STRATEGY RESEARCH PROJECT

STRATEGIC APPROACH TO INFORMATION SYSTEMS PROTECTION

BY

LIEUTENANT COLONEL RONALD R. HEULER
United States Army

USAWC CLASS OF 1999

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

USAWC STRATEGY RESEARCH PROJECT

Strategic Approach to Information Systems Protection

by

LTC Ronald R. Heuler
United States Army

Colonel Gerald J. Wilkes
Project Advisor

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

ABSTRACT

AUTHOR: LTC Ronald R. Heuler

TITLE: Strategic Approach to Information Systems Protection

FORMAT: Strategy Research Project

DATE: 07 April 1999 PAGES: 58 CLASSIFICATION: Unclassified

The National Security Strategy (NSS) states that the national security posture is dependent on information infrastructure and its protection. Information and information systems have strategic value due to ubiquitous interconnection with national infrastructure. Because of the strategic implications, comprehensive protection of information systems is essential. Unfortunately, many Department of Defense (DoD) information systems are still being fielded without adequate consideration of this important aspect. Protection of information systems cannot be an afterthought. It must be integrated with the solution to information system requirements. This SRP examines a conceptual framework for the fielding of protected information systems for those involved in the planning, budgeting, design, implementation, operation, and support of DoD information systems.

TABLE OF CONTENTS

PREFACE

(Start text of Preface or Acknowledgements here)

LIST OF ILLUSTRATIONS

LIST OF TABLES

STRATEGIC APPROACH TO INFORMATION SYSTEMS PROTECTION

> Our military power and national economy are increasingly reliant upon critical infrastructures. Advances in information technology…have created new vulnerabilities to information attacks as these infrastructures have become increasingly automated and interlinked. If we do not implement adequate protective measures, attacks on our…information systems…might be capable of significantly harming our military power and economy.
>
> — National Security Strategy, United States of America[1]

The Strategic Value of Information

The preceding quote emphasizes the significance of our information infrastructure, systems, and technology. Joint Publication 3-13, Joint Doctrine for Information Operations, provides the Department of Defense (DoD) perspective by stating, "All forms of national power, to include military operations in particular, … depend on information and information systems,"[2] as well as stating that "[I]nformation itself is a strategic resource, vital to national security."[3] Information and information systems have strategic[4] value due to ubiquitous interconnection with national infrastructure. Any information system left inadequately protected may have implications for national security. Because of the strategic implications, protection of information systems and networks is essential. Unfortunately, many DoD information systems and networks are

still being fielded without adequate consideration of or attention to this important aspect.

Protection of information systems cannot be an after-market add-on. It must be integrated with the solution to information transport, storage, processing, and dissemination requirements. The Honorable Mr. Emmet Paige, former Assistant Secretary of Defense for Command, Control, Communications, and Intelligence (ASDC3I), has stated that, "systems security must be designed and built into our systems up front. [It] cannot be an afterthought."[5] Information protection must be a systems engineered solution that is integrated with the implementation or upgrade of the information system. Systems that are designed from inception with security in mind and which have protection integrated throughout the acquisition and fielding process result in more secure systems with longer utility and lower life-cycle costs than those in which security is an afterthought.

Integration of information protection with information systems entails a comprehensive, holistic approach to the planning, design, implementation, and life-cycle support of the system. Integrated information system protection must include consideration of risk-management, defensive concepts, product selection criteria, people and process relationships to the system, and life-cycle support issues. This paper will identify

and dispel some common misperceptions that adversely affect integration of protection with information systems. A conceptual framework for integrated systems protection for those involved in the planning, budgeting, design, implementation, operation, and support of DoD information systems will then be developed. If adopted and applied, the framework described herein will support implementation of better protected information systems with concomitant operation and maintenance and life cycle support benefits.

Information Misperceptions

Some erroneous perceptions pertaining to information must be addressed before development of a comprehensive approach to integrated information systems protection. Among the most common misperceptions is that information is a new element of power or that information is power. Another is that information processing (and protection thereof) are predominantly technology issues associated with the electronic devices that transport, process, and store data. Such misperceptions affect the ability of information system planners, designers, and implementers to apply comprehensive solutions to information protection.

Numerous sources have credited information and information technology as the source of the much publicized Revolution in Military Affairs.[6] Information cannot be solely responsible, for is not new nor is it a new element of power. The following

historic examples show that information has always been essential to the application of military power. More than 200 years before the birth of Christ, Sun Pin, the great-grandson of Sun Tzu, and general of King Wei, of the state of Ch'i, manipulated information to achieve victory over general P'ang Chuan.[7] Sun Pin made it known that the soldiers of Ch'i feared P'ang Chuan. To bolster that perception he had his soldiers light successively fewer campfires each night. P'ang Chuan, believing that Ch'i forces were deserting in mass, conducted a forced march of 100 li (30 miles) to attack Sun Pin. He fell into an ambush, his forces were annihilated, and he was killed. Another historic example of the use of information in this context occurred in 32 B.C. In this case, Octavianus, Julius Caesar's heir, employed information techniques to turn the Roman public against Marcus Antonius.[8] Octavianus obtained, or fabricated, a copy of the will of Marcus Antonius and used it to convince the Roman Forum that Antonius planned to leave Roman lands to his half-Egyptian heirs. The Forum and the Roman people were so outraged that three Roman armies were sent to destroy Antonius, his legions, his Egyptian wife (Cleopatra), and the Egyptian Army. Octavianus achieved supreme rule of the Roman Empire as a result. These examples show clearly that information is not a new phenomenon and has long been instrumental in military and political affairs.

The second misperception is a myopic technical focus on the information environment. This simplistic focus on enormously fast and efficient data transport, storage, retrieval, and processing is not conducive to a comprehensive approach to information system protection. To contravene this misperception, the information pyramid is presented as an analogy for a more comprehensive view of the information environment.

An Analogy for the Information Environment

The information environment is really a complex interrelationship of information, technology, people, and processes. The information pyramid is one analogy for this environment. The base of the pyramid is data, the next level is information, the third level is knowledge, and the apex is understanding (Fig. 1).

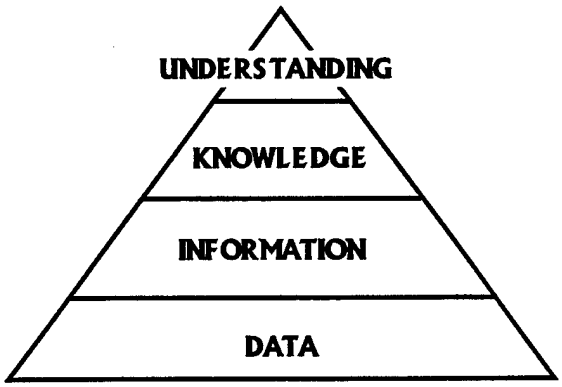

Figure 1. The Information Pyramid

A geometric comparison of the levels, and the commonly held simplistic view of the figure, point out the plethora of data

compared to the paucity of understanding. A closer look at the levels and the associated processes presents a view of the information environment more relevant to protection of information systems. From the base of the pyramid, data (available as ones or zeros in storage media) goes through a conversion process (data processing) of decoding or demodulation to take the form of information (Fig. 2).

