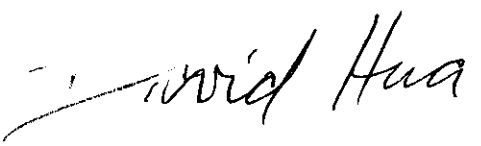
# The Role of Military Networks in the Battlefield

An Honors Thesis (HONRS 499)

By

Michael Reese

Thesis Advisor
David Hua



Ball State University
Muncie, Indiana

Date: May 2004

Expected Date of Graduation:
May 2004

Abstract

Computers have become a way of life for many people in the Twenty-first century and computers have even found their spot on the battlefield. This research paper covers military computer networks and the issues facing the networks and the users in the battlefield. This paper will cover the events leading up to the modern design of military computer networks as well as the employments of the computer networks in battlefield.

Acknowledgements

- I would like to give special thanks to Dave Hua for his input as my faculty advisor.
- I would also like to thank Travis McSherley for his help and advice in the editing of this paper.

# Contents

# *Introduction*

In the past decade the Internet has become a valuable tool that we use everyday for work, research, shopping, entertainment, talking to friends and family and whatever else we can find use of on the Internet. But, did you know that that same Internet that we use everyday was first designed, developed and used by the United States Armed Forces for secure communications lines over thirty years ago? The development of the Internet provided not only another method of secure communications between the United States Armed Forces but also created other means to share information with another person without having to fax or print and mail documents

The key event in the development of the Internet was a standardized protocol, TCP/IP that allows computers to communicate with each other. This standardization made the creation of personal computer networks possible no matter how many different kinds of computers and operating systems were running on the network. Without communication, computer networks and distributive systems would be worthless because, as stated in Debastiani's government report, "Computers and communication have a direct relationship" (13). The military uses these computer networks to communicate with troops with laptops in the battlefield as well as set up operations, share information, such as updated maps and known enemy equipment and movement among headquarters and other services of the Military. The speed of electronic communication via computer, alone, has saved time by passing up-to-date

information electronically instead of vocally and there is no doubt that electronic communication has saved a number of lives by allowing an enormous amount of information to be passed quickly to those who need it most.

This paper is a study of the United States Military's computer networks on and off the battlefield. In this paper we will take a brief look at the history of computer networks in the United States Armed Forces and the current state of the military's computer networks and their employment in the battlefield. In addition this paper will study a few of the problems facing the networks and the proposed solutions to those problems.

# Chapter One

## *The Makings of the United States Armed Force's Computer Network*

The origin of military computer networks goes back as far as the World War II era. Before this period, orders were sent to troops written on paper and passed by messenger or they were transmitted over very short ranges with radios. Transmitting messages in this fashion from the battlefield to the base or vice versa took a lot of time and time is not in abundance on the battlefield. Lapse in the communication time is not in the best interest of an operation.

The beginnings of electronic communication networks in the battlefield began in World War II when fax machines and teletypes were used to transmit data between bases and field headquarters. The general use for fax machines in this era of military history was to send updated weather maps to air bases and aircraft while teletypes were only used to send text messages (Torrieri, 14).

In the 1950's the first computer ever to be used by the military, Moby Dick, was introduced. It was built by Univac, the same company that later supplied the military with Univac 1005 computers to be used on the supply network (Debastiani, 17 and 56).

**The Vietnam War Era**

The 1960's brought about many changes in the methods of electronic communication within the military. In the early 1960's the Secretary of Defense,

Robert McNamara, rebuilt the command and control system into the Worldwide Military Command and Control System, WWMCCS (Gruber, 4). The WWMCCS increased United States military commanders' situational awareness of the battlefield anywhere on the planet (5).

The Vietnam War brought a lot of changes to the military's communication network. In the early 1960's the digital communications network was used for supply and finance records as well as command and control operations and intelligence systems. Because intelligence and command and control operations are considered a higher priority, those sections used the more reliable and higher speed wideband communications. The supply and finance records were transferred using punch cards and high frequency radio waves. Transferring the supply data to the digital network lessened the burden on the signalmen who were previously responsible for all data transfer (Bergen, 300). However, in the Southeast Asian climate, the punch cards, used to feed information to the computers, were often ruined by the heat and humidity and would cause the computers reading them to jam (299). The punch card data was transferred from bases in Okinawa, the Phillipines, Phu Lam and the United states by high frequency radio waves at rates of about three to one hundred cards per minute. The bases would then transfer that data back onto punch cards. The high frequency radio wave transmission was so unreliable and slow that in some instances the signalmen responsible for the data would pack up the punch cards in suitcases and boxes and air-mail the packages to the bases overseas. Even in the best of circumstances, this process took a lot of time. The problem caused by the failure in data communications noted by the signalmen's advisors was that the, "Inadequacy of

communication... inhibits the maintenance of up-to-date stock records... at a central point and slows down distribution and re-supply" (Bergen, 300).

The communication failures of the punch card and high frequency radio wave network led to the birth of Autodin. Autodin stands for automatic digital network. It was created in February 1963 by the Defense Communications Agency. It was created to serve as a worldwide high speed data network (Bergen, 301). As stated by General Harlingen, Autodin was "a mixed blessing, creating nearly as many problems as it has solved" (303). Autodin included only the Army and Air Force's computer networks. It was not expanded to the Navy or Marines due to the uncertainties of the quality of the connections (302). The NSA considered Autodin too insecure and created its own digital network, Criticomm.

