Computer Networks and Information Warfare

Implication for Military Operations

David J. Gruber, Lt Colonel, USAF

July 2000

17

Occasional Paper No. 17
Center for Strategy and Technology
Air War College

Air University
Maxwell Air Force Base

Computer Networks and Information Warfare:
Implications for Military Operations

by

David J. Gruber, Lt Col, USAF

July 2000
Occasional Paper No. 17
Center for Strategy and Technology
Air War College

Air University
Maxwell Air Force Base, Alabama

Computer Networks and Information Warfare: Implications for Military Operations

David J. Gruber, Lt Col, USAF

July 2000

The Occasional Papers series was established by the Center for Strategy and Technology as a forum for research on topics that reflect long-term strategic thinking about technology and its implications for U.S. national security. Copies of No. 17 in this series are available from the Center for Strategy and Technology, Air War College, 325 Chennault Circle, Maxwell AFB, Montgomery, Alabama 36112. The fax number is (334) 953-1988; phone (334) 953-2985.

Occasional Paper No. 17
Center for Strategy and Technology
Air War College

Air University
Maxwell Air Force Base, Alabama 36112

Contents

Page

Disclaimer

The views expressed in this publication are those of the author and do not reflect the official policy or position of the Department of Defense, the United States Government, or of the Air War College.

The Author

Lieutenant Colonel David Gruber, USAF, is an electrical engineer who has spent his career in communications and computer positions. Prior to attending the Air War College, he was the Chief of Networks for Air Combat Command, where he was responsible for the design, installation, operation, and funding of classified and unclassified computer networks at numerous Air Force bases. He was instrumental in fielding the Defense Message System and developing the tactics, techniques, and procedures for network operations throughout the Air Force. He also designed and fielded networks in support of multiple expeditionary force deployments throughout Southwest Asia. While in command of the Communications Squadron at Moody AFB, Georgia from 1994 to 1996, he developed the operational plans and deployed support for the Air Force's first Air Expeditionary Force. Earlier, Lieutenant Colonel Gruber served as the communications engineer supporting the Chairman of the Joint Chiefs of Staff, the communications design engineer for the Next Generation Weather Radar (NEXRAD), and as a satellite earth station installation engineer. He has published articles on the command and control of Air Expeditionary Forces and Cyber Attacks. Lieutenant Colonel Gruber received his BSEE from the US Air Force Academy and a Master of Science in Systems Management from the University of Southern California. He has attended Squadron Officer School, the Army Command and General Staff College, and the Air War College.

Preface

The growing need for computer network defense is critical to the ability of the U.S. military to conduct operations, but there is no general understanding or or agreement on the meaning of the term. The first step in building a consensus is to gain a common view of how information has grown into a critical component that directly affects the conduct of military operations. Given discussions about the concepts of network warfare and cyberspace, the U.S. military needs is a framework for describing cyberspace and computer network defense.

One analogy is that of airspace management, in which the roles and responsibilities of the Federal Aviation Administration, NORAD, and the National Weather Service in managing and protecting airspace provide a framework for describing the roles and responsibilities of network operation centers, network defense centers, and the Defense Information Systems Agency in managing and protecting cyberspace. With this construct, the operations, intelligence, and communications communities within the U.S. Air Force will be able to coordinate their efforts to improve computer network defense in an age when the U.S. military depends on information for the conduct of military operations.

The U.S. Force, with its emphasis on global reach, global power, and global command and control, has grown to become highly dependent on the flow of information to combat and support units. The problem, however, is that the U.S. Air Force view on information operations and especially the concept of defensive counterinformation that involves protecting those operations, does not provide an adequate concept for protecting that information. The present approach by the U.S. Air Force is to build insurmountable walls around its networks in order to prevent adversaries from threatening U.S. information systems. Since history is littered with examples in which fixed defenses failed, this strategy for defending information networks will not be effective.

This study argues that military organizations need to establish operational approaches to cyberspace, and that the current approach for organizing air operations provides a useful construct for thinking about this problem. In principle, air traffic controllers use a hierarchical organization to identify and track all aircraft that enter and leave a controlled space. One group of controllers manages the airspace around airports, a second group is responsible for managing the air routes between airports, and a third group of controllers manages the airspace in hostile environments. At the same time, meteorologists also are involved in managing air traffic because when a severe storm threatens air routes or specific airfields, meteorologists work with the air controllers to re-route traffic.

An important function of air defense controllers is to monitor air traffic by searching for aircraft that do not belong in a particular location. When an unidentified aircraft is found, air defense controllers determine whether it is friendly or hostile, and if hostile, direct military aircraft to deal with the threat. Air superiority is derived from the ability to identify these vehicles and to prevent them from using airspace. The unifying element in managing friendly aircraft, monitoring the environment, and protecting against hostile aircraft is common situational awareness, which is a product of the information that is created by airport surveillance radar, in-transit radar, and air defense radar. As a consequence, three communities with different functions work together to manage and protect airspace. It does not matter whether the airspace environment is benign, such as that over the United States, or hostile, as is the case when the Air Force engages in combat operations against an adversary. This model for managing airspace has important implications for computer network defense.

The current Air Force approach to computer network defense uses computer personnel to monitor network traffic as it enters protected areas. Like a virtual gate guard, these personnel attempt to differentiate good and bad traffic, and when bad traffic is detected, the computer personnel block it while allowing everything else to pass through the network. This model has several drawbacks. The first is that the only way to identify bad traffic is if it has been previously identified as such, which implies that an attack with a previously unknown code sequence will not be stopped if computer personnel do not recognize it.

Second, an attack on the computer network could be conducted with a legitimate code sequence by sending thousands of email. In this way, an attacker could prevent the receipt of legitimate email by sending thousands of electronic mail messages to that individual, which is comparable to mailing millions of empty envelopes to the same address. The problem is that an electronic gate guard could not effectively stop this attack because each individual electronic mail message is legitimate, and the network personnel will have no idea whether the traffic is good or bad because the only purpose of these gates is to identify whether traffic reaches its intended destination.

