Planning Considerations for *Defensive Information Warfare*
-Information Assurance-

Task Order 90-SAIC-019

Prepared for Defense Information Systems Agency (DISA)
Joint Interoperability and Engineering Organization (JIEO)
Center for Information Systems Security (CISS)

Contract No. DCA 100-90-C-0058

December 16, 1993

Form SF298 Citation Data

Report Date *("DD MON YYYY")* 16121993	**Report Type** N/A	**Dates Covered (from... to)** *("DD MON YYYY")*

Title and Subtitle Planning Considerations for Defensive Information Warfare -Information Assurance-	**Contract or Grant Number**
	Program Element Number
Authors	**Project Number**
	Task Number
	Work Unit Number
Performing Organization Name(s) and Address(es) DISA	**Performing Organization Number(s)**
Sponsoring/Monitoring Agency Name(s) and Address(es)	**Monitoring Agency Acronym**
	Monitoring Agency Report Number(s)
Distribution/Availability Statement Approved for public release, distribution unlimited	
Supplementary Notes	
Abstract	
Subject Terms "IATAC COLLECTION"	
Document Classification unclassified	**Classification of SF298** unclassified
Classification of Abstract unclassified	**Limitation of Abstract** unlimited
Number of Pages 69	

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 074-0188

1. AGENCY USE ONLY (Leave blank)	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	12/1/92	Briefing

4. TITLE AND SUBTITLE
Planning Considerations for Defensive Information Warfare

5. FUNDING NUMBERS

6. AUTHOR(S)
DISA, JIEO, CISS

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

IATAC
Information Assurance Technology Analysis
Center
3190 Fairview Park Drive
Falls Church VA 22042

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center
DTIC-IA
8725 John J. Kingman Rd, Suite 944
Ft. Belvoir, VA 22060

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION / AVAILABILITY STATEMENT

12b. DISTRIBUTION CODE
A

13. ABSTRACT ***(Maximum 200 Words)***

The US military depends on information as a key part of its competitive advantage. Operation Desert Storm was an object lesson in the critical importance of information in warfare, in that it demonstrated the DOD'S ability to obtain and use information effectively while preventing Iraq from obtaining and using comparable information. This object lesson was observed and understood by other nations and organizations, but they also observed that the US did not protect
against disruption of the massive information infrastructure it mobilized for the Gulf var. If the US military is to maintain a competitive advantage in future conflicts, then the Defense Information Infrastructure (DII) upon which the US military depends must be protected commensurate with its criticality.

14. SUBJECT TERMS
Information assurance, information warfare

15. NUMBER OF PAGES

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	UNCLASSIFIED	UNCLASSIFIED	None

EXECUTIVE SUMMARY

The US military depends on information as a key part of its competitive advantage. Operation Desert Storm was an object lesson in the critical importance of information in warfare, in that it demonstrated the DoD's ability to obtain and use information effectively while preventing Iraq from obtaining and using comparable information. This object lesson was observed and understood by other nations and organizations, but they also observed that the US did not protect against disruption of the massive information infrastructure it mobilized for the Gulf War. If the US military is to maintain a competitive advantage in future conflicts, then the Defense Information Infrastructure (DII) upon which the US military depends must be protected commensurate with its criticality. This analysis shows that:

- The DoD is highly dependent on the accuracy and availability of information.
- The DoD is dependent on the DII for information services.
- The DII is highly vulnerable to accidental and intentional disruption.
- These vulnerabilities are commonly known and widely publicized.
- Many individuals, groups, and nations have demonstrated disruption capabilities.
- The DoD's current ability to respond to disruption of DII functions is inadequate.

If the Department of Defense is to maintain operational readiness and fulfill its national security responsibilities, the information infrastructure upon which it depends for information services must be strengthened against accidental and intentional events that lead to disruption (corruption of information or denial of services).

In order to sustain US military capabilities, the following information assurance (availability of services and integrity of information) considerations must be given priority attention.

- Information assurance should be recognized and treated as a critical readiness issue.
- Defensive information warfare policy, doctrine, strategy, tactics, techniques, and procedures should be developed.
- Infrastructure design is different than systems design and should be treated as such.
- Existing technical and human vulnerabilities should be addressed.
- Information assurance standards, technologies, tools, and guidelines should be developed.
- Top level technical management of information assurance should be improved.
- Real-time control mechanisms to enhance information assurance should be developed.
- Testing programs should be created and used to enhance assurance.
- Flexible, automated, prioritized responses to disruption should be implemented
- Information assurance knowledge should be reduced to a usable and teachable form
- Information workers should begin to train as defensive information warriors.
- Readiness exercises and war games for defensive information warfare should begin.