The next step forward in the development of the Internet, the Integrated Wideband Communication System, was created in 1965. Two years later, all of the Army's major depots in South Vietnam were connected to the 14th Inventory Control Center. These connections ranged in transmission speed from ten to two hundred punch cards per minute. In fact, the relay station located in Phu Lam was transferring data at roughly five hundred thousand cards a day. The data transfer rates of the Autodin network was three thousand words per minute on the teletype connections, and two thousand four hundred bits per second on a new magnetic tape communications system (Bergen, 302).

In the late 1960's computer scientists began of the development of the modern day Internet. One of the key steps in the design of the Internet, ARPANET was created by the Defense Advanced Research Projects Agency, DARPA, to allow for

communication among the members of the agency (Cisco, 469 and 675). ARPANET was also developed as a military electronic communications system that could survive a nuclear war (Gruber, 2). At the beginning of the project, in 1969, the communications network only consisted of three universities in California and one university in Utah. ARPANET then grew to be the favorite mode of communications between the universities and the Department of Defense. Due to the rising security issues the military was removed from ARPANET and place on their own network MILNET. MILNET is the military equivalent of the Internet overseen by the Defense Communications Agency. The National Science Foundation also developed a similar network named NSFNET, which was the initial model for the modern civilian Internet. MILNET was renamed Defense Data Network and then later renamed again as the Defense Information Switched Network, DISN. The Defense Communication Agency, the organization responsible for monitoring MILNET, was renamed the Defense Information Systems Agency, DISA. Although there were many name changes, one thing remained the same, the success of all of these networks was due to the standardization of the networks all using the same communications protocol, TCP/IP (8). TCP/IP is still very much in use today, as the communications protocol of the Internet we use daily (Cisco, 65)

The TCP/IP communications protocol was developed by DARPA as a standardized digital communications protocol. This standardization made it possible for computers to communicate globally, no matter the type of computer or operating system used. TCP/IP stands for Transmission Control Protocol/Internet Protocol. The protocol has four layers, Application, Transport, Internet, and Network Access.

The Application layer, also known as the "process layer", contains most if not all of the applications used by the user. The next layer, the Transport layer, also known as the "host to host" layer, takes care of the flow and reliability of the data being transferred. The next layer down is the Internet layer whose sole purpose is to send packets of data from the source computer to the destination computer on any network. The fourth and bottom layer is the Network layer. This layer includes the local and wide area networks and the physical connections between all networked computers (Cisco, 65).

In the late 1960's most military computers used on the battlefield were commercially built computers protected by rugged cases and were typically located in a truck or van for ease of movement. The military used commercial computers due to the lower cost than computers that were specifically designed for military use (Debastiani, 17).

**The 1980's**

In 1983 computers in United States Army were an average of nine years old and thirteen years old in the Army Reserves (Debastiani, 20 and 21). Knowing this, it is no surprise that intelligence stated that the Soviet government was at least five years ahead of the US government in Command and Control computer technology (31). The military started working on the concept of modern networking by developing the distributive processing concept. The Air Force began developing a local area network of six hundred computers with file sharing and electronic mail capabilities. Once they had created this network, the Air Force also built LAN offices

with the responsibility of creating the networking standards for the remainder of the Air Force computer networks (Gruber, 10). "Dumb terminals" were set up to connect computers to their respective base's data processing center. The "dumb terminal" connections were multiplexed telephone lines that allowed more computers to access the data processing centers at one time. The Air Force also worked on developing their Wide Area computer network. They used long distance telephone carriers to go from the base to the regional military computer centers (9). Although the Air Force only mentioned the use of wired connections, wireless communications such as satellite, radio and microwave were available to all forces during the early 1980's (Debastiani, 13).

**The 1990's**

During the Persian Gulf War, United States Special Forces used cellular phones to send GPS data to bomber planes ("The Army's...", 19). Soon after the Gulf War the Army began a digitization initiative led by Army Chief of Staff Gordon Sullivan. The objective of Sullivan's digitization initiative was to get more information about enemy positions and their capabilities to Army units in the battlefield where the information was needed most. The digitization initiative was also designed to help a commanding officer make more and better informed decisions while in combat conditions (7).

In 1996, the United States Air Force commanders all had email capabilities but lacked the technicians necessary to keep the system up. The Air Force also had difficulty with their computer networks because of incompatibility and difficulty in

training technicians on the different computer systems. Air Force computers varied because groups were allowed to purchase their own systems (Gruber, 11). In the mid-1990's the dumb terminals used in the Air Force were replaced with personal computers because they were cheaper (12). The "dumb terminals" met their end in 1996 when some squadrons deployed in Bahrain brought their "dumb terminals" and found that they could not be connected to the rest of the network because the Air Force communications squadron had already set up the network. The Air Force also used laptops to access classified networks to access the satellite and weather maps (17).

At the end of the 1990's the Air Force networks, with the use of their network technology, were able to update their guidance systems almost as soon as data came in from the reconnaissance planes (Gruber, 6).