The purpose of this study is to improve the understanding of the defense establishment of the growing importance on information networks in the U.S. military, with particular emphasis on the role of computer network defense in the U.S. Air Force.

I. Introduction

The ability to disrupt, disable, or create military effects with cyber-attacks has gained increasing attention in the U.S. military. Unfortunately, the development of information warfare as an offensive tool raises concerns about the vulnerability of the United States, which is highly dependent upon the flow of information. The problem is that the United States may present a more lucrative set of targets for information attack than many of our potential enemies. As the President's Commission on Critical Infrastructure Protection argued, the United States is highly vulnerable to cyber-attacks against power grids, the banking system, and communications networks. This dependence upon information, which has profound advantages for the U.S. military, implies that the United States is vulnerable to an attack by determined adversaries and raises questions about the ability of the U.S. military to conduct combat operations.[1]

As exemplified by the Persian Gulf War, the U.S. Air Force had developed a systematic approach for attacking an adversary, which rested on defining a nation's wartime capability in terms of a system of systems.[2] With this approach, the U.S. military produced an air campaign that was so devastatingly effective that it prevented Iraq from continuing military action against Kuwait or even from defending itself against coalition attacks. By using military force to destroy Iraqi command and control information systems, these attacks blinded the Iraqi leadership and disrupted their ability to conduct synchronized combat operations. Not only did this lead to victories in every encounter with Iraqi military forces, but this degree of success against Iraq demonstrated the importance of information in military command and control and highlighted the vulnerability of the systems that carry this information.

These lessons reinforced the experiences learned in earlier contingencies by highlighting the growing importance of information in offensive and defensive operations. This realization was enshrined in U.S. military doctrine when General Shalikashvili, who was Chairman of the Joint Chiefs of Staff, identified "information superiority" as the critical element that would lead to military success.[3] The Air Force believed that it was uniquely qualified for this mission, and claimed information superiority as one of its six core competencies.[4] When the Air Force published *Cornerstones of Information Warfare*, it argued that both offensive and defensive information operations are critical to the U.S. Air Force and the military services, and should be a central component of Air Force doctrine.[5]

The U.S. Air Force used similar terminology for information operations as it did for air power in general. The concept, according to air power theory, is that by destroying precisely defined targets, an adversary can be defeated without the need for the use of opposing armies.[6] If a ground war is required, air power will weaken the enemy to the point where ground forces will be required to "mop up" enemy pockets of resistance and occupy enemy territory. The objective of the U.S. Air Force was to incorporate information operations into the theory of air power in the same fashion as the other components of aerospace power. The intent was to create effects against the adversary while simultaneously protecting the United States and its military forces from attack.[7]

When the Air Force Doctrine Center published *Air Force Doctrine Document 2-5, Information Operations* in August 1988, it defined information operations in terms of two concepts.[8] The first, which is known as "information-in-warfare," involves actions and processes that are designed to gain and exploit information. The other concept, "information warfare," comprises the actions that are designed to attack and defend information and information systems. This doctrine emphasized the role of defensive counterinformation, which refers to protecting the ability of the U.S. Air Force to conduct operations. This concept received the highest priority.[9]

The emphasis on defense raises the question of what must be defended. The initial answer was demonstrated by the establishment of the U.S. Department of Defense's Joint Task Force for Computer Network Defense. The problem, however, is that the network, as with the concept of airspace, is too broad to be defended. Since the original DOD Advanced Research Project Agency network (ARPANET), which was the forerunner of the Internet, was designed to withstand the massive destruction that nuclear war would create, and have the redundancy to continue to support the surviving forces, the network in effect encompasses all of cyberspace.[10]

This network, which can be understood as units that are the size of air force bases, uses sensors at a limited number of points of entry and departure to provide defense. In addition, the DOD Internet, which is known as the Defense Information Switched Network, has a limited number of connections to the civilian Internet, which could be used to monitor traffic and block intrusions. This approach was tried when the short-lived Air Force Information Warfare Squadron at Shaw AFB in South Carolina installed sensors at every air base in the 9th Air Force and at locations in Southwest Asia. The Air Force learned a number of lessons from this experiment. One lesson was that while the squadron could identify and counter some attacks, they could not identify all of the attacks, including the cyber attack against Langley AFB in Virginia that was cited by the Presidential Commission.[11] Another lesson was that this squadron did not improve the flow of information or improve the security of the network. The unanswered question from the experiment with the Information Warfare Squadron is whether defending the network is the proper way to protect the information systems of the U.S. military.

The first attempt at network defense was organized in terms that are similar to how Air Force security police protect a combat air base. Few would argue with the proposition that maintaining air base perimeter defense and controlling the base gates are essential to Air Force operations. Similarly, few would argue that network defense is unimportant. Since the real function of networks is to facilitate the flow of information from one location to another, protecting this information flow will demand the development of concepts that transcend the typical approaches to network defense.

II. Military Operations and Information Systems

The dependence of the U.S. Air Force on information systems has grown tremendously. During the early days of flight, the primary function of airpower was reconnaissance, which sought to determine the enemy's order of battle while denying the same information to the enemy. The information requirements for this mission were few. The reason was that the higher headquarters tasked flying units to search for enemy units within certain coordinates, and since both the headquarters and flying units used the same maps, the information that was passed consisted of grid locations. However, the combat support functions always involved a greater dependence on information because the airfield could not operate without a ready supply of fuel, parts, food, personnel, and money. What began as austere information requirements steadily grew during the inter-war years.

During World War II, the dependence of air power on information increased dramatically, particularly in terms of the time-critical functions of command and control, weather, and intelligence. To conduct military operations, aircraft units required significant amounts of information, including rough target coordinates, precise arrival times, the coordinated plan of attack and logistics information, of which available fuel, munitions, and aircraft status are notable examples. This information flowed between the higher headquarters and the support bases to the expeditionary airfields, but by modern standards, the total amount of information was low. For example, target coordinates were defined in square blocks rather than the detailed coordinates that are used today, and weather maps were sent by facsimile machines and teletypes.[12] Although the amount of information that was required to sustain operations was small by modern standards, it still taxed the communications systems of the era.