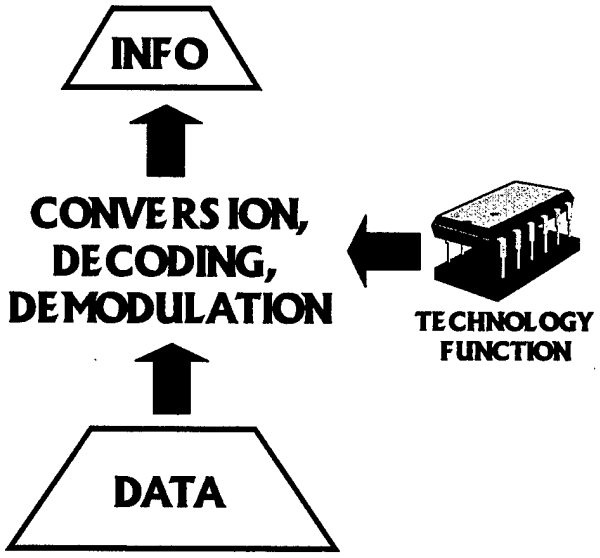

Figure 2: Data Processing

It is at this level, data technology, that advances have been most revolutionary in terms of exponential increases in processing speed, transport bandwidth, and storage capability.[9] This may explain, but does not excuse, skewed emphasis on technology-focused solutions to information protection. The next interface, conversion of information to knowledge through

human experience and perception (information processing) requires processes such as organizing, sorting, and filtering. (Fig. 3.)

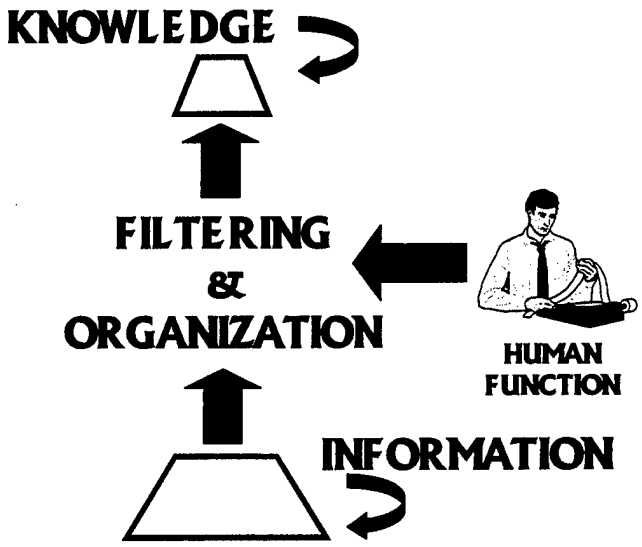

Figure 3: Information Processing

Despite advances in artificial intelligence and intelligent agent technology, human application of concepts of exclusion, belonging, and representation are required to change large amounts of textual, audio, or visual information into knowledge.[10] The next step, conversion of knowledge to an "understanding" of how to apply knowledge (or knowledge processing), requires functions that are the sole domain of the human brain including analysis, synthesis, generalization,

abstraction, extrapolation, and value judgment.[11] See Figure 4, below:

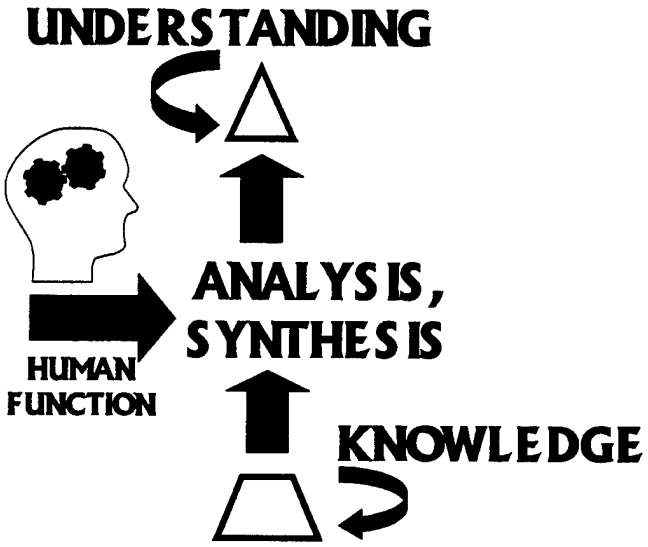

Figure 4: "Knowledge Processing"

The following example, drawn from the Battle of Tannenberg in 1914, shows the pyramidal relationships and applications in practice. The German Army intercepted numerous Russian encoded wireless transmissions (data). These were demodulated and decoded (data processing) and turned into information. Those pertaining to troop dispositions were selected and organized (information processing) thereby creating knowledge. In this case the knowledge was a clear and accurate situational awareness.[12] German commanders were able to analyze this

knowledge, synthesize courses of action, evaluate risks, and create the understanding to apply military power necessary to defeat the Russian army. German commanders attributed victory to knowing all the enemy's plans.[13] Superficially it would appear that "knowledge is power," however, "...knowledge of the enemy, alone, is not enough. We must (also) possess the means to act on what we know...",[14] and an ability to protect the process. At Tannenberg the Germans exhibited control of the information environment as well as the means to act (Fig. 5).

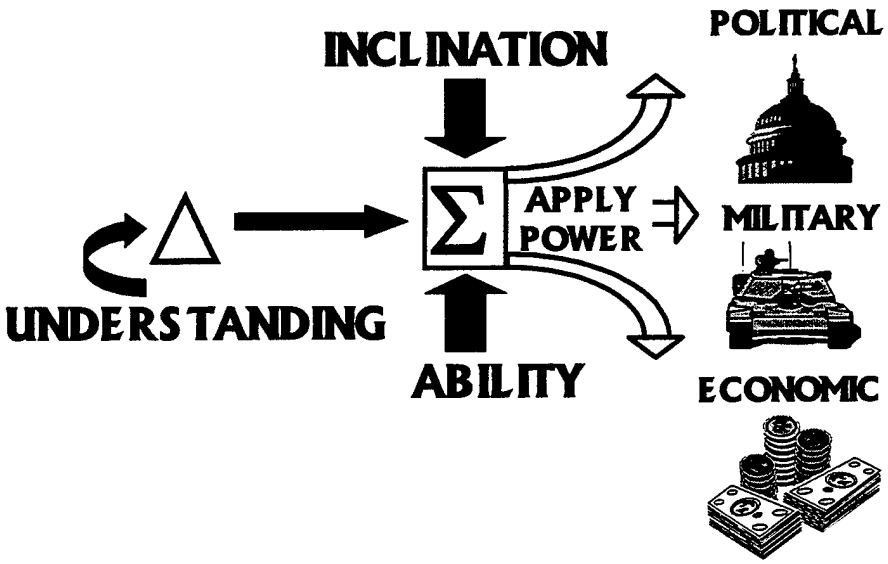

Figure 5: Application of Power through Understanding

The example clearly disabuses common misperceptions of the information environment. It shows that information systems

function due to the interaction of technology, people, and processes. Logically, integrated protection of information systems must encompass system components, human and technical processes, and interrelationships. Despite the apparent obviousness of the discussion above and the seemingly clear necessity to approach systemic problems with system encompassing solutions, sometimes misperceptions affect the viability of information protection solutions.