# Chapter Two

## *Modern Day Uses of*

## *Computer Networks in the Battlefield*

**Uses of the Military's Computer Networks**

The uses of military computer networks have increased along with the technology. From the Joint Chiefs of Staff's publication *Joint Vision 2020,* "Information, information processing, and communications networks are at the core of every military activity" ("The Army's...", 14). The previous uses for the military's computer networks, as noted before in Chapter One, were to facilitate communication between headquarters, battlefield commanders and supply stations. More uses for the networks are providing fast and accurate communication between fire bases and fire support as well as providing accurate intelligence to officers in the battlefield (8-9). As far as electronic intelligence is concerned, "Without reliable communication in war, information stored in the computer becomes degraded, untimely and inaccurate" (Debastiani, 17). If battlefield commanders are to be victorious they must have the most accurate and up-to-date intelligence to make their decisions. With the increase of more sophisticated weaponry, the military's computer networks have adopted a new role in the battlefield. Computers are now used to control weapons remotely such as the UAV's.

The United States Armed Services' computer network systems help soldiers in the battlefield by providing advance notice of possible enemy hideouts and known positions. The network speed, or the speed at which the data is transmitted, has lowered the reaction time for officers. Even during the recent war in Iraq, the speed of the Army Battle Command System, the Army's digital warfare system, allowed battlefield commanders to change an operation's plans in the middle of that operation in only a matter of seconds due to recently updated intelligence. The speed of the system also made it possible for the commanders to create complex missions within only a few hours ("The Army's...", 16).

The military is relying more and more on computer networks with the increase of sophisticated weapons systems such as the UAV, Unmanned Aerial Vehicle (Gruber, 16). A lot of bandwidth is consumed between the UAV and the remote operator's station and those communication lines need to be very secure in order for the UAV to survive and fulfill its mission. The UAV uses a lot of bandwidth because it transmits a large amount of video data back to its base so that the operator can control the UAV more efficiently. The Army's current bandwidth capability is sufficient for the standard digital text and voice messages, yet insufficient for all attempted video signals. The Army has a lot of plans for digital video transmission such as the UAV's, teleconferencing, video battlefield display and telemedicine. A video battlefield display is useful to commanders back at base so that they can see the events happening on the battlefield and coordinate their forces accordingly. Telemedicine is a very useful tool for doctors and surgeons that allows them to see the extent of a soldier's wounds in the battlefield and give the medic the proper

advice to prolong the soldier's life until he or she can be transported back to a medical unit ("The Army's...", 17).

**Computers in Use**

The Department of Defense currently operates over ten thousand computer systems and one and a half million personal computers. Only two thousand of these computers are considered critical (Cordesman, 12). Critical computers are computers with mission critical operations that need to remain operational and that may contain classified information. Critical computers have more security and more backups to keep them operational.

The Department of Defense has contracted out the Xybernaut Corporation to design and produce a computer capable of being worn by soldiers in the battlefield. The funding for the project was proposed at $3.4 million dollars in 2003 ("Wearable Computers...", 1). The new wearable computers will make it easier on communication officers in the battlefield. The computers are heat and water resistant making the computers more battle ready (16). The wearable computers will allow the computer operator or communications officer to move more freely than with the previous laptop computers.

**Network Communication Channels**

Currently the United States Department of Defense, including the military, operates on the DISN, Defense Information Switched Network. The DISN is a more secure form of the Internet used only for military and Department of Defense

purposes. This network uses the same standard protocols as the civilian internet ("The Army's...", 22) and is still connected to the civilian Internet but physical connections to the civilian Internet are few and well monitored (Gruber, 3).

The United States Armed Services use both wired and wireless connections on the DISN. Wired connections in use are fiber optics and copper cabling. Wireless connections in use are radio frequencies, PCM lasers and microwaves.

Fiber optic cabling is a cable of a single flexible glass fiber or multiple fibers that transmit binary data in the form of light pulses at a high speed. No light equals a zero and a pulse of light equals one. Transmitting data by cable is a very reliable method of high speed communication for wide area networks with permanent nodes, or stations, but in battlefield conditions cable is not mobile enough for a communications team to keep up with troop movements. A positive aspect of using fiber optic cabling is that it cannot be jammed by the enemy and it is very difficult to intercept the signal without the monitors noting the disturbance in the line. Like all cabling, in battlefield conditions, fiber optic cabling can be cut or damaged by heat (Torrieri, 1). As far as non-battlefield conditions, fiber optic cabling is the optimal choice for headquarters and higher level command centers that will be operational at their current location for a long time ("The Army's...", 19).

Local area networks in command centers are interconnected with standard copper cabling or PCM, pulse color modulated lasers. These connections are capable of transmitting data at speeds of megabits per second, one million bits per second. PCM lasers are only capable of transmitting data accurately and efficiently over to twenty kilometers. Within the command centers, computers are connected using fiber

optic cabling to allow for high speed communication, necessary to conduct a successful operation ("The Army's...", 19).

Radio wave data transmission has been used by the military for a many decades, since before World War II. Radios have become more reliable since those days and now in addition to voice transmissions, they are capable of transmitting electronic data. In 2003, the military had deployed over two hundred twenty thousand digital radios in the battlefield. These high bandwidth radios cost about $127,000 each, totaling about $28 billion already invested in the project. More radios are expected to be deployed in next few years ("The Army's...", 20).

Satellites are used by all services of the military but they are reserved for higher-level command centers. This form of communication has been deemed BLOS, beyond line of sight, communication ("The Army's...", 25-26).

**Network Security**

Network security is a major concern on military networks. The data contained on military networks can contain classified information and data necessary for a victorious outcome of an operation. The Department of Defense uses a combination of a few different techniques for securing the DISN.