The integration of computers, communications systems, and satellites for the U.S. military began during the tenure of Robert McNamara as Secretary of Defense in the 1960s. McNamara used these technologies to centralize the military command and control system in what became known as the Worldwide Military Command and Control System (WWMCCS). While this system never fully integrated all of the functions of command and control, the ability to link these technologies dramatically increased the situational awareness of military commanders.[13] By the late 1960s the Department of Defense had become heavily dependent on automation systems to process the information that was necessary for the military to conduct combat operations.

The conduct of theater level operations changed dramatically by the introduction of computer and communications advances, especially during the Vietnam War. The use of computers, precision guided munitions, and electronic warfare systems had a decisive effect on a wide range of military functions during this war.[14] Intelligence officers used data from multiple systems to determine enemy force locations and capabilities. Automated command and control systems enhanced the ability of the military services to integrate their combat actions. And the logistics systems that managed the huge flow of equipment and supplies from the United States to the Far East grew increasingly dependent on information systems. Significant changes to combat operations resulted from the development of satellite reconnaissance and smart weapons. For example, munitions required the extremely precise targeting data that satellites could provide, although flight planning was still conducted with “paper charts and grease pencils,” despite significant advances in automation and access to huge amounts of data. [15] With the emergence of these automated tools, the Vietnam War marks the time when the U.S. Air Force became highly dependent on the timely flow of information.

The Air Force and the Navy had only limited situational awareness of the airspace over Vietnam, which was produced by three U.S. Air Force radar systems. The Air Traffic Control and Landing System used long-range radars to manage the airspace in theater. The second was the Tactical Air Control System, which functioned as ground control intercept radars for directing friendly aircraft toward enemy aircraft. The third was a modified bomb scoring system radar, which the Strategic Air Command had used to evaluate the bombing efficiency of aircrews at bomb ranges in the United States. Air Force planners determined that instead of evaluating proficiency, the system could be redesigned to direct aircraft to specific locations and signal when to drop bombs over targets regardless of weather conditions.[16] In 1966, this system, which was known as Combat Skyspot, was deployed to five bases in South Vietnam and one base in Thailand. By the end of 1966, air controllers had directed 10,000 missions.[17] In addition to these Air Force capabilities, the U.S. Navy provided air traffic control and airborne intercept with both ship and airborne radars. As a result of these systems, the U.S. military developed a significant capability for tracking friendly and enemy aircraft and directing friendly aircraft to attack enemy targets.

As a consequence of lessons from the Vietnam War about situational awareness in air combat, the Air Force developed the Boeing E-3A Sentry Airborne Warning and Control System (AWACS) in the late 1970s. Among the significant advantages of airborne radar over ground based systems is the fact that enemy aircraft cannot hide behind terrain, which provides a measure of timeliness and flexibility that ground based systems lack. With this technological advance, the Air Force gained a qualitative edge because the information collected by radar could be distributed throughout the theater. For example, the locations of target were available on displays in the cockpits of fighter aircraft at nearly the same time that radar provided data to the controllers in AWACS aircraft. The ability to feed the exact locations of targets into the guidance systems of precision air-to-air and air-to-ground munitions effectively increased the operational effectiveness of military forces and decreased the reaction time during military operations.[18]

As the U.S. Air Force learned during the Persian Gulf War, it could no longer plan and conduct air combat operations with industrial age tools, which for the operational community meant that new technological approaches to controlling aircraft must be developed. During the Vietnam era, the Tactical Air Control Center evolved into a sophisticated Air Operations Center, which served as the focal point for air operations. Commanded by the senior Air Force commander and supporting the Joint Commander, the Air Operations Center included intelligence as well as planning, operations, and liaison groups. Later, the development of the Contingency Theater Air Planning System (CTAPS) automated many of the processes in the center, and demonstrated that much more development work was needed. As a result of the lessons learned during the Persian Gulf War, the Air Force massively redesigned how it would exercise command and control over air operations in the future.

One conclusion from the Persian Gulf War was that the U.S. Air Force was not fully prepared to support its logistics system. During the years before the war, nearly every functional area had been automated, which included the tools that order equipment, track aircraft maintenance actions, monitor the movement of critical parts, and even track pilot flight hours. In addition to logistics systems, manpower staffs needed access to automated personnel records, comptrollers needed access to financial information, and the medical community required access to patient records. All of these functions require access to computers that are located in the United States.

The U.S. military did not immediately understand that operational units in the field would need access to these information systems. Eventually, combat support personnel in Southwest Asia realized that they needed access to the same computer systems that they had used at bases in the United States. This requirement became a critical problem as airplanes in need of repair lined up on the tarmac because they were waiting for parts that personnel in the theater could not be certain had been ordered. The Air Force Communications Command responded by deploying a Base Assistance Team–Mobile from Gunter AFB in Montgomery, Alabama to Saudi Arabia, which consisted of the personnel, computer terminals, and communications equipment that are needed to connect to mainframe computers that are located in the United States. Once the terminals were activated, units in the field gained access to logistics information.

The significant lesson for the Air Force was that the absence of logistics, finance, personnel, and medical support systems would hinder its ability to sustain military operations overseas. To put this in the terms of classical military strategy, the support systems had evolved into a strategic center of gravity. However, this lesson was not put into practice in the U.S. military because after the war, combat support organizations used the same systems that they had used before the war, and developed new ones to automate other military functions. While little thought was given to how the U.S. military would use these systems during the next war, the emergence of the concept of an Air Expeditionary Force compelled the Air Force to reexamine this issue.