Misdirected Information Protection Efforts

Due to misapplied technology solutions focused at the data level of the information environment, there are cases when resources allocated to protect information networks have been ineffectively employed. The following example illustrates this phenomenon.

In 1998, the U. S. Army Signal Command and the U. S. Army Communications Electronics Command proposed, to the Director of Information Systems for Command, Control, Communications, and Computers (DISC4), a comprehensive approach for the protection of the Unclassified Internet Protocol (IP) Router Network (NIPRNET) and U.S. Army web servers. This integrated approach addressed system level planning, design, implementation, network life-cycle support issues, and associated processes and personnel issues.[15] The DISC4 staff recommended an alternative solution, based on specific hardware, that considerably de-

emphasized requirements for integrated training, maintenance, and life-cycle support. Their approach allowed major commands and individual commanders to independently acquire and implement stand-alone, product-focused solutions without consideration of pervasive system issues.[16] Results of their decision were recently apparent in Department of the Army direction to disconnect all Army web servers from the Internet due to inadequate protection of the content.[17] In addition, a current National Security Agency advisory states that one of the devices specifically selected by DISC4 staff principles exhibited "…discrepancies between the product and the requirements in the firewall protection profile."[18] A perception-reality mismatch is clearly evidenced by the disparity between the scope of the information environment and the narrow focus of the implemented solution in the preceding example. Eliminating such mismatches and ensuring proper application of resources requires a more balanced approach to information protection.

Balanced Approach to Information Protection

In keeping with a perspective that is broad in scope and nature, application of information protection cannot be a total risk-avoidance solution to insuring the viability of information as a strategic resource. A balanced protection effort entails several things, among them is an understanding of what is to be protected, what to protect against, and how to pursue a rational

approach to implementing the protection. For the foreseeable future, protection of information transport, storage and retrieval, and processing systems encompasses networks, people, and processes. Such protection is required to address numerous threats including computer network attacks from a wide variety of sources, power outages, natural phenomenon like fire and flood, poorly designed, tested, or deployed hardware or software, and intentionally or unintentionally introduced viruses. This necessitates a rational approach based on a risk management philosophy. Just because a theoretical window of vulnerability exists doesn't mean that it will be exploited or that resources should be expended to protect it. A comprehensive systems engineering approach to the planning, design, implementation, and life-cycle support of protected information transport systems necessary to shape the information environment is addressed in the following sections of this paper.

PROTECTED INFORMATION SYSTEMS - AN INTEGRATED APPROACH

The Defense Science Board (DSB) maintains that current information system vulnerabilities are largely due to a lack of attention to security and survivability during design and development.[19] DSB reports also state that there is a significant "lack of comprehensive, principled, demonstrably-effective approach(es) for architecture, design, and analysis of secure, survivable information systems."[20] Joint Publication 3-13 defines an information system as, "the entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information."[21] Integrated information protection for this entire infrastructure must therefore logically comprise comprehensive protection of all system elements. This includes far more than the simple provision of point defenses such as firewalls and intrusion detection systems. A strategic[22] concept for information protection encompasses all of the assessments, plans, policies, and procedures, hardware and software tools and techniques, testing, modeling, and simulation, administration, operations and maintenance, and life cycle support required for robust system protection. Joint Publication 3-13 also mandates that information, information systems, and information based processes will be protected relative to the value of the information they contain and the risks associated with their

compromise or loss."[23] Comprehensive information protection is therefore dependent upon the sensitivity of the information, the threat thereto, the risk if the information is affected, the type and criticality of the process relying upon the information and the relative cost to implement the protection.[24] Above all, the approach must result in an integrated solution to secure and survivable information system requirements. The important point is that, "it [security] must be built in from the beginning. Attempts to add [security] after the design or implementation is complete are usually unsuccessful and expensive."[25]

This paper divides the approach to protection of information systems into four interdependent phases or sub-processes: planning, design, implementation, and life cycle support. Although these sub-processes are arranged sequentially herein, the overall process is a highly parallel, integrated product team effort. This multidisciplinary team should consist of design engineers, security engineers, acquisition personnel, logistics planners, system users, and system operators and maintainers. The integrated process involves all of these stakeholders early in system development and keeps them involved throughout its life-cycle.

Planning Process

The planning process begins with the conduct of several interrelated assessments and analyses. They are threat

analysis, vulnerability assessment, functional requirements analysis, and technical requirements analysis. None of these can be performed in a vacuum as they all, in conjunction, make possible the risk-management approach called for by Joint Publication 3-13[26] and the Army Command and Control Protect Implementation Plan.[27]

Threat analyses and vulnerability assessments are best conducted in consonance. Threat assessments are used to determine threat levels and to implement security decisions. Threat is assessed in the categories shown in Table 1, below:[28]

Threat Category	**Definition**
Existence	Presence of a threat or the ability to gain access to the targeted system.
Capability	Attacker's expertise in the use of tools and ability to exploit system vulnerabilities.
Intent	Denoted or connoted desire of a specified enemy to conduct an attack.
History	Demonstrated activity of a specific attacker over time.
Targeting	Information indicative of preparation to attack specific targets.
Security Environment	Political and situational considerations based on the system and its operational relationships.

Table 1: Threat Categories and Descriptions

In addition to external threats, internal threats must be considered. One expert, Charise Castagnoli, of Internet

Security Services, says... "70 to 80 percent of security breaches are internal."[29]

Information systems are also vulnerable to threats from other human and environmental sources. These include data loss due to viruses, power outages, natural disaster, and human error (Fig. 5).[30]

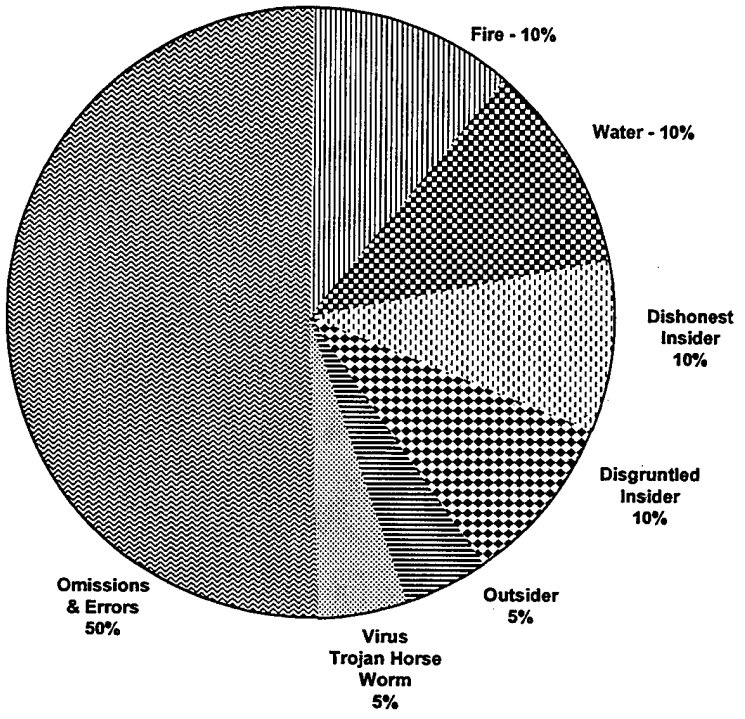

Figure 6: Sources of Threat to Information Systems

The risk management approach dictates that all of these be considered and addressed proportionately (contrary to current Network Security Implementation Plan emphasis on anti-external hacking defenses such as firewalls and intrusion detection systems).[31] A more balanced approach entails application of some

resources to policies and procedures in order to reduce vulnerability to human error, and to data redundancy and disaster recovery in order to minimize environmental threats.