Information assurance for the DII must also be cost effective. This analysis shows that the costs associated with these tasks will increase dramatically over time if the DoD does not act now. Furthermore, the efforts made to protect the DII will provide widespread benefits to US

commercial industries.

By the timely reinvestment of a small portion of the savings that will be gained from the current consolidation and migration to standard information and communication systems, the US will avoid enormous future expenses, mitigate possibly catastrophic military consequences, and enhance its national competitive edge for years to come.

Is Information Assurance an Unsolvable Problem?

NO! We can not make people immortal, but that does not mean we should abandon medicine. Nobody can provide perfect information assurance, but that does not mean the DoD should ignore a problem that may result in catastrophic military consequences.

The issues that must be considered for proper information assurance in the DII span a wide range, and a wide range of solutions exist to address these issues. There are some challenges in information assurance that are now and will likely remain imperfectly addressed for some time to come, but the vast majority of the challenges to&y can be adequately addressed with a reasonable amount of well directed effort

Perhaps a more enlightening view of this issue is the question of how much it will cost to address information assurance, and how much the US will save as a result of wisely spending that money. In this limited report, we cannot even begin to address the specific issues for specific solutions in specific systems, but we advocate financial and military analysis before undertaking costly action. We also believe that early investment will pay enormous dividends in both the short-term and the long-term:

- By assuring the US is able to win on the information battlefield
- By dramatically reducing the long term cost of information assurance
- By reducing the costs of disruptions in the DII.

The information assurance challenge is not only one that can be met, but one that must be met, if the US is to attain and retain a competitive edge in both the DoD and national information arenas.

What Are the Top DII Priorities?

Based on our study, we believe that the following three items are the most vital things the DoD can do in order to provide a DII with adequate information assurance.

1. Design the DII for automated detection, differentiation, warning, response, and recovery from disruptions. It is absolutely vital that these capabilities be designed in from the start, and that they be sufficiently automatic that they are effective without human intervention. Without these capabilities, the DoD will not be able to sustain readiness during a substantial disruption attack.

2. Design the data centers, network components, and network control centers for ease of repair (modular, reconfigurative). Without the ability to recover from disruption of these facilities, under attack, the DII and the DoD will grind to a halt, and will not be able to reconstitute either offensive or defensive capabilities in any meaningful time frame.

3. Train today's information workers to become defensive information warriors capable of defending the DII against informational attack. Without trained information warriors, the DoD will not be able to sustain the DII no matter how automatically the DII reacts or how well it is designed.

TABLE OF CONTENTS

1 BACKGROUND AND OVERVIEW

Over the last 5 years, the world has changed dramatically. The breakup of the Soviet Union, government financial considerations, and many other factors have caused the US to shrink the size of its military. In order to accommodate this change and still maintain US effectiveness as a military power, the DoD has looked more and more toward technological solutions that make it more efficient. The increasing prominence of computer networks, the shrinking price of high performance computers, and the proliferation of high speed digital communications have led to fighting styles that are both more effective and less costly than previous military methods. US fighting forces are faster and more agile than ever before, US weapons are more accurate and effective and cause less collateral damage, and US technological intelligence capabilities are unmatched.

Information warfare is now US military doctrine: Recent changes in US military doctrine have stressed information warfare as a central component of joint forces operations. [1] [22] [12] The US Army, [4] Navy, and Marines [3] [2] have all responded with their own expressions of policy based on that doctrine.

Offensive and defensive components of information warfare: Infoxmation warfare consists of offensive and defensive components. Offensive components were demonstrated in the Gulf War, where the US disabled Iraq's state and military command and control structures to the point where Iraq's military was literally paralyzed. [8] Although this is by no means the first example of offensive information warfare, [9] [106] it is certainly a startling demonstration of information warfare's effectiveness.