III. Emergence of Networks

An important aspect of the information revolution within the U.S. Air Force was the fact that it was not preceded by significant planning. In 1969, the Defense Advanced Research Project Agency developed a communications network, known as the ARPANET, that linked major universities and defense laboratories into a network that was designed to survive a nuclear blast, identify portions of the network that no longer existed, and route traffic around them.[19] While the initial ARPANET included only three universities in California and the University of Utah, what began as a limited experiment soon expanded into the preferred method of data communications by the Department of Defense and universities.

In view of its success, the network soon became congested, which led to the addition of numerous additional sites. Eventually, the Department of Defense removed the military segment from the ARPANET to create the MILNET, which was an unclassified network that was managed by Defense Communications Agency.[20] The National Science Foundation drew on lessons from ARPANET to develop the NSFNET, which later evolved into the Internet.[21]

As the MILNET matured, the DOD changed its name to the Defense Data Network, and later to the Defense Information Switched Network. The name of the Defense Communications Agency also changed to the Defense Information Systems Agency. An important point is that both of these civilian and military networks remain compatible because they followed common standards during development.

Once fielded, the Internet was constantly refined. Committees were established, first by the Government and then by concerned users, to evaluate and approve new ideas. While this technology matured rapidly and significantly improved the capabilities of the Internet, the early Internet lacked both system-wide management capabilities and built-in security, both of which hindered companies and universities when they tried to connect equipment from different manufacturers. It became apparent that the growth of the Internet would require strong network management, which resulted in a series of new protocols.[22] The DOD expanded the Defense Data Network to include nearly every military base, but supported a minimal volume of electronic mail because the Defense Data Network was not heavily used.

With the maturing of wide-area network technologies, the merger of data processing and communications was inevitable, which in the 1980s accelerated the process of bringing the communications and computer fields together. The Air Force upgraded base level data processing centers by merging these with base telecommunications centers, and by 1986 had both standardized and modernized the mainframe computers at 121 locations.[23] By standardizing its policies, operating procedures, and computer systems, the Air Force realized that it could generate significant savings by closing a number of base level data processing centers and consolidating their functions at a few regional centers.

It is important to understand that by the early 1980s personal computers had begun to enter the commercial world. Therefore, in order to access the base data processing center from anywhere on the installation, a “dumb terminal” at the user’s location was connected to the data processing center through multiple telephone wires. Since there were typically hundreds of dumb terminals at a base, the communications squadron would "multiplex" the multiple pairs of wires together by using technology similar to that used by the telephone industry. This process of regionalization did not change how users gained access to mainframe computers. Since the user was not typically located in the same building as the data processing center, the Air Force found that long-distance telephone carriers could extend the multiplexed telephone lines from the base computer to regional data processing centers. This process of regionalization was extremely successful because the Air Force realized significant cost savings since it reduced a large number of personnel positions while still providing an adequate level of service.

The Air Force was not alone in its efforts to consolidate and regionalize computer capabilities because the DOD was doing the same. While the Defense Information Systems Agency (DISA) believed that it should operate the networks that the Air Force had established to support regionalization, the Air Force argued that the networks which support Air Force functions should be controlled by the Air Force. At the same time, the DOD hoped to find savings by emulating initiatives in civilian industries. As a result, the Secretary of Defense issued a number of Defense Management Review Decisions, two of which -- Decisions 918 and 924 -- directed the consolidation and regionalization of Defense level data automation centers, and eliminated the dividing line between the DISA and the military services. Although DISA was given responsibility for building and operating all networks and applications, it did not have the necessary supporting structure. Later guidance from the Department of Defense limited DISA's role because it divided responsibilities between DISA and the military services. While the Air Force and the other Services controlled all voice and data communications within the their bases, DISA controlled all communications between the bases and the commercial Internet.

Initially, the Defense Management Review Decisions had little impact. Since the Air Force purchased telephone service from commercial telephone carriers, the principal change was to shift the contracting agency from the Air Force to DISA offices. But the merger of communications and computers was far from complete, which had significant implications for how information systems would be used in future conflicts.

The U.S. Air Force began to grasp the power of personal computers. In 1981, Air Force Communications Command created an office automation system, which within three years had grown into a local network that linked more than 600 computers.[24] This new tool provided a number of automated office aids, such as linked calendars, file sharing, and electronic mail. Given this success, the Air Force Communications Command established a Local Area Network (LAN) Office, which was tasked with developing standards for the rest of the Air Force. However, the Air Force Communications Command lacked the authority to make its recommendations mandatory across the Air Force, or to consolidate and centralize spending on automation throughout the Air Force.

In 1979, Intel Corporation co-founder Gordon Moore noted that the density of transistors on chips, and thus the price to performance ratio of computers, doubled every eighteen months, which he postulated would continue indefinitely.[25] The fact that computer power has doubled every eighteen months, in what later became known as Moore's law, had a significant effect on the Air Force. As computers became more capable, the Air Force established standard contracts that allowed any Air Force organization to procure them. Once equipped with the authority to buy their own computers and connect them as they wished, Air Force squadrons built local area networks that allowed squadrons to share internal files and expensive printers. The problem, however, was that most of the squadron LANs were built by inexperienced people who did not have well-defined maintenance concepts, the personnel to operate them, or adequate funding. In many cases, these “hobby shop” networks were so unreliable that they undermined the efficiency of the squadrons.

A critical development was the explosive growth in the volume of electronic mail, which started as a convenient way to communicate but evolved into the central tool for transferring information. Higher headquarters began to depend upon email as the “unofficial” means to get the word out across the major commands, while wing and base commanders learned that the loss of important email messages could have significant organizational and operational consequences. As wing commanders directed their communications personnel to connect the imperfect squadron LANs, by 1996 the Air Force moved to the point where all wing, group, and squadron commanders had electronic mail. However, this level of responsibility could not be handled by immature and under-funded network infrastructures and untrained communications technicians. There were significant efforts in the Air Force to deal with this technology, but this immature base information infrastructure could not provide the level of service that was essential for modern military forces.