Concurrently with threat and vulnerability assessments, business process and technical requirements analyses contribute to the overall design by "influencing design decisions, product selection, and cost benefit trade-off decisions."[32] Threat, vulnerability, performance, functional, and technical objectives cannot be considered singly. A balance must be struck depending on their relative importance and the degree of assessed risk.[33] This balance is essential to successful engineering and design of the system.

Engineering and Design Process

The engineering and design process, conducted in conjunction with the planning process, is also a series of trade-offs based on the concept of risk management. Design includes architectural considerations, evaluation of product selection criteria, and conduct of prototyping, modeling, and simulation to assess effects of architectural and product choices. A wide variety of system architectures, network designs, security mechanisms, and hardware and software tools must be considered in designing the system. The following sections address defensive concepts that are to be embodied in the architecture and topology of the system being designed.

Defense in Depth

Architectural considerations include defensive depth, diversity, and agility. From an architectural perspective a defense in depth strategy using currently available protection technology in a layered system of defenses can be effectively employed to insure the confidentiality, integrity, and availability of the information system under design.[34] This strategy employs multiple security mechanisms that provide a range of protection across the breadth and depth of the information system.[35] Figure 6 depicts the defense in depth concept and identifies layers of protection and some of the protective measures employed at each layer or boundary.[36]

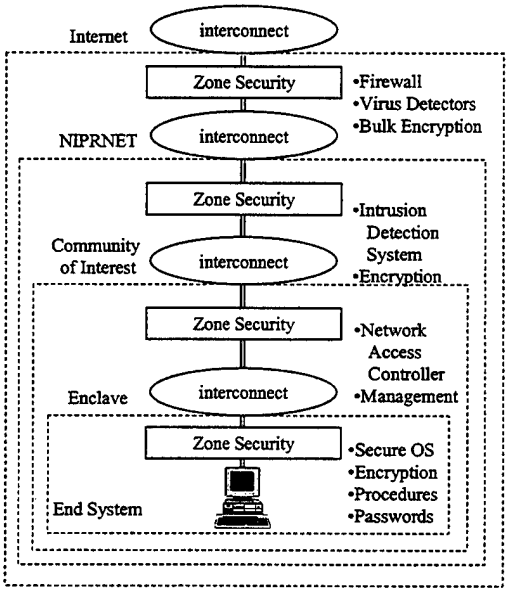

Figure 7: Defensive Layers and Measures

Defensive Diversity

The idea behind diversity of defense is that a variety of security systems or products reduces chances that a common error can compromise the entire network. It also reduces the probability that an attacker can learn enough by defeating one product to invade the entire system.[37] There is clearly a trade-off to be considered regarding diversity. Multiple security devices and products have second and third order effects in the realms of operations and maintenance, training, and integrated logistic support that may negate the security benefits derived therefrom. The risk-management approach addresses these issues during the system design process. The design of resilient information infrastructure must, however, encompass diversity of hardware and software so that common failure modes cannot result in system wide failure.[38]

Defensive Agility

Sun Tzu said, "...experts in defense conceal themselves under the nine-fold earth, thus they are capable of protecting themselves."[39] Tu Yu, a philosopher of the early 9th century elaborates, "[T]hose expert at preparing defenses consider it fundamental to rely on the strength of obstacles... [T]hey make it impossible for the enemy to know where to attack. They secretly conceal themselves as under the nine-layered ground."[40] This philosophy is embodied in the design principle of defensive

agility or adaptability. Successful information protection tends to be adaptive. Much like a neural network, the defensive topology can be engineered to dynamically change (logically) as it adapts to recognize attack scenarios.[41] In this way the protected information system is designed to prevent disclosure of "learned" paths through its defenses. Repeat attacks following previously discovered patterns are frustrated by defensive measures that have mutated to combat those attacks.

Product Selection Criteria

Product selection and selection criteria are essential to the design process. Use of appropriate selection criteria during the design process contributes to the success of implementation and life-cycle support processes. Among other things, products should be chosen to facilitate standards-based interoperability, ease of integration and operation, simplicity of management, implementation of upgrades, and supportability. Criteria for selection of security products that comprise the layered, diverse, and agile defense should address the parameters shown in Table 2, below:[42]

Essential Product Selection Criteria
a. Real-time detection, reporting, and reacting capability.
b. Ease of, and ability to, update security configurations.
c. Support for existing network operating systems and standards.
d. Non-obtrusive ease of management.
e. Compatibility with existing and planned management applications.
f. Capability of self-protection.
g. Interoperability with local, regional, and national systems.

Table 2: Essential Product Selection Criteria

In order to characterize vulnerability of products for use in protected information systems, the DSB has recommended that DoD develop a commercial-off-the-shelf information (COTS) systems technology evaluation capability.[43] The U.S. Army Communications-Electronics Command (USACECOM) Technology Integration Center (TIC) is such a capability and has been used to support some Army information system programs including the Common User Installation Transport Network (CUITN). The TIC also supports prototyping, modeling, and simulation activities described below.

Prototyping, Modeling, and Simulation

Prototyping, modeling, and simulation contribute to the analysis of security features of architectures, topology, and components and to evaluation of standards based compatibility and interoperability. A key element of the engineering and design process is the creation of system level prototypes or test-beds and the exercise of models and simulators to emulate the operation of protected information systems. The DSB has recommended development of modeling and simulation environments for evaluation of security features of network architectures, topologies, and components, and for analysis of standards based compatibility and interoperability.[44] This capability enables the engineer or acquisition manager to evaluate the ramifications and risk management based effects of architectural and design choices before major implementation investments are made. The USACECOM TIC has provided this capability in the fielding of several protected information systems. In addition to supporting the engineering and design process, the TIC has been employed to evaluate new security products and upgrades to existing products, reducing the risk associated with integrating upgrades into in-place systems and facilitating life-cycle support thereof.

Engineering and design of information infrastructure capable of enduring in the face of intentional, unintentional,

or environmental disruptions or attacks is an integral part of the multi-disciplinary integrated process. Functional and technical solutions developed in the planning process result in a description of a system to be acquired and implemented.

Acquisition Approach

The approach chosen to acquire the planned and designed system directly affects the implementation and life-cycle support processes. Many information protection issues affected by the acquisition approach are not directly addressed herein. However, it is important to remember that the acquisition approach, like the overall protection effort, is focused on the total system solution. One of the multi-functional team members (usually either the Program Management Office or the industry partner) must act as the overall system integrator.