Defensive components of information warfare include such diverse areas as counter-intelligence, counter-deception, information security, and others. Information security is intended to provide data confidentiality, information integrity, and service availability. DISA's mission revolves around computation, communication, and information services, and thus information security is a primarily concern. This study addresses the informational aspects (as opposed to the physical aspects) of information integrity and service availability:

Within this paper, the term "information assurance" is used to mean information integrity and service availability. The term information assurance applies to the use of information*. The ultimate goal of information assurance is to protect users, business units, and enterprises from the negative effects of corruption of information or denial of services. For example, if the financial data in a payroll database is valid in the sense that it could be correct, but is not in fact correct, there may be no negative impact on the information system, but the enterprise may suffer when people get the wrong amount of money in their paychecks. Similarly, if an order for an engine

* Within DoD 5200.28-STD "Department of Defense Trusted Computer System Evaluation Criteria," the terms "assurance," "life-cycle assurance," and "operational assurance*" are used in technical policy statements that apply primarily to trusted, commercially available automatic data processing systems. These terms should not be confused with the usage of "information assurance" in this paper.

part in a supply and logistics system is lost in the part of the system that dictates which pallets get loaded onto which boat, the information system continues to operate, but the supply service is denied to the person requiring the parts. Naturally, if the information systems processing, storing, or communicating information become corrupt or unavailable, that may also affect the enterprise as a whole, but simply protecting the systems without protecting the information, processing, and communication is not adequate.

Within this paper, the term "disruption" is used to mean corruption of information or denial of services. The term disruption applies to a wide variety of events. Disruption applies to events whose impacts are felt immediately, over a period of time, and even events that are never noticed. Disruption applies to effects at many different levels: information systems, the information infrastructure, users, business units, or the enterprise as a whole. Disruptions can be obvious, as in the case of complete failures of information systems, subtle, as in the case of wrong part numbers in a catalog resulting in wrong part orders, or extremely subtle and indirect, as in the case of a change of address card causing a wrong address to be put into a shipping database, causing the mis-shipment of air conditioning rechargers, causing air conditioning to fail in a computer center, causing computers processing supply and logistics information in that computer center to fail, thus making it impossible to order the air conditioning rechargers needed to restore services. Disruptions can be caused by a wide range of sources, from random and naturally occurring events, through mischief, to malicious acts by military adversaries. Information assurance addresses all facets of disruption.

The DII is required to support the DoD in modem warfare: Over the past decades, the DoD, defense agencies, and industry have developed elements of the defense information infrastructure in a highly decentralized manner. This has led to the fielding of many proprietary, duplicative, and stand-alone information systems. This resulted in suboptimization, inefficiencies, and a lack of interoperability. To obtain efficiency, improve effectiveness, reduce costs, increase interoperability, and meet the coordination requirements of joint deployments, the DoD has undertaken the transition to a modern open-system information infrastructure. [10] This multi-year transition is being guided by centralized policy from the Office of the Secretary of Defense while the execution will be carried out in a decentralized fashion.

DISA has been assigned the responsibility for promulgating design requirements for the migration of DoD information systems into an integrated, resilient, global network capable of providing all appropriate information: [6] [11]

- To anyone properly requiring it.
- In a timely and accurate fashion.
- For reasonable costs.
- From peacetime to global war.

'Ibis objective integrated information network is called the Defense Information Infrastructure (DII).

Prudence demands the DoD assume battle damage: National security decision makers must assume that in future conflicts the DII will be attacked and sustain battle damage, both by 'hard kill' destructive weapons, and by 'soft kill' informational attacks. The designers of the DII should assume that the DII will be subjected to greater operational stresses than those experienced in the Gulf War to support a two theater engagement as called for by the current national defense strategy, [12] and anticipate hard and soft kill attacks while under this level of stress.

"It is a doctrine of war not to assume the enemy will not come, but rather to rely on one's readiness to meet him, not to presume that he will not attack, but rather to make one's self invincible" (Sun Tsu as cited in [3])

Defense against disruption is a critical readiness requirement: To provide information to anyone properly requiring it in a timely and accurate fashion is to require availability of services and integrity of information. Providing information services in a military context must include a recognition of the outcomes of hostile action to disrupt those services. The loss of information services in the context of the DII could result in military defeat

DoD policy recognizes this: "The Director Defense Information Systems Agency, as central manager of the Defense information infrastructure (DII), shall ensure the DII contains adequate protection against attack." [1 1 1]

Thus, DISA has a clear responsibility to defend the DII against intentional disruption. In noncombat situations, the DII is also required to operate despite accidental incidents, so DISA has a requirement to defend against these events as well.