As the Air Force leadership recognized that their dependence on the base information infrastructure was growing, it developed policies and guidance for managing this system. For example, the Air Force created the Network Control Center with responsibility for the base network as well as all data that entered and left the base. The Air Force used management tools to monitor network performance, and assigned personnel from the communications squadron to work in the Network Control Center, which was an essential step in improving network service. While not specifically authorized, other organizations on air force bases continued to procure equipment and build their own LANs. The network control center was theoretically responsible for network growth, but in practical terms any organization that had funds to spend on computer equipment could add what they wanted.

A further step in the evolution of the network occurred when U.S. Air Force personnel demonstrated the ability to use a personal computer to emulate the dumb terminal connection between the regional data processing center and the Defense Information Switched Network. This capability promised to produce significant savings for the Air Force. By the mid-1990s, the dumb terminals had outlived their usefulness and had become too expensive to maintain. Further, the cost of the long distance telephone calls that connected dumb terminals to regional centers was significant and growing. Many of the major commands in the Air Force realized that they could replace dumb terminals with personal computers that are connected to the base information infrastructure. The decision to give Air Force major commands the budgetary authority to replace dumb terminals with personal computers accelerated the development of base networks.[26] Finally, the Network Control Centers managed the growth of the network centrally.

The decision to add computers formally signified that the network was critical to the success of military operations. If the network went down for any reason, people at the base would not be able to gain access to the regional data centers. Another problem was that organizations which had reassigned their own manpower to operate their own LANs were reluctant to give control of the LAN to the Network Control Center. In the absence of additional manpower for supporting the LANs, the Network Control Centers could not guarantee that they would provide the same level of service as the base computer organizations. Not unsurprisingly, it was common to see the establishment of “fiefdoms” or rogue networks on the base, which were owned by the organizations who could spare the manpower but were controlled by the Network Control Center.

In summary, the network grew from a useful tool for sharing printers and files to a system that determined the ability of the U.S. Air Force to accomplish its peacetime and wartime missions. By the mid-1990s the Air Force directed the Combat Information Transfer System program office to install base networks, but in the absence of a master plan for managing this growth in computer networks, the dependence of the U.S. military on information had caught the Department of Defense and the Air Force by surprise.

Congressional Influence on Computer Networks

The U.S. Air Force as well as the Department of Defense sought to enhance productivity through automation, but there were many failures. The problem typically encountered by program managers was that the gradual expansion of system requirements led to automating all the functions of an organization. For example, a government division or branch would ask their information technology division to automate a specific business process, and senior management officials would ask their information technology office to evaluate whether the request was feasible and affordable. If the specific process could be clearly delineated, the technology office would approve the project and senior management would fund the request. Inevitably, someone would notice that the proposed system could have an even greater impact on the organization if just one more process was included. Senior management officials would concur, and the second process would be incorporated into the initial project. Usually, it took only a few minor "upgrades" before the system was so complex that doubts about whether it could be developed successfully would arise.

The growth in requirements was not the only reason for failure. In many cases, the requirement was simply too complex for current technology. For example, failures in major programs caused the DOD to restrict the growth of military requirements and force the military services to better estimate the total lifecycle costs of computer projects.[27] As a result of these problems, Congress created the Information Management Reform Act, otherwise known by the names of its primary authors, the Clinger-Cohen Act, which was incorporated into the National Defense Authorization Act of 1996.

The purpose of the Clinger-Cohen Act, which was to, "streamline information technology acquisitions and emphasize life cycle management of IT as a capital investment," changed how the government developed, procured, and operated information technology.[28] This act also repealed the Brooks Act, which had made the General Services Administration exclusively responsible for the acquisition of information technology. Instead of centralizing federal information processing in one organization, it gave the Office of

Management and Budget overall responsibility for acquisition and management policy, and made the heads of executive agencies responsible for acquiring information technology and effectively managing their technology investments.[29] The Clinger-Cohen Act was a landmark piece of legislation because it required federal agencies and departments to demonstrate that investments in information technology would actually improve business processes. Congress wanted evidence that the money being invested in information technology would result in cost savings and increased efficiency.

A significant provision of the Act was the requirement that executive agencies appoint a Chief Information Officer (CIO), which in addition to advising the head of the executive agency, would be responsible for developing, maintaining, and implementing the organization's information technology architecture as well as automating work processes.[30] The intention was for the CIO to manage the network equipment and computers as well as the computer software.

Not surprisingly, the Clinger-Cohen Act had a significant effect on government agencies. In the case of the Department of Defense, the Secretary of Defense appointed the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence as the new CIO for the department. In the Air Force, the Assistant Secretary of the Air Force for Acquisition was appointed as the first Air Force CIO, and charged with working directly for the Secretary of the Air Force. The Air Force CIO had the authority to delegate its power to subordinate commands, which allowed the Air Force major commands (MAJCOM) to appoint their own directors of command, control, and communications, who reported to both the MAJCOM commander and the Air Force CIO.

With this new structure the Air Force gained the ability to resolve a number of problems. A prominent example was the large number of automated systems that were created in a "stovepipe" fashion. While personnel officials developed personnel systems, and intelligence agencies developed intelligence systems, there was no central authority to ensure that the systems were optimized to support the needs of distributed users or that they were interoperable. Worse yet, no one analyzed the traffic or security implications of these disparate systems for the DOD, the military services, or the base information systems. The Clinger-Cohen Act offered to fix this problem because, for the first time, Chief Information Officers were given the authority to integrate information technology projects across the DOD, the Air Force, and the major commands. This development would have profound implications for the U.S. Air Force as it shifted toward an expeditionary force in the late 1990s.

IV. Expeditionary Air Force and Information Networks

The dependence on the flow of information has been accelerated by the sophistication of weapons systems, their dependence upon a support infrastructure, and the evolution of the U.S. Air Force into an expeditionary force. Taken together, these trends are compelling the military to reexamine the concept of computer network defense.