Time-hopping is a form of security used for wireless data transmission. Time-hopping uses previously agreed upon slots of time when data can be transmitted. However, this does not cut down on transmission interception but it does make it difficult for the data to be accurately decrypted (Torrieri, 129).

Frequency hopping is another method used by the military to keep their radio frequencies secure. Frequency hopping uses prearranged changes within a range of frequencies, and the radios in use today automatically jump to and transmit data at the new frequency for the amount of time designated. Frequency hopping is the best method for removing the threats of both interception and jamming (Torrieri, 153). The military has developed a hybrid form of frequency hopping that has increased the range of radio frequencies in which the radios can transmit (217).

Frequency and time hopping are two methods that protect jamming and interception of data. Encryption, translating the data into code, protects the transmitted data. Data can be encrypted simply by rearranging the sender's message using the same format that the receiver uses to decode the message. In the case of electronic data, encryption is based on more complex mathematical algorithms (Torrieri, 382). To protect voice data, the military uses scrambling devices and voice encryption/decryption devices. The scrambler jumbles voice data into signals so that an interceptor without a descrambler would only hear noise. A descrambler is used to convert the scrambled data back into comprehensible voice data (Torrieri, 405).

A form of both wireless and wired computer network security is provided by the DISA. The DISA, or Defense Information Systems Agency, monitors incoming and outgoing information between the separate civilian and military Internets. However the DISA does not currently monitor the communication among the military sectors of the Defense Information Switched Network, or DISN (Gruber, 10).

Another organization in the fight to protect our nation's communications network is the JTF-CNO. The JTF-CNO was created in December 2000 to take

command of information warfare ("Joint Task Force...", 2). In more detail, JTF-CNO is split into two different divisions. CND, Computer Network Defense, maintains the security of the Department of Defense's computer networks and the CNA, Computer Network Attacks, commands cyber-warfare strategy and operations (1). The JTF-CNO is a fairly small organization compared to the complexities of its tasks. It employs only one hundred twenty two people and is in constant operation. The proposed budget for 2003 is $26 million. The JTF-CNO analyzes previous attacks not only to upgrade network security but to determine whether or not critical information was accessed or if the network was damaged in any way by the intrusion or attack (2).

**Cyber Warfare**

Cyber warfare is a fairly new tool in the United States Armed Services arsenal. Cyber warfare mostly deals with harassing enemy communication and information systems during a conflict as an additional tool to decrease the threat to United States combat forces in the battlefield (Gaudin, 1). Cyber warfare can be any form of the following: hacking into an enemies system and changing the information in the database, general disinformation and propaganda, even sending virus email, overloading systems, and shutting down electrical grids (Debastiani, 3, 27 and 116). Cyber warfare is a "less messy" form of warfare meaning it causes fewer casualties on both sides of the battle (Gaudin, 2). Cyber warfare can still cause casualties even though it does not directly target enemy personnel. If an attack were directed towards a power grid, a hospital's power could be taken away as a side effect of the attack.

Cyber warfare is not always the best option, especially in the case of the United States. Dan Wooley, a former Air Force communications and computer specialist, once said cyber warfare is, "A tool that allows weaker nations to offset American military efforts" (Gaudin, 3). The United States relies heavily on technology in every major industry; even our health and national security infrastructures are online. If we were to use cyber warfare in an attack, it could be reengineered to be used against us.

One use of computer warfare took place during the Gulf War when United States forces gathered intelligence by hacking into Iraqi email systems. Another computer warfare operation took place in Kosovo in the late 1990's, cyber-warfare was used to spread propaganda and change Serbian intelligence in order to protect NATO aircraft during their bombing missions (Cordesman, 25 and 37). However, these intrusions were noticed and in response, Serbian hackers attacked NATO websites (36).

Cyber warfare is not always a legal method of warfare either. Using it against non-military targets could have the potential for war crime charges against the forces that use it. Even if the targets are of a military nature they must be deemed necessary targets or war crime charges are still plausible ("U.S. Military...", 1).

In 2003, the US publicly stated that they were working to create a new strategy and a system for the use of cyber warfare in combat. This system would create a set of rules for the United States forces to follow when cyber warfare is deemed necessary (Gaudin, 1).

**The Future of Military Computer Networks**

The United States Army began a "transformation" initiative in 1999. "Transformation" is an attempt to make thirteen brigades capable of quick deployment and an increase in a unit's situational awareness without losing their full fighting capabilities by 2009 ("The Army's...", 18). Computer networks are a key element necessary to achieve the full transformation (3). In order for the military's computer infrastructure to be capable of handling the changes the amount of available bandwidth must increase. In an attempt to increase the available bandwidth of the military's network three new improvements in communication technology will be available and deployed by the year 2010. These new technologies are Joint Tactical Radio Systems (JTRS), Multiband Integrated Satellite Terminal (MIST) and Warfighter Information Network-Tactical (WIN-T). JTRS is a new radio for use in the battlefield by combat soldiers. Both WIN-T and MIST are designed for higher level use with satellites for beyond line of sight, BLOS, communications (11).

# Chapter Three

## *Military Computer Network Problems and Solutions*

The United States Armed Forces computer networks do face the same problems as do civilian computer networks, such as hardware and software problems, personnel issues and network incompatibilities. However, military computer networks also face a greater physical threat on the equipment and personnel. Most if not all of the additional problems facing computer networks on the battlefield concern the wear and tear, including destruction of network hardware, due to the harsh nature of the battlefield. Additionally, military computer networks are a choicer target for hackers who wish to steal sensitive information or just to prove their hacking expertise.

