen Luebke USA, Systems Project Officer, interview by author, 18 Feb 1998, Carlisle, PA.

[16]Plt Sgt Simone James USA, System Project Officer, interview by author, 18 Feb 1998, Carlisle, PA.

[17]Rita Johanson, Unit Movement Coordinator and Systems Administrator at Fort Stewart, telephone interview by author, 27 March 1998.

[18]Luebke.

[19]Sum.

[20]Lynne M. Woods, Systems Administrator, interview by author, 18 Feb 1998, Carlisle, PA.

[21]Terry J. Young and Robert A. Brace II, US Army War College Program for Joint Education (PJE) Academic Year 1998. (Carlisle, PA: US Army War College, 1997) 14, 43-77.

[22]In personal discussions with Herb Kaskoff, the program manager of the Worldwide Port System (WPS), the planning data that came from the units showed only about 25% accurate planning information.

[23]Fontaine, 54.

[24]West, 15-16.

[25]The 501st Transportation Battalion had been trained on the Automated Aircraft Load Planning System (AALPS), and lost their SA due to a medical emergency in 1994. It was not until the AALPS Program Manager visited the unit and discovered the problem that the problem was resolved.

[26]West, 14.

[27]Personal contracting experience during the Bosnia conflict while working as Program Manager of the Transportation Coordinator Automated Command and Control Information System showed the actual costs in danger zones to be this high on 3 separate contracts.

[28]West, 25.

[29]Ibid., 13.

[30]Shalikashvili 28-29.

[31]Reimer, 17.

[32]West, 38-40.

[33]Ibid., 37.

[34]Reimer, 8.

Bibliography

Clinton, William J. A National Security Strategy for a New Century. Washington D.C.: The White House, May 1997.

Cohen, William S. Secretary of Defense. Report of the Quadrennial Defense Review. May 1997.

Fontaine, Yves J. LTC USA. "Strategic Logistics for Intervention Forces." Parameters Vol XXVII, No 4. Carlisle, PA: US Army War College, Sep 23, 1997. 42-59.

Institute for National Strategic Studies of National Defense University. Strategic Assessment 1996 Instruments of U.S. Power. National Defense University Press.

James, Simone, E7 USA. System Project Officer. Interview by author, 18 Feb 1998, Carlisle, PA.

Johanson, Rita, Unit Movement Coordinator and Systems Administrator at Fort Stewart. Telephone interview by author, 27 March 1998.

Minihan, Kenneth A. LtGen USAF. National Cryptologic Strategy for the 21st Century. June 1996.

Reimer, Dennis J. GEN USA. Army Vision 2010.

Shalikashvili, John M. GEN USA. Joint Vision 2010.

Sum, Narin, MSGT USA. Systems Administrator. Interview by author, 18 Feb 1998, Carlisle, PA.

West, Togo D. (The Honorable) and General Dennis J. Reimer. A Statement on the Posture of the United States Army Fiscal Year 1998. February 1997.

Woods, Lynne M. Systems Administrator. Interview by author, 18 Feb 1998, Carlisle, PA.

Young, Terry J, and Robert A. Brace II. US Army War College Program for Joint Education (PJE) Academic Year 1998. Carlisle, PA: US Army War College, 1997.