The U.S. Air Force relies on a large communications infrastructure at each base to carry hundreds of simultaneous telephone conversations and support the flow of classified and unclassified computer communications. In the case of an overseas base, the volume of external communications is so drastically limited that in some cases the base can handle roughly 24 simultaneous conversations.[31] The problem, however, is that the amount of information which is required to launch a single sortie continues to grow, as exemplified by the data required for targeting. For example, targets are defined in terms of square inches rather than city blocks. Since a single sortie could be used to attack several targets, flight planning involves the identification of flight paths with three-dimensional accuracy that is measured in tens of feet. This is especially important when the attacker wants to use terrain to mask aircraft from air defense sites. The information demands of targeting are further complicated by the ability to download target coordinates from satellites to munitions that are on aircraft as those aircraft are flying into combat.

The ability to conduct such attacks places a tremendous burden on the information infrastructure, in particular on the information needs for operational planning. As newer aircraft are built with more sophisticated computers, the need for information likewise increases. In the case of the B-2 bomber, the flight crew uploads computer files that were built at the base mission-planning center, which the aircraft uses to determine its flight path, ingress and egress points, and target locations. The flight crew creates this information from high-resolution maps, satellite imagery, and the Global Positioning System. In addition to programming munitions with the precise locations of the targets, the crew will use bomb damage assessment imagery to review in real-time the effects of the attack and to determine the aimpoint for subsequent weapons. While each of these functions requires huge amounts of data, the exponential growth in the information that is required to support a single sortie will increase even more significantly in the future. For example, the projected information that will flow into the maintenance hanger for the F-22 fighter aircraft will exceed the capacity of any base network that is currently operated by the Air Combat Command.[32]

The advent of the Expeditionary Air Force is forcing the U.S. military to reexamine the information that it will need for conducting combat operations. The U.S. Air Force has shifted its thinking from a force that is forward-deployed on bases around the world to a force that is based in the United States and that deploys in times of crisis. The implication is that military equipment must be lighter and require less space because it will be moved from garrison bases in the United States to overseas bases. Most of U.S. Air Force fighter and bomber squadrons do not have significant problems with this conversion because Air Force combat squadrons are designed for forward deployment from bases in the United States to prepared sites in Europe. By contrast, combat support squadrons have a great deal to learn about deploying to forward locations. The problem is that support organizations continue to be dependent on databases that are located in the United States, and that the amount of information that flows between support organizations and mainframe computers in the United States has grown since the Persian Gulf War because more wartime processes have been automated.

The lesson that modern military operations require significant amounts of information was apparent during the deployment of the first Air Expeditionary Wing (AEF) to Bahrain in 1996. Some of the combat support squadrons that had not deployed overseas since the Persian Gulf War brought the same “dumb terminals” that they had used during that war. While these could not be connected at the deployed base, communications squadrons brought enough equipment to build a limited information infrastructure at the deployed bases, which involved both an unclassified segment for combat support use and a classified segment for command and control. In addition, combat support squadrons attached network-capable laptop computers to the network so that they could communicate with computers in the United States, use electronic mail, and connect to the Internet.[33] The Wing Operations Center deployed with laptop computers that could be attached to the classified network, and that could receive the air tasking order, classified imagery, and other command

and control information. An important lesson from the experiences of the first Air Expeditionary Force was that a robust information infrastructure would be vital to military success.

Subsequent deployments of the Air Expeditionary Force to Jordan, Qatar, and Bahrain included the equipment that was necessary for building a robust information infrastructure. These steps, however, did not solve the problems associated with expanding what still remains the limited capability of the external communications systems that handle classified systems and transmit satellite imagery. An unresolved problem, which was identified by the Air Combat Command Commander, General Richard Hawley, is how much bandwidth is necessary to supply the imagery that military organizations are likely to require in modern combat operations.[34]

This question raises significant issues about the architecture that the Air Force had proposed for protecting U.S. Air Force information systems, which in military jargon is known as defensive information operations. The fundamental problem with both classified and unclassified networks relates directly to the failure of the Department of Defense to focus on the information flow itself. Since no individual was responsible for understanding how computers at deployed locations actually communicate with databases in the United States, organizations produced their own highly individualized information systems that did not support the ability of the U.S. military to conduct combat operations. However, this approach raises questions about the ability of the U.S. military to assure access to the information that will be needed to support military operations.

V. Framework for Computer Network Defense

The emphasis on information warfare has reduced the ability of the Defense Information Infrastructure to support combat operations. The underlying reason is that the current U.S. approach emphasizes the importance of watching for hostile computer attacks rather than supporting the flow of information that U.S. forces need to conduct military operations. Not unexpectedly, the focus on watching for hostile computer attacks has distorted the fundamental purpose of the information infrastructure, which is to assure that information flows from computers in the United States to operational units that are located at remote locations.[35]

One solution to this problem is to consolidate all of the information organizations under one commander, who would have the authority to implement policies that are designed to support combat forces in the field. In fact, most of the groups involved in defending computer networks already work for the same organization. For example, the Defense Information Systems Agency serves several functions, including developing and operating the mainframe computers and network infrastructure that supports the continental United States and European divisions of the Defense Information Switched Network. This organization is devoted to network defense. In the case of Southwest Asia, the United States Central Command controls the network that is established by air expeditionary wings at overseas bases. The underlying problem is not the existence of too many independent organizations, but the tendency of organizations to use independent standards for optimizing their performance rather than using common standards for the entire system.

The U.S. military needs to develop a framework for computer network defense that optimizes the performance of the entire system rather than optimizing the connectivity of individual subsystems. Again, the case of how in-flight aircraft are managed provides a useful analogy. The DOD and Federal Aviation Administration track an aircraft flight from its source, or its entry into U.S. controlled airspace, to its destination. Success is measured not by whether any specific radar or traffic control center is available, but with the safe arrival of flights. At the same time, the system can identify and investigate potentially hostile aircraft in a coordinated fashion. Success is measured in terms of the ability to track friendly aircraft or react to hostile aircraft, while failure is expressed in terms of near misses and time delays.