### Hardware Problems

Computer hardware is very vulnerable to the elements, especially in the battlefield. Water can short out or warp many components within a system. Heat can melt components and dust and dirt can jam disk drives, especially if the dust or dirt makes its way into the computer's hard drive. Steps have already been taken to prepare systems for battlefield elements. The military has contracted out the Xybernaut Corporation to create a waterproof and heatproof laptop for use in the battlefield ("Wearable computers…", 1).

Aside from the battlefield elements, one of the biggest problems with computer hardware in the military is the lack of the standardization of parts. In 1983,

the military had fifty nine different computer systems made by twenty nine different manufacturers. The computers used forty four different programming languages as well as fifty three different support systems (Debastiani, 38). The differences in the systems make it difficult to provide the spare parts necessary for repair. Under battlefield conditions supply lines may be cut and equipment cannibalization will occur if spare parts are nowhere to be found (20). With the differences in computer systems, cannibalization could not occur, possibly leaving a unit stranded in the middle of a firefight without any form of communication with their base.

Providing an ample supply of spare parts for all the systems in use would take up a lot of space and possibly waste a lot of money if those parts are never used. However, the best solution for the differences in the military's computer systems would be to implement a standard computer system for an entire division that way parts can be interchangeable among different machines and the supply rooms will not be packed with a large amount of spare parts

Another hardware problem is the availability of supplying enough power for the computer systems. The power supply for a communications officer in the field must be very mobile and the batteries in current use do not have a long life. Speed and mobility are great assets for a combat soldier. Batteries, when carried in bulk, add a lot of weight to an already weighed down soldier, slowing the soldier down and lessening the soldier's agility. Generators would supply an ample amount of power but they are not mobile enough for battlefield units ("The Army's...", 34). The only possible solution for the power supply problem is to research and design a longer lasting and lighter-weight battery to power mobile computer systems.

Also, a potential problem with power supplies is their weakness against EMP, electromagnetic pulse. EMP occurs just before a nuclear explosion, no matter how big the blast. EMP can burn out a power supply as well as other computer hardware components. The only way to protect a power supply from EMP is to shield it in a protective casing or shelter (Debastiani, 10).

**Software Problems**

When it comes to computer software used by the military security is a big issue. Software written for use in the civilian market is cheaper than similar programs designed by the military but security is a major issue. Some of the questions that must be asked when a new software package is being studied are as follows. Can the programmer of the civilian software be trusted? Is the program secure or without any backdoors? (Gross, 1). Programmers often add backdoors to their program's source code in order for an easy repair. Sometimes these backdoors are found by hackers and exploited in viruses or intrusions.

Commercial-market software is cheaper than military-designed programs but it cannot be trusted. The simplest and best solution for software security is to use only programs written by military programmers. This solution may cost more but security is a priceless commodity in the military where lives may depend on the information held within the network.

**Personnel Problems**

The United States military has some problems with their computer personnel. It is hard to train repairmen on all of the systems in use by the military and it is hard to retain those repairmen after their term of enlistment is up. The repairmen typically move on to higher paying civilian jobs. During the Vietnam War, the Army contracted out repairmen from computer companies that supplied the Army's computer systems. However, the contracted repairmen were not trained nor were they loyal enough to stick around and do their jobs when a fight broke out (Debastiani, 21).

Some solutions to the personnel problem are to offer more or better incentives to keep the repairmen the Army currently has and better recruitment offers to increase the enlistment of soldiers with computer experience. Standardization of computer equipment would also help during the training process of potential computer repairmen and network technicians as well as making them work more efficiently when a problem arises.

**Systems Standardization**

As noted before in the personnel and computer hardware/software issues, the lack of standardization causes problems in each of the different military services. Some computers and computer programs will not work together and the data cannot be transferred correctly. To be able to repair the different systems more parts would have to be kept in stock taking up more space. As for the personnel side of the issue, the use of many different computer systems makes training longer and more difficult.

The Military Computer Family, MCF, was one attempt to standardize the military's computer networks. It consisted of three parts; hardware, software and architecture. Architecture is the basic set of instructions that the computer is built on. Using the MCF, the military's computer systems would be cut down from fifty-eight systems to only three (Debastiani, 23 and 24). Other standardization systems have been attempted on the military's computer systems but none have been followed completely by all branches of the military for them to be effective.

**Bandwidth**

The greatest concern when it comes to the Internet for the average person is the connection speed, or the bandwidth. The concern is that data is not transferring fast enough to load a website at a rate that suits the user. The military shares the same concern. However, if data is not transferred fast enough the effect is a decision made on little information that could result in the loss of American soldiers' lives (Debastiani, 13).

There have been no official studies to determine how much bandwidth is currently needed and supplied. Unofficially it has been said that the current bandwidth need is around ten times more than the amount currently supplied ("The Army's...", 8). However, in battlefield conditions bandwidth usage has risen to thirty times the amount supplied (9). The lack in the supply of bandwidth means that the military's battlefield networks could potentially crash or shut down (10). Even if the network is bogged down by the amount of data attempted to be sent, the transfer of critical data and the data necessary to safely carry out a mission, could be slowed

down. In desperate situations such as firefights, a delay in communications, if only for a few minutes, has the potential to cause an operation to fail (32).