While the process is already underway to integrate legacy systems into a DII, and there are already criteria in place for protecting classified and sensitive data and managing permanent and transient faults, there are fundamental issues that have not yet been adequately addressed. Specifically, no one fully comprehends what the intentional disruption implications are for such a large, complex, and critical system operating under the stressful conditions of information warfare.

Intentional disruption is not adequately addressed by current techniques: Existing efforts are primarily oriented toward preventing the illicit disclosure of both classified and unclassified but sensitive data, and preventing random or naturally occurring faults from resulting in failures. Government standards, policies, techniques, and procedures for information security address the disclosure problem, while standard engineering design practice, and in the case of more stringent requirements, the field of 'Fault Tolerant Computing' address the accidental disruption problem.

Standards, procedures, tools, and techniques for providing secrecy, standard engineering practice, and the field of fault tolerant computing do not and were never intended to address intentional disruption. Thus, the requirement for information assurance 'fell through the cracks'

in most current information processing and transport designs. Intentional disruption needs to be addressed by information assurance, which should underpin defensive information warfare.

There are a small number of research groups around the world that have been working on the information assurance problem for a number of years. Known foreign research locations include The People's Republic of China, Russia, Germany, Israel, Australia, Denmark, England, and Japan.

Benefits of information assurance extend beyond the DoD: As the nation's information systems are being tied together, whether in the DII or the NII, the points of entry and exposures increase, and thus risks increase. The technological advancement toward higher bandwidth communications and advanced switching systems has reduced the number of communications lines and further centralized the switching functions. Survey data indicates that the increased risk from these changes is not widely recognized. [16] [17] [18] Efforts made by DISA to promulgate assurance standards for the DII will have a positive impact on information assurance that will extend beyond the DoD and impact all segments of the national economy. As DoD standards become the basis for product designs, the savings gained by reducing downtime and exposure to intentional disruptions will have a positive financial benefit on the US.

Cost factors greatly favor selective immediate action: Data from cost studies shows that the cost of providing information assurance to the DII in the design and specification phase can be up to several orders of magnitude less than the cost of providing the same protections after integration is substantially completed. This savings will come in two forms: it will reduce the cost of implementing whatever protection is deemed appropriate, and it will guide the architectural structure of the DII to facilitate protection at lower cost. This approach applies to all new components of the DII.

For legacy systems, the cost of injecting information assurance may be astronomical, so a different approach should be considered. A timeframe should be established for replacement or enhancement of legacy systems, and DISA should plan on requiring appropriate information assurance features in replacement systems over that timeframe. Based on normal replacement cycles, this process should be completed over the next 10-12 years.

History shows that the cost of incremental improvement increases as perfection is approached. Rather than strive for perfect information assurance, risks should be managed in a reasonable way that balances cost with the protection it provides.

Based on these factors, it is the conclusion of this study that the most cost effective overall approach to providing information assurance to the DII will be to immediately incorporate information assurance requirements into design standards, and to provide network-based tools and techniques to detect and respond to disruptions.

Summary: By recognizing information assurance as a critical readiness issue and addressing it immediately, the DoD and the nation as a whole will greatly benefit:

- By assuring the US is able to win on the information battlefield.
- By dramatically reducing the cost of achieving protection.
- By reducing DoD costs due to disruption of the DII.
- By reducing current losses impacting the US national economy.

The DoD must recognize the threat of disruption and DISA must provide adequate information assurance guidelines for the DII.

In this initial study, information assurance issues are discussed in a qualitative manner. Based on these qualitative understandings, DISA should be able to begin the considerably linger and more complex task of quantifying these results and generating detailed information assurance criteria for defensive information warfare.

2 DISRUPTION VULNERABILITIES IN THE INFORMATION AGE

. Information has been critical to warfighting throughout recorded history. Over 5000 years ago, there were spies, well defined command and control structures, supply and logistics systems, documented strategic planning, and mechanical cryptographic systems. [19] Numerically inferior forces with informational advantage have historically dominated in military conflict [106] because of what is now called the force multiplier provided by that advantage. Better battlefield intelligence and communications leads to a fighting pace and efficiency that often overwhelms an enemy, better strategic knowledge leads to more well directed weapons design, morale is dependent upon the availability and content of information from home, and psychological operations are centered on impacting the enemy's human information processing. These information factors and many others have had significant impacts on the outcome of wars from Biblical times [102] through to today, [8] and they will likely continue to impact warfare for the indefinite future. [20]

If this has been true throughout history, why is it that there is a pressing need to reconsider this issue in a different light today?