This aircraft traffic model is relevant to how the U.S. military manages the information infrastructure. In the early days of electronic communications, success was measured by whether a communications line was in place, which meant that if an individual at one end of the line could signal a person at the other end and receive a reply, then the circuit was in working properly. If the person did not receive a response, then the line was cut or the person at the remote end was not there. As technology matured and many circuits were multiplexed on a single line, the measure of success evolved into the status of the numerous circuits and equipment to which it was connected. But this approach can produce failures.

For example, when the Commander of Air Combat Command visited Prince Sultan Air Base in Saudi Arabia in 1996, U.S. Air Force personnel complained that they were spending too much time updating maintenance information on systems that communicated with mainframe computers in the United States. The problem was that a division in the Defense Information Systems Agency, which was responsible for the European segment of the Defense Information Switched Network, had unilaterally prohibited the network in Saudi Arabia from using an outgoing circuit. This decision produced congestion on that circuit, which meant that all communications traffic going in and out of Saudi Arabia was delayed. While the local communications personnel, the United States Central Command, and the Defense Information Systems Agency focused on checking the status of equipment, it was more important for these organizations to monitor the flow of information through the network – just as aircraft controllers monitor the progress of aircraft moving from one area to the next.

A second example occurred during the 1996 Joint Warfighter Interoperability Demonstration, which was one of the first times that the 9th Air Force Information Warfare Squadron supported an exercise. While communications personnel built a network that connected the mock base at Shaw AFB to the outside world, personnel at the Information Warfare Squadron evaluated the traffic between the deployed base and the remote mainframe computer on the basis of whether that traffic was on their approved lists. When that traffic was not approved, the squadron blocked that traffic on the network. One lesson from this experience is that a failure to coordinate the actions of those who support information flow with those who defend against network attacks will predictably cause missions to fail. If the U.S. military used this approach for air traffic control, it would lead to the destruction of friendly aircraft when aircrews failed to file flight plans.

It is imperative for network control organizations to minimize the time that it takes for information to move from one location to another, rather than monitoring whether equipment is operating properly. More importantly, these examples highlight the need for a model of computer network defense that manages and protects computer networks in an era when U.S. military forces are increasingly dependent on information systems for supporting military operations.

VI. Conclusion

If the model for computer network defense that is used by the U.S. Air Force was similar to the air control model, the focus of computer network defense would shift from watching roadblocks to ensuring that information flows reliably and regularly – in much the same way as air traffic control and air defense systems support aircraft operations. With this approach, computer network defenders and network controllers would share the same situational awareness, which would have profound implications for the success of defending computer networks against attack.

One implication would be to prevent corrupted software from entering computer networks through floppy disks or communications links. The Air Force and DOD policies require users to protect themselves by scanning new disks with virus protection software packages. This function of computer network defense is comparable to the air traffic control model because it means that network "defenders" would have the authority to scan traffic on the network, much as airports have the authority to scan passengers and cargo for weapons and other illegal goods.

A second implication for network defense involves the question of defined airways, which in the case of airspace management means that controllers maintain the separation of aircraft by distance and altitude. All aircraft heading across the United States must fly within designated routes, or assigned air routes in the sky, which provide a safety margin because controllers can more easily separate traffic if they know the direction in which the traffic is heading. If we apply this analogy to computer network defense, network information systems would require that all electronic mail is confined to the same port numbers and web addresses. The function of network controllers is to monitor traffic on these port numbers and web addresses just as air controllers monitor planes in flight.

The third implication relates to how air-defense controllers monitor friendly air traffic while looking for threats. The function of air-defense controllers is to search for flights that are not being managed by air traffic controllers, particularly those that cross national borders, by linking radars that monitor the air traffic along the nation's borders with radars that monitor air traffic within the country. To employ this model of an integrated picture of all air traffic for cyberspace, network controllers would monitor traffic and take action to deal with intruders. When the network is congested, network controllers will have the ability to divert critical information around congested areas, which is analogous to the ability of air traffic controllers to divert air traffic around storms.

In conclusion, the objective for the U.S. military is to create a system which encourages those who manage the network and those who monitor and protect the free flow of information to share a common view of cyberspace. The military personnel who are responsible for providing information assurance, which is similar to controlling aircraft, will be responsible for monitoring and controlling the movement of information between bases at overseas locations and mainframe computers in the United States. The intent is to ensure that those who search for computer attacks will share the same information as those who manage congestion and delays in the network.

It is inevitable that as the U.S. military builds an information system that increases its effectiveness in military operations, the ability to defend computer networks will be as essential to the successful conduct of military operations in the twenty-first century as defending airbases was in the twentieth century.

Notes

1. Executive Order 13010 of July 15, 1996 as amended on November 13, 1996 and April 3, 1997.

2. John Warden III, "The Enemy as a System," *Airpower Journal,* Spring 1995, pp. 41-55.

3. *Joint Vision 2010*, Published by the Chairman of the Joint Chiefs of Staff, p. 19.

4. *Global Engagement, A Vision for the 21st Century* Air Force, p. 9.

5. *Cornerstones of Information Warfare*, White Paper created by the former Chief of Staff of the Air Force, Gen Ronald Fogelman and the former Secretary of the Air Force, Shelia Widnall

6. See John Warden III, "The Enemy as a System," *Airpower Journal,* Spring 1995, pp. 41-55.

7. *Air Force Doctrine Document 2-5*, Information Operations, p. i.

8. *Air Force Doctrine Document 2-5*, p. i.

9. *Air Force Doctrine Document 2-5*, p. 15.

10. Andrew S. Tanenbaum, *Computer Networks, Third Edition,* (Upper Saddle River, NJ: Prentice-Hall, Inc., 1996) p. 47.

11. Tim Bass, Alfredo Freyre, David Gruber, and Glenn Watt, "E-Mail Bombs and Countermeasures: Cyber Attacks on Availability and Brand Integrity," *IEEE Network*, March/April 1998, p. 10.