There are many reasons for the large bandwidth requirement, the sophisticated weapons systems used in the military, security precautions taken, or simply the amount of soldiers logged onto the network trying to keep in contact with family and friends back home. Sophisticated weapons systems like the Unmanned Aerial Vehicles, UAV's, that have recently been brought to public attention in the war in Afghanistan are a great asset to the military's arsenal. However, in order maintain their functionality, UAV's must use a lot of bandwidth to transmit video data ("The Army's...", 8). To keep UAV's a functioning weapon on the battlefield the military is planning on moving the UAV's to their own separate network (11). This solution will cut down the total bandwidth demand but not enough to bring the demand below the total bandwidth supplied.

The bandwidth problem will increase as the sophistication of the equipment and technology grows ("The Army's...", 11). To keep data and communications secure the encryption and decryption that takes place during transmission uses a lot of time and bandwidth. Also, the frequency and time hopping techniques mentioned before in Chapter Two add to the bandwidth usage (23).

It was once thought that data compression would lower the amount of required bandwidth but in some studies data compression actually increased the amount of bandwidth needed. Data compression was also noted to cause loss of data during the compression/decompression process ("The Army's...", 68). It is very well known that messages containing only text use very little bandwidth compared to video and voice

messages (10). Removing all unnecessary videoconferencing sessions from mission critical networks would lower the bandwidth considerably and increase the amount of successful data transmissions over those networks (51).

Currently the military is working on providing new high bandwidth radio equipment, called JTRS, Joint Tactical Radio Systems, which will be capable of providing more bandwidth to soldiers in the battlefield ("The Army's...", 37). This plan will cost around twenty billion dollars and will not be completed until 2010, yet it is not the best solution to the Army's bandwidth problem ("The Army's...", 3, 8 and 46). The best solution is researching the current system and developing a new system to lower the amount of bandwidth needed by cutting down on all unnecessary bandwidth usage.

**Nuclear Warfare**

When on the battlefield computers are susceptible to more severe elements than they would in any office environment. Some of the worst possible battlefield elements for both computers and personnel are created by nuclear warhead detonations. Detonation of a nuclear weapon creates an extreme amount of heat that is fatal for people within the blast radius and a large amount of radiation that is harmful and potentially fatal to those outside of the original blast radius. Computers can be damaged by the heat which can warp and burn the glass fibers in fiber optic cables, melt copper wiring and could damage any exposed computer peripherals (Debastiani, 6).

However, heat is not the worst element for computer equipment. Electromagnetic pulse, EMP, is the worst effect of a nuclear detonation for computer equipment. EMP comes from the reaction of the atmosphere to the radiation emitted from a nuclear detonation. EMP is not harmful to people, only electronic equipment using integrated circuits. Integrated circuits, or ICs, are the circuit boards and microchips found in a lot of electronic equipment today, even if the device is not a computer or computer component. EMP burns out the integrated circuits that are the heart of the modern computer. To make matters worse, when integrated circuits are hit with EMP they create their own electromagnetic pulse that travels through the system causing even more damage to other integrated circuits nearby (Debastiani, 6). Once an integrated circuit is damaged by EMP it cannot be repaired.

The damage caused by EMP can reach farther than the radius of the heat damage of a nuclear blast. The range of EMP damage relates directly to the height above ground of the nuclear blast, the higher the blast the more damage caused by EMP (Debastiani, 7 and 8). In fact, a nuclear blast detonated two hundred miles above land would have the power to damage or destroy all integrated circuits in the United States as well as most of Canada and Mexico (9).

The United States' computer networks are more vulnerable to nuclear electromagnetic pulse because most of the cables used for data communication are above ground. If the cables were below ground, like the German infrastructure, the damage to computer networks would be less severe because the cables would be protected by a natural radiation shield (Debastiani, 16).

Creating computers with a protective casing would protect a single system from electromagnetic pulse. Integrating surge protectors and electrical absorbers into computer systems and integrated circuits would prevent EMP damage from spreading from one system to the next (Debastiani, 9).

**Radio Frequency Blackout**

Nuclear explosions also affect radio transmissions by causing interference. The dust cloud created by the initial explosion interferes with the line of sight radio communications used on the frontlines of the battlefield. The blast could also take out satellite communications if the satellites are hit by the blast's EMP. (Debastiani, 14 and 15). There is no way to counter the effects of a nuclear explosion on a radio network but the damage done can be limited by keeping the radio communications network separate from other networks (15). Keeping the networks separate would protect them from power surges passing from one system to another.

**Chemical Warfare**

Chemical warfare is not as harmful to computers as it is to the soldiers on the battlefield. However, corrosive chemicals can eat away at computer components and harm users if the computer is not properly decontaminated. The only solution for chemical warfare is to create an airtight casing so that chemicals cannot enter the system or keep the computer systems inside chemical proof shelters (Debastiani, 11).

**Information Warfare**

Over the last decade the nation's infrastructure has been built to rely on computer networks and online data storage systems to increase efficiency and ease of information access nationwide. However this reliance makes the United States even more vulnerable to cyber terror and electronic espionage (Cordesman, 2).

The United States has put their entire economic and critical infrastructure online. The critical infrastructure includes emergency, medical and power plant systems as well as other systems important to the survival of the American way of life ("Cyber-Security...", 1). An example of the cyber-warfare threat on the United States' critical infrastructure happened in 1998. The Galaxy 4 communications satellite failed causing trouble with over ninety percent of all ATM and credit card users as well as emergency medical workers (2).