The answer lies in the fundamental changes in information systems and the new ways in which people have come to depend on them over the last several years. Just as the industrial age led to fundamental changes in the way wars were waged, the information age is now leading to fundamental changes in the way wars are waged. [21]

The Gulf War is a recent example of how current US warfighting doctrine depends on and stresses information infrastructure. It is likely that the Gulf War was a unique experience in that there was no apparent attempt by the Iraqis to disrupt the information infrastructure the DoD put in place during Operation Desert Shield. A series of extraordinary efforts by military and civilian personnel in the middle-east, in the continental US, and throughout the world, created a temporary infrastructure capable of letting US forces fight as they had trained. [8] A prime planning concern for the future should be getting enough of an infrastructure in place to be able to handle a similar situation and acquiring the capability to support the multi-theater scenario called out in current defense guidance. [12]

2.1 Information Warfare Doctrine

Statements of new US military doctrine have been promulgated to reflect these new realities. These writings on doctrine explicitly address the role of information in modem warfare and speak to the resulting offensive and defensive aspects of information warfare.

- "The Joint Campaign should fully exploit the information differential, ... is, the superior access to and ability to effectively employ information on the strategic, operational, and tactical situations which advanced US technologies provide our forces." [1]

- "Our surveillance efforts will continue to emphasize exploitation of space and electronic warfare systems to provide commanders with immediate information while denying and/or managing the data available to our enemies." [2]

- "SEW [Space and Electronic Warfare] is a fundamental alteration of the tactical continuum that permanently has changed the face of naval warfare" [3]

- "... It explains the ten principles that assure the Warfighter will have information superiority over any opponent." [4]

- "In fact, space is now so integral to joint and combined military operations that were we to remove space assets from our military arsenal, as a nation we would be relegated to employing warfighting tactics much like those of WWII . . . [space force enhancement support] comes in the form of navigation, communications, surveillance, tactical warning and attack assessment, and environmental monitoring." [5]

The central role of information in warfare, as in the economies of modem information age societies, will continue into the future. As one author put it: "In the best circumstances, wars may be won by striking at the strategic heart of an opponent's cyber structures, his systems of knowledge, information, and communication." [106]

2.2 The DoD Is Dependent on Information

The DoD is dependent on information for all aspects of its operation. Historically, components of the DoD have implemented stovepiped information systems designed to fulfill special needs. This has resulted in a coordination problem in joint operations because integrating the diverse information stored in these stovepiped systems is difficult and time consuming, and thus limits the tempo of operations. To fully exploit the advantages of information in warfare, and to reduce the costs associated with information processing, duplicative systems, and redundant data entry, the DoD has made the doctrinal and policy decision to move toward a globally integrated Defense Information Infrastructure (the DII). [10]

The complexity, scope, and timeliness requirements of DoD information processing are exemplified by some of the applications supported by the DII:

- The inventory, supply, and logistics systems of the DoD and their service providers are now automated to the point where they cannot locate or deliver inventory in a timely fashion without properly functioning information systems, and joint forces coordinated logistics operations now rquire that a large number of distributed heterogeneous information systems operate properly together. [10] Increased demands on the information systems supporting the DoD's supply and logistics systems are produced by reduced lift capability, [12] and just-in-take delivery requirements called for in current DoD doctrine.

- The DoD now trains personnel at all levels to work in unison by using a geographically distributed network of simulators that communicate with each other in real time to emulate complex battle situations. This is how the DoD prepares soldiers, sailors, airmen, and marines for the sort of joint and coordinated efforts required to win a more rapidly paced war with fewer people. [105]

- The DoD personnel management systems are now automated to the point where it is impossible to pay, assign, move, or track people without properly working, globally networked information systems.

- The DOD'S procurement and contract management systems are now automated to the point where it is impossible to control costs, pay vendors, provision telecommunications, let or track contracts, allocate or release funds, or report on activities without automation.

- The use of "Command and Control" Warfare both to paralyze the enemy and to enhance friendly speed and agility has become a theme in DoD doctrine. [23] This capability requires reliable, available, accurate, real-time, globally interlined, robust information systems. [22]

The accomplishment of military functions, both direct combat operations and support, depend to varying degrees upon the availability and accuracy of information. For example, most activities in modem warfare depend on the reliable communication of command and control and situation information. Many military activities rely on timely, assured access to accurate position, environment, logistics, medical, personnel, or financial information. This dependency is not static based on the content of the information. Rather, employment of particular military weapons or operational tactics at a particular operational tempo depends on the assured availability of a certain quantity and quality of information at a particular time.