12. Thomas S. Snyder, *Air Force Communications Command: 1938-1991, an Illustrated History* (Scott AFB, IL: AFCC Office of History, 1991), p. 19.

13. WWMCS History, TRW Defense and Space Systems Support group, McLean, VA, WWMCCS System Spec. WSS-78, Annex J (UNCLAS) September 30, 1977, p. 3-4. Instead, it was "more a federation of self-contained sub-systems than an integrated set of capabilities." Quoted by Kenneth Allard, *Command, Control, and the Common Defense* (New Haven: Yale University Press, 1990), p. 135.

14. See Kenneth Allard, *Command, Control, and the Common Defense* (New Haven: Yale University Press, 1990), p. 138.

15. Scott M. Britten, "Reachback Operations for Air Campaign Planning and Execution," (Maxwell AFB, AL: Occasional Paper No. 1, Center for Strategy and Technology), p. 1. The quote originally appeared in Nick Cook, "USA Plots Mission Support Revolution," *Jane's Defence Weekly*, November 19, 1994, p. 29.

16. Thomas S. Snyder, *Air Force Communications Command: 1938-1991, an Illustrated History* (Scott AFB, IL: AFCC Office of History, 1991), p. 127.

17. Timothy N. Castle, *One Day Too Long: Top Secret Site 85 and the Bombing of North Vietnam* (New York: Columbia University Press, 1999) p. 15.

18. See Kenneth Allard, *Command, Control, and the Common Defense*, p. 141.

19. Bassam Halabi, *Internet Routing Architectures* (Indianapolis, IN: Cisco Press, New Riders Publishing, 1997), p. 3.

[20] Douglas E. Comer, *Internetworking with TCP/IP Vol. 1: Principles, Protocols, and Architecture, Third Edition*, (Upper Saddle River, New Jersey: Prentice Hall, 1995), p. 37.

[21] This discussion relies on Marshall Rose's definition of the Internet, in which "The term *internet* (lowercase-I) is used when making a generic reference to a network built using internetworking technology, whilst the term *Internet* (capital-I) is used when specifically referring to this network." Marshall T. Rose, *The Simple Book: An Introduction to Management of TCP/IP based internets* (Englewood Cliffs, New Jersey: Prentice Hall, 1991), p. 2.

[22] Marshall T. Rose, *The Simple Book: An Introduction to Management of TCP/IP based internets*, (Englewood Cliffs, New Jersey: Prentice Hall, 1991), p. xx.

[23] *Air Force Communications Command*, p. 195-212.

[24] *Ibid*., p. 212.

[25] George Gilder, "The Bandwidth Tidal Wave," *Forbes ASAP*, December 5, 1994. Located on the web at: http://www.forbes.com/asap/gilder/telecosm10a.htm

[26] In effect, this represented a loan that was based on the savings projections from the use of new computers, which were sent to the communications squadrons and controlled by personnel who worked in the Network Control Centers.

[27] See *Air Force Communications Command*, p. 212. In a report to Congress in 1995, the GSA stated that the "Estimated development costs can skyrocket due to poorly defined or shifting requirements. Delays in developing and deploying a new system can erode projected benefits and delay returns on investment, and poorly designed systems can aggravate operational problems or create new ones. In the worst cases, systems development effort can suffer from a cascade of problems that lead to the termination of the effort, and a total waste of expended funding. Large "grand design" systems are particularly vulnerable to such problems because of their "all or nothing" approach. Information Technology Investment: A Government wide Overview (Letter Report, 07/31/95, GAO/AIMD-95-208). Letter from the Government Accounting Office to the Chairman, Committee on Governmental Affairs, U.S. Senate, July 1995. Found at URL: http://www.itpolicy.gsa.gov/mke/library/gaoiti.txt.

[28] Robert Lagas, *Information Technology Management Reform Act Summary* (Office of Information Resources Management, National Institute of Health), at http://irm.cit.nih.gov/itmra/itmrasum.html.

[29] *Information Technology Management Reform Act of 1995*, Public Law 104-208, SEC. 5121-5124. Full text of Act located at http://www.gsa.gov/irms/ka/mke/capplan/s1124_en.htm

[30] *Information Technology Management Reform Act of 1995*, Public Law 104-208, SEC. 5125. Full text of Act located at http://www.gsa.gov/irms/ka/mke/capplan/s1124_en.htm

[31] David Gruber, "Full Range of Communications Tools Support Forces in Harsh Locations," *Signal: AFCEA's International Journal*, November 1997, p. 39.

[32] The F-22 System Program Office levied a requirement for OC-3 (45 Mbps) links to the F-22 maintenance hanger. Currently, the data rate supporting the unclassified network requirements at ACC bases are T-1 (1.544 Mbps).

[33] The first AEF deployed from the 347th Wing at Moody AFB, Georgia, at which time the author was the 347th Communications Squadron Commander.

[34] James A. Vaughan, *366th Air Expeditionary Wing Bandwidth Utilization Study,* Engineering *Shaik Isa Air Base, Bahrain, 3 April 1998 – 3 May 1998* (Tinker AFB, OK: 38th and Installation Wing, 1998), 1.

[35] One group operates the line of business application software in the United States; another group operates the mainframe computer itself; a third group operates the base network and moves information from the mainframe computer to an external gateway on the installation; a fourth group operates the network infrastructure that takes the information from the installation and moves it through the United States to a departure point under control of operators in Europe; a fifth group in Europe manages the infrastructure that pushes the information to Southwest Asia; a sixth group operates the network equipment within Southwest Asia; a seventh group operates the information infrastructure supporting the deployed AEF base; an eighth group, and possibly others, monitors the network to ensure that adversaries are not attacking; and finally, there is the person on the computer in the remote area who is working with information on the mainframe computer.

The Occasional Papers
series was established by the
Center for Strategy and Technology
as a forum for research
on topics that reflect
long-term strategic thinking
about technology and its
implications for
U. S. national security.

Center for Strategy and Technology
Air War College

Maxwell Air Force Base
Montgomery, Al 36112