Choice of an industry partner and solution provider is also a key issue. Companies that have system integration experience are typically better choices than are product vendors who may tend to focus on component or device level solutions at the expense of the process of integrating the security solution with the information system.[45] Other important acquisition related issues will be discussed in the following sections on implementation and life-cycle support.

Implementation Process

Implementing the protected information system comprises far more than constructing a network based on product selection and choice of architecture or topology. Implementation issues can be subdivided into two categories, technical and human. Technical information protection issues include the characterization and configuration of security products and system security validation and verification. Human issues include development of policies and procedures, security management, training, and security awareness. Technical issues, human issues, and their interrelationships are addressed in the following sections.

Technical Issues

Characterization of Security Products

Due to the complexity of information networks and the wide variety of technical and functional requirements, security devices are not plug and play components.[46] Characterization and pre-configuration of security products are actually part of test bed activities conducted in the design phase. Network characterization hardware and software is used to collect data from traffic analysis on existing networks. Results are used to evaluate and configure security devices as part of the system design. During implementation, pre-configured security products are integrated with the information system components thereby

eliminating complex, after-the-fact configuration efforts and interruption of key user services.

Security Validation and Verification (V&V)

Extensive technical testing ensures that system components are properly integrated and that system technical and performance requirements are met. Likewise, operational test of the system is necessary to ascertain that the customer's functional and business processes are accommodated. However, from the information protection standpoint, the key testing is focused on the human-technical interactions. This includes V&V of the security features and the proper functioning of security procedures. The process of V&V links technical and human processes and assures both customer and fielder that the fundamental security objectives (accountability, availability, confidentiality, assurance, and security management) have been met.[47] Development of information system V&V procedures should begin in conjunction with the engineering and design process. Engineering and design activities at the test bed, modeling, and simulation facility are conducive to development and refining of validation and verification procedures. V&V can be used as a venue for training system users, operators, and administrators on security procedures.

Human Issues

"A realistic security approach is more than the assembly of technical components, at the strategic level, security is still a [human] management function, not a technical issue."[48] The people who operate and maintain the information system and those who use it to collect, process, store, or disseminate information are a critical (and vulnerable) component of the information system.[49] Implementation of effective information system security must focus heavily on the human dynamic. Some key implementation issues are development of security policies and procedures, security management, system user and administrator training, and overall security awareness.

Policies and Procedures

Development of the security policies and procedures actually begins in parallel with the early stages of engineering and design. These documents flow directly from the planning process and the risk management based trade-offs among threats and vulnerabilities and functional and technical requirements. Content is dependent to some degree on the choice of the topology and individual components as well as supported business processes and the operation and maintenance concepts to be employed. During the system implementation, the policies and procedures are refined to reflect the actual system operation and use. Security policies (essentially the do's and don'ts for

the protected information system) are largely derived from the business process, threat environment, and vulnerability analyses described earlier. Policies must match reality; thus they should be crafted to reflect the trade-offs and decisions made in the planning process.[50] The procedures, the actual how to's for the protection measures afforded the information system, are primarily dependent upon the network topology and network components that satisfy system technical and functional requirements. Security procedures should be simple, otherwise users will attempt to circumvent or disable them.[51] A basic security features users guide of a few pages is sufficient to address security procedures and elementary security awareness issues.[52] V&V should be part of operational testing of system functional requirements addressed previously.

Security Management

Effective management of protected information systems relies on a balance between the use of automated security applications and a focus on the human dynamic. Security managers want security products and applications that are seamlessly integrated into existing management systems and platforms.[53] Integral security products such as network profilers, key generators, directory managers, and monitoring and auditing programs are among the tools available to assist the security manager in the conduct of his or her job. While

the security manager is essential to setting, maintaining, and implementing security policies and procedures, management of the human aspect of the protection often exceeds his or her purview. The structures and environment that surround the technical solution, and which are vital to the protection of the system require management to be involved at all organizational levels.

Managerial processes are required to contribute to the overall security environment throughout the organization. Managers at all levels have to empower employees, involve them in the information protection process, make security user-friendly, and maintain privacy for employees, yet still be focused on managing risk and minimizing potential damage. The integrated approach to system wide information protection requires managers to be aware of their significant responsibilities as part of the implementation process. "The manager who maintains a satisfied, well motivated work force does as much for security as the technician who installs the system."[54] This effort is considerably easier if managers are part of the initial planning process described earlier.

Training

The DSB has postulated that information system vulnerability is usually the result of human error, insufficient training, and lack of knowledge.[55] Training of information system users, operators, managers, and maintainers is clearly a key

aspect of the integrated approach to information protection. Training, in the context of protected information systems, is unique due to the number of people involved and the diverse focus of the training effort. The amount and type of training depends upon the degree to which, and level at which, the "trainee" interacts with the system. Procedural training is required for system users. Product and system training enables operators to ensure system availability. Security managers require detailed and comprehensive training on security administration and management procedures, including reactive procedures for contingencies. Personnel performing security management functions must be trained to detect, differentiate among, warn of, respond to, and recover from disruptions.[56] Training for maintenance personnel must be focused on product and system level troubleshooting and repair. Managers at all levels need security awareness training to help them create an environment conducive to information protection. The holistic approach that has been described so far requires that training be acquired as part of the integrated information system solution. Lessons learned from test-bed activities described previously are valuable to the development of training programs and material; security engineers who conducted those activities and developed security solutions must also play a key part in the training process.

Security Awareness

Implementing a protected information system requires the people involved in the processes to change established ways of doing business. Security awareness is one effective way to enable people to adapt to these changes.[57] A basic security awareness program addresses familiarization with the threat, security responsibilities, and physical security measures. The security features user guide previously mentioned is an effective basis for a security awareness program. Update mechanisms must be built into the program to reflect changes in the threat environment and to account for personnel turn over. System personnel at all levels must be aware that the greatest threat to information systems is human error or carelessness and that insiders commit the vast majority of computer crime.[58] These are areas in which awareness can have a significant effect on reducing risk. Likewise, responsible system use reduces risk of system corruption or loss or damage to data. Simple precautions, such as scanning disks for viruses, downloading only from trusted sites, and scanning downloaded files prior to use can avoid costly virus elimination procedures. Physical security measures are also critical to overall system security. Locking access ways to areas where system components or media are stored is an essential technique that enhances the protection of the information system. Above all, security

awareness must emphasize that information system protection is primarily dependent on people, not technology.[59]

Life-Cycle Support

The acquisition strategy must integrate logistics (software and firmware updates and upgrades, technical support, warranty, and training programs) with purchase of the hardware and installation and integration effort.[60] Just like the protection itself, the system support must be integrated with the solution, not an afterthought. As most, if not all, of the components of the information system will be COTS or non-developmental items (NDI), time lines and costs associated with support processes will probably prohibit establishment of organic support. As the technological life of hardware and software shrinks, vendor provided or private sector logistic support is a viable substitute for organic DoD capabilities.[61]

Life-cycle support of protected information systems presents a unique challenge, even if it is well integrated in the process. Not only does the information system or network need to be maintained in a status that allows continued service, but also protection features require continual update to reflect the rapidly changing nature of the threat. Life-cycle support for protected information systems is also unique in that it requires not only spares and repair parts but also entails

extensive software support, on-going threat and vulnerability assessments, configuration management of the system and security policies and procedures, and sustainment training for user, operator, administrator, and maintenance personnel.