With our reliance on national, even global, electronic communication the United States has a larger pool of electronic targets than its potential enemies (Gruber, 1). Even now, foreign nations are creating their own information warfare strategies and programs for eventual use in the battlefield against nations with better, more sophisticated weapons systems, and the United States is in mind as a potential target (Cordesman, 16). Some nations have already developed and used information warfare systems in their own campaigns. The Israelis and Palestinians have used computer networks to deface their enemy's websites and send virus e-mail (116).

The United States has had problems in the past with the use of computer network technology as a weapon. In order for the United States to retaliate against a computer attack they believe to be from a hostile nation or terrorist organization, the attack must be declared as an act of war and the United States' reaction must be a justified retaliatory action. However, there is no definition for an act of war against computer networks nor is there a definition of a justified cyber-attack (Cordesman, 6). Also, if the United States was going to strike back against a cyber-terror attack, there is a high risk that the method of attack used will be reengineered and sent back to the United States where it can do more damage (7).

Attempts have been made to determine the amount of funding needed to create this security program that will protect the nation's infrastructure but this is difficult due to the amount of exaggeration and the unknown amount of risk to the infrastructure (Cordesman, 4).

The amount of qualified personnel has been a problem. In 2000, there were only forty five to seventy five people in the nation with the qualifications necessary to work on a new computer network security system ("Cyber-Security...", 3).

Despite the lack of funding and personnel, the Department of Defense has developed a six phase security protocol to protect DOD and military computer networks from cyber-attacks. The first phase in the protocol, criticality, is to determine what information needs to be protected and how much protection is needed based on information to be protected. This phase also includes finding the weak points in the current systems and networks security programs (Cordesman, 118). One method the Department of Defense uses to determine weaknesses in their current

security procedures is by playing war games. The games create "Red Teams" that will simulate enemy attacks against the network as though they were attacking in a real war (119). The second phase, prepare, relies on strengthening the trustworthiness of the agents and the computers they use. Protect assets, the next stage of the DOD's security protocol, deals with determining what information needs the most protection. The possibilities in this step could be moving classified information to a network isolated from the global civilian Internet and developing a strong network defense system to protect all information on the Department of Defense's networks. The fourth stage, detect, scours the DOD's information networks to determine possible weaknesses or minor problems that could be exploited in the event of a cyber-attack. The fifth phase of the plan is the respond phase. In the event of an attack on the nation's information networks, this phase responds to the attack by fixing the system components damaged in the attack. The final stage of the DOD's security system, strengthen foundation, strengthens the network by amending the known weaknesses in the program and redesigning the security programs according to the anticipated future of cyber warfare (118).

Another step in the process to make the United States' computer network infrastructure secure took place with the creation of four new computer network communications related agencies under Presidential Decision Directive 63-1998. The four agencies that were created are:

- The National Coordinator for Security, Critical Infrastructure and Counter-Terrorism
- The Critical Infrastructure Assurance Office (CIAO)

- The National Infrastructure Protection Center (NIPC)
- The Information Sharing and Analysis Centers (ISACs)

The CIAO is concerned with the security of the economic and critical infrastructure. The NIPC takes care of the government agencies' network security. The ISACs take care of the industry's computer network security ("Cyber-Security...", 3).

**Hacking**

Hacking is a serious problem on both the military and civilian Internets. If a website or a system is hacked into, the information on that page or in the system could be changed. If there is classified information on the system or website that information could be accessed by foreign agents or spies (Cordesman, 18).

It has been mentioned that there were online terrorist hacker training camps but this is a myth (Gross, 2). However, Interpol states that there were a total of thirty thousand websites with free hacking software available to anyone who accesses the sites (Cordesman, 11). The types of software found on these sites can help a potential hacker build a virus to gain a path into a network or offer the hacker a free program to find weaknesses in a network's security system (McClellan, 1). Computer programmers have also aided, intentionally or unintentionally, hackers by building trapdoors and backdoors into their programs. Trapdoors and backdoors are meant to help systems administrators and programmers fix software problems yet these holes can be found by using programs offered online (Cordesman, 115).

In 1999, the Department of Defense stated that there were over twenty two thousand cyber terror attacks over the course of one year. These attacks were hacks

into other computers and the spread of viruses. Only three percent of these attacks actually caused any damage and about one percent of the attacks were hackers breaking into unclassified documents. The attempts to hack into the Department of Defense's computer networks, the same year, rose above fifty thousand, all of which failed (Gross, 2). As of July 2000 the amount of attacks rose ten percent (Cordesman, 114).

In a war game occurring in 1998, a group of NSA agents used hacking software downloaded free from the Internet to simulate a cyber-attack. The damage of the simulated attack using the easily acquired software included shutting down the power grid of the entire Pacific Coast and removing the United States Military's Command and Control communication networks (Gertz, 1). The extent of this damage was aided by the poor choice of passwords of most military personnel. Most passwords at the time were "password" (2). Another attack occurring in the late 1990's, two hackers accessed all of Rome Labs computer systems, used by the Army Corps of Engineers, and some systems worldwide (Cordesman, 41). The surprising fact of this attack is that one of the hackers was only sixteen years old with a twenty five megahertz computer, which at the time was still not the best computer on the market (43).