By analogy, information requirements are equivalent to petroleum budgets required to maintain a particular operational tempo. If either the information or the petroleum is unavailable, the desired operational tempo will not be obtained. (This analogy is not perfect in that once petroleum is used, it is gone, while information is not consumed in its application.)

In short, nearly every component of the US military and the infrastructure upon which it depends are highly dependent on information and information systems.

2.3 The DII Is to Fulfill DoD's Information Requirements

Horizontally and vertically integrated command, control, communications, and computer automation for joint and combined forces operations are pivotal to US military force. [10] The DII concept was created to: [1 1]

- Provide a consolidated global information infrastructure
- Provide robustness and resiliency to DoD information services

- Revolutionize information exchange
- Properly and transparently manage information on a global scale
- Reduce information technology burdens on operational and functional staffs.

The creation of the DII will enable DoD operational and functional staffs to access, share, and exchange information worldwide. It will include such improvements as end-to-end information support services, standardized data definitions, and interconnection of all voice, data, imagery, and video communications and computing systems. To remain reliable and transparent, centralized network and system management and diagnostic capability will be put in place. To reduce life cycle costs, the DII will consolidate or integrate data centers, maintain widely-available communications networks, use commercial off-the-shelf (COTS) and Government off-the-shelf (GOT) products, and centralize acquisition and technical control of these elements. [63] To improve efficiency, redundant data entry will be eliminated, and standardized training will be used.

2.4 Information Assurance Is Critical and Inadequate

The cost and efficiency advantages brought about by implementing the DII will increase the DoD's dependency on the DII. If elements of the DII are not available, information is inaccurate, or the DII does not properly provide required functional or information transfer capabilities, time will be lost and overall mission effectiveness will be diminished.

2.4.1 Secrecy Standards DO NOT Address Information Assurance

It is critical in understanding the information assurance challenge to understand the difference between **information assurance issues** which **relate to all information** and information systems, and **secrecy issues** which **relate to classified or sensitive but unclassified data.** Classified or sensitive but unclassified data is controlled based on its content, and is controlled because knowledge of it might be useful in ways that could adversely affect US interests or actions, because release could be a violation of US privacy laws, or because release could result in the assumption of financial risk. Information assurance requirements apply to **all information,** and **are based on use** rather than content.

Some assert that existing policies and standards that guide protection of data sensitivity are not adequate for addressing information assurance. [24] There is a need to consider information assurance in defensive information warfare planning.

2.4.2 Fault Tolerant Computing Standards DO NOT Address Information Assurance

It would be easy to assume that information assurance is already provided by existing fault tolerant computing standards and practices such as protection against random noise, [25] [26] lightning, [27] RF noise, [28] loss of packets, [29] and other transient factors that cause disruptions in information systems. Unfortunately, intentional attackers are not accurately modeled by the statistical models of faults used to develop existing reliability standards. (See note 1)

"Most communication channels incorporate some facilities designed to ensure availability, but most do so only under the assumptions of benign error, not in the context of malicious attack." [38] (note 6, p100)

2.4.3 Perfect Systems Are Infeasible

The field of 'high assurance' computing addresses information systems for the most critical applications. (e.g., life support systems, flight controls, nuclear warhead detonation) Unfortunately, building 'perfect' systems is far too costly and resource intensive for the wide variety of systems and networks found in the DII, and only adequately addresses certain types of very well defined control applications. (See note 2)

For the sorts of general purpose systems in the DII, there are classes of attacks that can not be perfectly defended against. Two well known examples are computer viruses [49] and exploitation of covert channels. [50] If the DoD spends its resources on trying to implement perfect solutions to these problems, it will surely fail and go bankrupt in the process, but the DoD can not simply ignore these and other similar problems, because they present a real and identifiable threat to national security and directly impact readiness and sustainability of US forces.

Feasible solutions will not be perfect. Rather, they should responsibly trade cost with protection. DISA should support analysis of cost effectiveness to avoid unnecessary duplication and to provide a uniform basis for comparison.