Post-Deployment Software Support (PDSS)

PDSS is a challenge in any information system due to the frequency of software updates and upgrades and the necessity to insure concurrency and compatibility of software versions. In a protected information system this complexity is compounded by the importance of maintaining the protected aspect of the system and concomitantly those systems to which it is connected. Planning and design of security devices to allow centralized, server-based distribution of version updates contributes to conformity of software versions throughout the system. System procedures should also allow for a test bed based verification of compatibility and standards based interoperability among software versions prior to implementation on the operational system. Lessons learned from the actual operation of the system can also be used to facilitate the development of updated security products that are timely and reflective of the changing nature of the threat and changes in system related business processes.

On-going Assessments

Red teaming (use of friendly personnel to conduct hostile attacks to assess system vulnerability) is an essential component of the information protection approach. Because the system and the environment in which it operates are constantly changing, such penetration testing is a continual process.[62] Red team efforts must be directed at application, system, and sub-system levels to ensure robustness of the defensive design discussed previously. These efforts must also focus on the human dynamic of the information system since most security problems result from human error.[63]

Configuration Management

At the time of delivery a hardware and software (component level) configuration baseline must be established. Physical and logical network mapping is also an important part of configuration management. Component configurations and network maps should be accurately updated when changes occur to the registered baseline. This registry information is invaluable in protecting assets, identifying tampering, and in recovering from a variety of attacks or other disaster based contingencies.[64] Software programs, usually part of network or security management applications, are available for recording changes to system hardware and software configurations. Configuration management also enables system hardware and software inventory

allowing network administrators to manage software licenses, support upgrade planning, and control software versions, which contributes to the overall protection of the system. Careful management of changes to security policies and procedures are required to ensure continued viability and applicability.

Sustainment Training

"Business leaders view employee education as the most important element of any security program."[65] For a protected information system, training is not a one-time effort. The changing nature of the environment and the turnover in personnel associated with many DoD systems makes user, operator, and administrator training a continual process. Sustainment training mechanisms include computer based training, periodic security awareness "in-service" seminars, and formal training classes offered by system integrators as part of the system solution.

A fully integrated and interoperable approach to protected information systems does not end with development and fielding. It extends through out the life-cycle and incorporates the concepts addressed herein.

Conclusions

Dr. John J. Hamre, the Deputy Secretary of Defense, describes information protection efforts for most information systems as largely "ad-hoc". While the information environment

has experienced an explosion in pervasiveness and technical complexity, Hamre charges that, "what has not kept pace is a disciplined, systematic approach to security."[66] This paper presents a conceptual framework for such a systematic approach. It addresses some of the interrelations among the various sub-processes that make up the integrated process for providing protection to information systems.

Adoption of a comprehensive approach, such as has been described, provides a number of benefits including, but not limited to, the following:

a. Facilitates risk-management-based determination of cost versus effectiveness allowing resources to be applied to the highest priority requirements.

b. Enables comprehensive and coordinated threat analysis, vulnerability assessment, user functional requirements determination, and technical specification review.

c. Increases industry involvement (compared to the individual purchase of stand alone hardware solutions) giving commercial system integrators a larger stake in the process and giving DoD greater access to state-of-the-art technology.

d. Capitalizes on a design effort that integrates modeling and simulation, test bed evaluation of competing commercial products, evaluation of standards based interoperability, and

characterization and configuration of security hardware and software products.

e. Incorporates development of plans, policies, procedures and guidelines that address risks associated with intentional and unintentional human actions.

f. Addresses user, operator, administrator, and maintainer training and security awareness as part of the protected information system implementation.

g. Integrates appropriate PDSS and other life-cycle support considerations with the acquisition, reducing overall life-cycle cost and extending system life time through the selection of scaleable products with software based migration paths.

Successful implementation of protection for information systems requires a multi-disciplinary team capable of formulating a comprehensive set of requirements, knowledgeable of current and emerging technologies, capable of influencing design of information systems from a protection perspective, capable of managing implementation of protection in information system, and dedicated to maintaining the protection of the information system throughout the life-cycle. Similarly, successful implementation of information protection relies on the multi-disciplinary thinking process postulated in this paper. Until the perspectives of those involved in the

planning, budgeting, design, implementation, operation, and support of DoD information systems is expanded to encompass system wide solutions based on balanced risk-management approaches, success will continue to be ethereal. While hope supposedly springs eternally, B. H. Liddel-Hart opines that, "The only thing harder than getting a new idea into the military mind is getting an old one out."[67]

WORD COUNT = 5,819

ENDNOTES

[1] The White House, A National Security Strategy for a New Century (Washington, D.C.:Government Printing Office, 1998), 20.

[2] Joint Chiefs of Staff, Joint Publication 3-13, Joint Doctrine for Information Operations (Washington, D.C.: U.S. Joint Chiefs of Staff, 9 October 1998), I-18.

[3] Ibid.

[4] Strategic defined in this case as, "necessary to or of great value or importance to" national security. See: Webster's Third New International Dictionary (Springfield, MA: G&C Merriam Co.,1965), 2256.

[5] The Honorable Emmet Paige <PaigeE@aoa.com>, "Speaking at ADRP on 24 May," electronic mail message to Todd Kersh <KershT@aoa.com>, 15 May 1998.

[6] Ryan Henry and C. Edward Peartree, "Military Theory and Information Warfare," Parameters Volume 28, Number 3 (Autumn 1998), 121.

[7] Sun Pin, Military Methods, trans. Ralph D. Sawyer (Boulder, CO: Westview Press, 1995), 53.

[8] Barry Porter, "Actium, Rome's Fate in the Balance," Military History (August, 1997), 29.

[9] Michael Wilson, "Hardwar, Softwar, and Wetwar: Operational Objectives of Information Warfare," copyright 1995, <http://www.7pillars.com/papers/Hardwar.html>; Internet; accessed 3 September 1998.

[10] Ibid.

[11] Ibid.

[12] Richard N. Armstrong, "Tactical Triumph at Tannenberg," Military History (August, 1997), 61.

[13] Ibid., 80.

[14] U.S. Army War College Selected Readings, Course 4, Implementing National Military Strategy, Volume III, "Cycles of War," Major General Robert H. Scales, Jr. (Carlisle Barracks, PA: United States Army War College, 19 November 1998), 23-4.

[15] Headquarters, U.S. Army Signal Command, C2 Protect Campaign Plan, Information Briefing presented to Director of Information Systems for Command, Control, Communications, and Computers (DISC4), 16 March 1998.

[16] Headquarters, Department of the Army, Improving the Army's Information Systems Security, Electronic Message, HQDA-SAIS, 161700Z April 1998.