The best way to defend against hackers is by building a strong network security program, such as the DOD's security program mentioned on pages 32 and 33 of this paper, in every section of the Department of Defense (Cordesman, 138). However, not just any security program will do. Building a security system of only firewalls will not stay secure very long (Gruber, iii). The system should have

network monitors and human personnel viewing network activity in addition to the firewalls to determine whether the data being transferred is good or bad (iv). Also, the fact that the user is the biggest asset in network security must be stressed (Cordesman, 158). It was measured that ninety percent of network defense is the user's responsibility (153).

Antivirus software can protect against incoming viruses as long as the software is updated properly and frequently (McClellan, 2). Another method the Army uses in the fight against hacking is not to use programs designed for general civilian use on systems and networks containing classified information (Cordesman, 115).

# Glossary of Abbreviations

ARPANET – Developed in 1969 by DARPA, ARPANET was the first "Internet" designed for the military as a communication system that could withstand a nuclear war.

Autodin – Automatic Digital Network, designed by the Defense Communications Agency in 1963 for the Army and Air Force as a worldwide electronic data communications network.

BLOS – Beyond line of sight communication, such as satellite communications.

CIAO – The Critical Infrastructure Assurance Office

Criticomm – Created by the NSA in response to the insecurity of Autodin.

DARPA – Defense Advanced Research Projects Agency, creators of ARPANET.

DISA – Defense Information Systems Agency, the agency with the responsibility of keeping MILNET secure.

DISN – Defense Information Switched Network, the name for the military's version of the Internet.

EMP – Electromagnetic Pulse occurs at the detonation of a nuclear device. It is harmless to personnel but fatal to computers and their components.

GPS – Global Positioning System

IC – Integrated Circuit

ISACs – The Information Sharing and Analysis Centers

JTF-CNA – Joint Task Force-Computer Network Attacks

JTF-CND – Joint Task Force-Computer Network Defense

JTF-CNO – Joint Task Force-Computer Network Operations

JTRS – Joint Tactical Radio Systems

LAN – Local Area Network, a computer network spanning over a small geographical area such as an office or building.

MCF – Military Computer Family, a standardization strategy for the military's computer systems.

MILNET – The original name for DISN

MIST – Multiband Integrated Satellite Terminal

NATO – North American Treaty Organization

NIPC – The National Infrastructure Protection Center

NSA – National Security Agency

NSFNET – National Science Foundation Network, the initial model for the modern civilian network.

PCM lasers – Pulse color modulated lasers.

TCP/IP – Transmission Control Protocol/Internet Protocol

UAV – Unmanned Aerial Vehicle, also known as a drone.

WAN – Wide Area Network

WIN-T – Warfighter Information Network-Tactical

WWMCCS – Worldwide Military Command and Control System.

# Bibliography

"The Army's Bandwidth Bottleneck." August 2003. IWS-The Information Warfare Site. http//www.iwar.org.uk/rma/resources/cbo/bandwidth-bottleneck.htm (31 Dec. 2003).

Bergen, John D. United States Army in Vietnam. Military Communications, A Test for Technology. Washington: GPO, 1986.

Cisco Systems, INC. Cisco Networking Academy Program: First-Year Companion Guide 2nd Ed. Indianapolis: Cisco Press, 2002.

Cordesman, Anthony H. and Justin G. Cordesman. Cyber-threats, Information Warfare, and Critical Infrastructure Protection: Defending the U.S. Homeland. Westport, CN: Praeger, 2002.

"Cyber Security-How Can We Protect American Computer Networks from Attack?" Committee on Science: US House of Representatives. Hearing Charter. 10 Oct. 2001. http://www.house.gov/science/full/oct10/full_charter_101001.htm (1 Jan. 2004).

Debastiani, Richard J., Col. Computers in the Battlefield: Can they Survive? Washington: GPO, 1983.

"Digital Warfare System Adapted to Hunt for Rebel Leaders." The Courier Times. New Castle, IN. 2 Jan. 2004. A1, A3.

Gaudin, Sharon. "Cyber-warfare: Latest Weapon in Military Arsenal." 28 Feb. 2003. http://itmanagement.earthweb.com/secu/print.php/1856001 (20 Nov. 2003).

Gertz, Bill. "Computer Hackers Could Disable Military." 16 Apr. 1998. http://www.newdimensions.net/headlines/m02.htm (21 Nov. 2003).

Gross, Grant. "Are Military Computers Safe?" PC World 24 July 2003. PCWorld.com. Online. Google. (20 Nov. 2003).

Gruber, David J., Lt. Col. "Computer Networks and Information Warfare: Implication for Military Operations." July 2000. Center for Strategy and Technology: Air War College: Air University, Maxwell Air Force Base, Alabama.

"Joint Task Force-Computer Network Operations." Feb. 2003. http://www.stratcom.af.mil/factsheetshtml/jtf-cno.htm (20 Nov. 2003).

McClellan, Alain, Senior Master Sgt. "Attacks and Threats Against Military Computer Networks Continue." http://www.vnis.com/story.cfm?textnewsid=558 (20 Nov. 2003).

Torrieri, Don J. Principles of Secure Communications Systems. Dedham, MA: Artesh House, INC., 1985.

"U.S. Military Grapples With Cyber Warfare Rules." 8 Nov 1999. http://www.hartford-hwp.com/archives/27a/021.html (21 Nov. 2003).

"Wearable Computers for the Military." 9 Dec. 2002. http://www.webdesk.com/wearable-computers-for-the-military/ (21 Nov 2003).