2.4.4 Current Disruption Defenses Depend on People

Current US defenses against disruption depend almost entirely on human prevention, detection, differentiation, warning, response, and recovery. Detection of most disruption attacks comes only when people notice something is going wrong. In many cases, detection never occurs, while in other cases, detection takes several months. Differentiating natural, accidental, mischievous, and malicious disruption is a manual process, and the root cause is often undetermined or misidentified as accidental. Warning has to be properly controlled to prevent false positives and false negatives, and depends on forensic analysis. Response commonly takes from hours to days, and is almost e&rely manual. Recovery too is almost always a manual process, takes from hours to days, and is often performed improperly. (See note 12)

Human attack detection has several problems besides the limited response time and large numbers of false negatives. Perhaps the most important problem is the expectation of breakage and the inabiity to differentiate properly between breakage and malicious attack, Another problem is the tendency to detect fewer faults over time in an environment where faults are commonplace. [51] This can be exploited by an attack wherein the number of disruptions are slowly increased, while the human operator becomes increasingly insensitive to them. Enhanced training improves performance, but humans are clearly still limited, particularly when it comes to detecting subtle attacks characterized by the coordination of numerous seemingly different and

dispersed events and attacks designed to exploit the reflexive control aspects of human behavior [103]

Automated tools for detecting misuse in computer **systems** and local area networks are currently emerging, and this technology is rapidly approaching commercial viability. [124] The most advanced misuse detection systems include localized responses to statistical anomalies and rule-based response to known attack patterns. DISA should enhance computer misuse detection systems to cover broader ranges of attacks, systems, and responses at the wide area network and infrastructure levels. (See note 14)

2.4.5 The Current Infrastructure Is Highly Vulnerable

Well trained intentional attackers understand the common assumptions made by designers of information and secrecy systems, and explicitly design attacks to exploit the weaknesses resulting from these assumptions. Protective techniques that work against statistically characterized events is rarely effective against directed attack, and techniques designed to provide secrecy is rarely effective against disruption. One relatively limited study of the impact of malicious node destruction using a structure that works very well against random destruction found that preventing intentional attacks with standard fault tolerant computing techniques may require an order of magnitude increase in costs. [36] Studies and demonstrations of computer viruses in secrecy systems approved for DoD use have demonstrated that these systems are ineffective against disruption. [39]

Current system reliability estimates do not account for deliberate software corruption. [38](p 55) Telecommunication networks can fail from software malfunction, failures can propagate in operations or control systems, [43](p32) and system availability estimates seem to overlook this cascading effect. As an example, telephone networks are supposedly designed for something like 5 minutes of downtime per year, [33] and one company advertises that if 800 service fails, restoration is guaranteed in under 1 hour. Yet in a single incident in 1990, the AT&T (American Telephone and Telegraph) 800 network was unavailable for over 4 hours, [43] which seems to imply that this failure covers expected outages over the next 50 years! Considering that a similar failure brought down telephones in several major cities for several days in 1991, [93] there appears to have been a flaw in this availability analysis. (see note 3)

According to a National Research Council report: "As computer systems become more prevalent, sophisticated, embedded in physical processes, and interconnected, society becomes more vulnerable to poor systems design, accidents that disable systems, and attacks on computer systems. Without more responsible design, implementation, testing, and use, system disruptions will increase, with harmful consequences for society. They will also result in lost opportunities from the failure to put computer and communications systems to their best use." (The opening paragraph of [38])

2.4.6 The Best Defense Is NOT a Good Offense

Reliance on any offensive capability the US might have as a defense against disruption of DoD information systems would be misplaced. This is because of two features of non-physical offensive information warfare technologies: vulnerabilities can be exploited by small, mobile, hard to identify, physically distributed groups' of individuals located anywhere in the world, [48] and it is not possible to determine with certainty whether or not an attack is underway [49] or to identify the source of an attack that is known to be under way. [52]

Offensive capabilities can theoretically be used in one of two ways to defend against attacks; preemptively or responsively.

- **Preemptive:** It is impossible to launch a preemptive strike when the enemy can't be located and can operate from anywhere. Preemptive strikes may also lead to extremely negative consequences.

- **Responsive:** Responding to attack with counter-attack is also impossible if the enemy can't be located or the attack can't be detected. Response may also be ineffective in stopping an attack once it is launched because in information warfare, destroying the enemy may not deflect the attack. [48]

Regardless of the power, speed, and accuracy of the offense, the DoD will require an adequate defense if the US is to prevail in a hostile information warfare environment.