[17] Headquarters, Department of the Army, Guidance for Publicly Accessible Army Web Sites, Electronic Message, HQDA-SAIS-ZA, 251700Z September 1998.

[18] Secretary of Defense, Firewall Security, Electronic Message, ASDC3I, 161217Z December 1998.

[19] Defense Science Board, Report of the Defense Science Board Task Force on Information Warfare - Defense, "Appendix F, Technology Issues," (Washington D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, November 1966), 2.

[20] Ibid., 3.

[21] Joint Publication 3-13, Joint Doctrine for Information Operations, I-11.

[22] Strategic used in the context of an undertaking that is broad in scope and nature, exhibits complexity, requires synchronization of multiple and diverse components, and requires balancing of priorities and resources. See: William T. Johnson, The Principles of War in the 21st Century: Strategic Considerations, (Carlisle Barracks, PA: Strategic Studies Institute, 1 August 1995), 14-18.

[23] Joint Publication 3-13, Joint Doctrine for Information Operations, I-5.

[24] Product Manager, Defense Data Network, Carlisle Briefing for LTG Campbell, (Information Briefing presented to DISC4, 18 June 1998), Slide-4.

[25] Cyril H. P. Brooks, Information Systems Design (Sydney, Australia: Prentice-Hall of Australia, 1982), 94.

[26] Joint Publication 3-13, Joint Doctrine for Information Operations, I-5.

[27] Headquarters, Department of the Army, Keeping the Highway Open and Secure for Force XXI, Volume III, "The Army Command and Control (C2) Protect Implementation Plan (IP)", (Office of the DISC4, undated), 6.

[28] Defense Science Board, Report of the Defense Science Board Task Force on Information Warfare - Defense, "Appendix C, A Taxonomy for Information Warfare?," (Washington D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, November 1966), 14.

[29] Peter H. Lewis, "Greatest Threats to Computer Networks Come from Within," Minneapolis Star Tribune, 15 March 1998, sec. D, p. 7.

[30] M.E. Kabay, Info War: News form the Front, (Information Briefing presented at Carlisle Barracks, 15 March 1999),Slide-8.

[31] U.S. Army War College Selected Readings, Course 4, Implementing National Military Strategy, Volume III, "Information Assurance - The Achilles' Heel of Joint Vision 2010?", Commander Sam Cox, (Carlisle Barracks, PA: United States Army War College, 19 November 1998), 23-14.

[32] Brookes, 92.

[33] Joint Publication 3-13, Joint Doctrine for Information Operations, I-9.

[34] U.S. Army Information Systems Engineering Command (USAISEC), System Security Requirements Specifications for the Carlisle Barracks Network, Version 4 (Fort Huachuca, AZ: Commander USAISEC, August 1998), A-1.

[35] Dan Galik, "Defense in Depth: Security for Network-Centric Warfare," April 1998, <http://www.chips.navy.mil/chips/archives/98_apr/Galik.htm>; Internet; accessed 12 January 1999.

[36] Ibid.

[37] Strategy Research Corp., "Security Strategies," undated, <http://night.i-land.net/~chang/src/strategies.html>; Internet; accessed 17 January 1999.

[38] Defense Science Board, Report of the Defense Science Board Task Force on Information Warfare - Defense, "Appendix E, Think Pieces," (Washington D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, November 1966), 2.

[39] Sun Tzu, The Art of War, trans. Samuel B. Griffith (Oxford, England: Oxford University Press, 1963), 85.

[40] Ibid., 86.

[41] Ecole Polytechnique Federal de Lausanne, "Neural Networks Structure Adaptation," undated, <http://lslwww.epfl.ch/~aperez/FAST/slide02.html>; Internet: accessed 18 January 1999.

[42] U.S. Army Information Systems Engineering Command (USAISEC), Security Design Description for the Carlisle Barracks Network, Version 1 (Fort Huachuca, AZ: Commander USAISEC, May 1998), 9-10.

[43] Defense Science Board Report, Appendix F, Technology Issues, 4.

[44] Ibid., 8.

[45] Stuart Mclure and Joel Scambray, "Looking back at 1998 Sheds Light on Security Gains and Areas to Fix in the Next Decade," InfoWorld (Framingham, MA: December 28, 1998), 51.

[46] Mark Barber and Gib Winter, "Firewalls: Take as Directed," January 1997, <http://www.chips.navy.mil/chips/archives/jan_97/file7.htm>; Internet; accessed 4 February 1999.

[47] System Security Requirements Specifications for the Carlisle Barracks Network, Version 4, A-4.

[48] Arie Segev, etal., "Internet Security and the Case of Bank of America," Communications of the Association for Computing Machinery (New York: October 1998), 86.

[49] Defense Science Board Report, Appendix C, A Taxonomy for Information Warfare?, 7.

[50] Frederick M. Avolio, "Firewalls are not Enough," undated, <http://www.tis.com/prodserv/gauntlet/FirewallsNotEnough.html>; Internet; accessed 1 January 1999.

[51] James A. Lingerfelt, "Strategies for Countering Threats to Information Technology Assets," November 1998, <http://www.usia.gov/journals/itps/1198/ijpe/>; Internet; accessed 2 January 1999.

[52] U.S. Army Information Systems Engineering Command (USAISEC), Security Features User's Guide, Version 2 (Fort Huachuca, AZ: Commander USAISEC, September 1998), 2.

[53] Fred V. Reed, "Automated Secutity Products Become Key Network Tools," Signal (Arlington, VA: August 1998), 31.

[54] Richard H. Baker, Computer Security Handbook (Blue Ridge Summit, PA: TAB Professional Books and References, 1991), 4.

[55] Defense Science Board Report, Appendix F, Technology Issues, 8.

[56] Defense Science Board Report, Appendix E, Think Pieces, 3.

[57] Baker, 51.

[58] Ibid., 5.

[59] Morrie Gasser, Building a Secure Computer System (New York: Van Nostrand Reinhold Co., 1988), 14-15.

[60] Headquarters, Department of the Army, (Draft) Army Regulation 700-127, "Chapter 3, Section I, ILS Management," undated, <http://www.acala1.ria.army.mil/ACALA/AP/ar700-127/Ch3sec1.htm>; Internet; accessed 15 January 1999.

[61] Brigadier General Richard A. Black, "Lessons From Acquisition Reform: Innovation, Integration, and Education," Logistics Spectrum (Washington, D.C.: January-February 1998), 8.

[62] Deborah Radcliff, "The Physical Security Danger Within," InfoWorld (Framingham, MA: 20 April 1998), 98.

[63] Ibid.

[64] Dale Long, Computer System Security, Part 2, January 1997, <http://www.chips.navy.mil/chips/archives/97_jan/file6.htm>; Internet; accessed 4 February 1999.

[65] Radcliff, 98.

[66] Robert K. Ackerman, "Government-Industry Gridlock Hampers Information Security," Signal (Falls Church, VA: May 1998), 30.

[67] Admiral Arthur K. Cebrowski, "Network-Centric Warfare: Its Origin and Future," United States Naval Institute - Proceedings (Annapolis, MD: Volume 124, Issue 1, January 1998), 35.

BIBLIOGRAPHY

Ackerman, Robert K. "Government-Industry Gridlock Hampers Information Security." Signal, May 1998, 25-30.

Armstrong, Richard N. "Tactical Triumph at Tannenberg." Military History, August 1997, 58-64, 80.

Avolio, Frederick M. "Firewalls are not Enough." Undated. <http://www.tis.com/prodserv/gauntlet/FirewallsNotEnough.html>. Internet. Accessed 1 January 1999.

Baker, Richard H. Computer Security Handbook. Blue Ridge Summit, PA: TAB Professional Books and References, 1991.

Barber, Mark, and Gib Winter. "Firewalls: Take as Directed." January 1997. <http://www.chips.navy.mil/chips/archives/jan_97/file7.htm>. Internet. Accessed 4 February 1999.

Black, Richard A. "Lessons From Acquisition Reform: Innovation, Integration, and Education." Logistics Spectrum (January-February 1998): 7-9.

Brooks, Cyril H. P. Information Systems Design. Sydney, Australia: Prentice-Hall of Australia, 1982.

Cebrowski, Arthur K. "Network-Centric Warfare: Its Origin and Future." United States Naval Institute - Proceedings (Volume 124, Issue 1, January 1998): 28-35.

Cox, Sam. "Information Assurance - The Achilles' Heel of Joint Vision 2010?." U.S. Army War College Selected Readings. Course 4, Implementing National Military Strategy, Volume III. 19 November 1998, 23-7 to 23-15.

Ecole Polytechnique Federal de Lausanne. "Neural Networks Structure Adaptation." Undated. <http://lslwww.epfl.ch/~aperez/FAST/slide02.html>. Internet. Accessed 18 January 1999.

Galik, Dan. "Defense in Depth: Security for Network-Centric Warfare." April 1998. <http://www.chips.navy.mil/chips/archives/98_apr/Galik.htm>. Internet. Accessed 12 January 1999.

Gasser, Morrie. Building a Secure Computer System. New York: Van Nostrand Reinhold Co., 1988.

Henry, Ryan, and C. Edward Peartree. "Military Theory and Information Warfare." Parameters Volume 28, Number 3 (Autumn 1998): 121-135.

Johnson, William T. The Principles of War in the 21st Century: Strategic Considerations. Carlisle Barracks, PA: Strategic Studies Institute, 1 August 1995.

Kabay, M. E. Info War: News From the Front. Information Briefing, presented at Carlisle Barracks, PA, 15 March 1999.

Lewis, Peter H. "Greatest Threats to Computer Networks Come from Within." Minneapolis (MN) Star Tribune, 15 March 1998, sec. D, p. 7.

Lingerfelt, James A. "Strategies for Countering Threats to Information Technology Assets." November 1998. <http://www.usia.gov/journals/itps/1198/ijpe/>. Internet. Accessed 2 January 1999.

Long, Dale. "Computer System Security, Part 2." January 1997. <http://www.chips.navy.mil/chips/archive/97_jan/file6.htm>. Internet. Accessed 4 February 1999.

Mclure, Stuart, and Joel Scambray. "Looking back at 1998 Sheds Light on Security Gains and Areas to Fix in the Next Decade." InfoWorld (28 December 1998): 51-52.

Paige, Emmet <PaigeE@aoa.com>. "Speaking at ADRP on 24 May." Electronic mail message to Todd Kersh <KershT@aoa.com>. 15 May 1998.

Pin, Sun. Military Methods. Translated by Ralph D. Sawyer. Boulder, CO: Westview Press, 1995.

Porter, Barry. "Actium, Rome's Fate in the Balance." Military History, August 1997, 26-33.

Product Manager, Defense Data Network. Carlisle Briefing for LTG Campbell. Information Briefing, presented to DISC4, Washington, D.C., 18 June 1998.

Radcliff, Deborah. "The Physical Security Danger Within." InfoWorld (20 April 1998): 95-98.

Reed, Fred V. "Automated Secutity Products Become Key Network Tools." Signal, August 1998, 30-32.

Scales, Robert H. Jr. "Cycles of War. "U.S. Army War College Selected Readings. Course 4, Implementing National Military Strategy, Volume III. Carlisle Barracks, PA: United States Army War College, 19 November 1998, 23-1 to 23-6.

Segev, Arie. "Internet Security and the Case of Bank of America." Communications of the Association for Computing Machinery, October 1998, 81-87.

Strategy Research Corp. "Security Strategies." Undated. <http://night.i-land.net/~chang/src/strategies.html>. Internet. Accessed 17 January 1999.

Tzu, Sun. The Art of War. Translated by Samuel B. Griffith. Oxford, England: Oxford University Press, 1963.

U.S. Army Information Systems Engineering Command (USAISEC). Security Design Description for the Carlisle Barracks Network, Version 1. Fort Huachuca, AZ: USAISEC, May 1998.

U.S. Army Information Systems Engineering Command (USAISEC). Security Features User's Guide, Version 2. Fort Huachuca, AZ: USAISEC, September 1998.

U.S. Army Information Systems Engineering Command (USAISEC). System Security Requirements Specifications for the Carlisle Barracks Network, Version 4. Fort Huachuca, AZ: USAISEC, August 1998.

U.S. Army Signal Command. C2 Protect Campaign Plan. Information Briefing, presented to Director of Information Systems for Command, Control, Communications, and Computers (DISC4), 16 March 1998.

U.S. Defense Science Board. Report of the Defense Science Board Task Force on Information Warfare - Defense, With Appendix A through F. Washington D.C.: Office of the Under Secretary of Defense for Acquisition and Technology, November 1966.

U.S. Department of the Army. (Draft) Army Regulation 700-127. "Chapter 3, Section I, ILS Management." Undated. <http://www.acala1.ria.army.mil/ACALA/AP/ar700-127/Ch3sec1.htm>. Internet. Accessed 15 January 1999.

U.S. Department of the Army. Guidance for Publicly Accessible Army Web Sites. Electronic Message, HQDA-SAIS-ZA, 251700Z September 1998.

U.S. Department of the Army. Improving the Army's Information Systems Security. Electronic Message, HQDA-SAIS, 161700Z April 1998.

U.S. Department of the Army. Keeping the Highway Open and Secure for Force XXI, Volume III. "The Army Command and Control (C2) Protect Implementation Plan (IP)." Office of the DISC4, undated.

U.S. Joint Chiefs of Staff. Joint Publication 3-13, Joint Doctrine for Information Operations. Washington, D.C.: U.S. Joint Chiefs of Staff, 9 October 1998.

U.S. Secretary of Defense. Firewall Security. Electronic Message, ASDC3I, 161217Z December 1998.

Webster's Third New International Dictionary. Springfield, MA: G&C Merriam Co., 1965.

White House, The. A National Security Strategy for a New Century. Washington, D.C.: Government Printing Office, 1998.

Wilson, Michael. "Hardwar, Softwar, and Wetwar: Operational Objectives of Information Warfare." Copyright 1995. <http://www.7pillars.com/papers/Hardwar.html>. Internet. Accessed 3 September 1998.