2.5 Observations Regarding the DII

The DII design includes information processing components, the DISN transmission segment, the DISN network management segment, and the DISN services segment. [1 1]

2.5.1 Information Processing Components

Today's information processing components consist largely of low-assurance computer systems. Every general purpose DoD and civilian computer system tested for information assurance so far has proven vulnerable to disruption. [39] Many existing DoD information processing components don't even meet nominal business operational control requirements common throughout industry. For example, a recent GAO audit to determine whether controls in large data centers were adequate to assure data integrity showed:

". . . that both [Cleveland and Indianapolis] Defense Information Technology Services Organization (DITSO) Centers had serious deficiencies [that would] allow any knowledgeable user to gain access to pay data, and to add, modify, or destroy it, or accidentally or intentionally to enter erroneous data, without leaving an audit trail." [115]

A degree of assurance in existing DoD systems is provided by their physical isolation from an integrated network. As the DoD moves toward a networked DII, DISA should assure that DoD decision makers understand that these newly connected systems are vulnerable to disruption of a wider variety from more sources, and make suitable investments in information assurance to offset the increased risk.

2.5.2 DISN Transmission Segment

The vast majority of current communications devices, systems, and networks used in military support systems do not provide high assurance. (See note 8)

"Just how vulnerable our networks have become is illustrated by the experiences of 1988: There were three major switching center outages, a large fiber optic cable cut, and several widely reported invasions of information databases by so-called computer hackers." [38](p2) One outage in 1991 impacted millions of customers and temporarily disrupted air traffic control centers in New York (which caused slowdowns in much of the northeastern US and across the nation).

2.5.3 DISN Network Management and Services Segments

Many of the legacy systems being integrated into the DISN network management components consist of proprietary designs. The assurance in these systems, as in the information processing components, is provided, in large part, by their physical security. As the DoD moves toward a consolidated network management system for the DII, it will magnify the potential vulnerability of its network management segment to disruption and introduce the potential of causing widespread damage.

Current DII services consist almost entirely of electronic messaging, file transfer, bulletin boards, and directory systems. [7] These services are predominantly implemented with low-assurance computer systems that process unclassified information. As the DoD moves toward a networked DII, users will have a high degree of flexibility in selecting services through integrated network management, advanced intelligent network techniques, and common signaling systems. [60] This flexibility will make users more dependent on these services to accomplish their mission, and it will also make these services more vulnerable to disruption from a wider variety of sources. (See note 9)

2.5.4 Interactions Between Components

Existing components of the DII have well known and easily exploited vulnerabilities to disruption, but even if these components were individually strengthened against disruption, they would not necessarily provide information assurance when networked together. The combination of otherwise assured systems in an assured network environment can lead to an overall system that is not assured. In one case, two systems that were independently safe against corruption by a particular computer virus were both disrupted by that virus when they were networked together.

The cause was a mismatch in the way integrity was implemented and the way peer-to-peer communications works in modem networks. [39] There is still no overall theory of how to safely connect network components, but in the limited cases where connection safety is understood, unsafe connections should be avoided. [66] [67]

Simply bolting together a variety of information security features doesn't solve the protection problem. To get synergistic benefits by combining information assurance features, they have to be properly combined, and this is not yet a well understood phenomena. [39] In most cases, rather than enhancing protection by combining features, the entire system is only as strong as the weakest link.

The people who architect the DII must come to understand this issue and exploit that understanding to provide adequate information assurance.

2.5.5 The Human Component

Clearance processes do not detect people who turn against the US after they are cleared, people who have breakdowns, people subjected to extortion, or many other "insider threats." Many sources claim that the majority of computer crimes come as a result of an authorized person using that authority inappropriately. Although sufficient evidence is not available to support this contention, there is clearly a potential for "soft-kill" harm from an insider that is greater than from an outsider because the insider has fewer barriers to bypass in order to succeed.

The current DII design assumes. that insiders act properly to a large extent. A proper infrastructure design should not make such an assumption or depend on it for meeting design criteria. DISA should ensure DII design criteria explicitly address the insider threat.

2.5.6 Physical Attacks

Elements of the US information infrastructure are also highly vulnerable to physical attack. For example, several authors have noted that US telecommunications capabilities could be disabled for a substantial period of time by proper placement of 20 or fewer small explosive devices. Information processing facilities often depend on easily disrupted public utilities for electrical power and water. Further, the potential targets and methods for physical attack on an exterior structure such as a heat exchanger that can halt computer operations very efficiently are often inadequately protected.

Although this is a vital area to be covered, it is not within the realm of this study to address it, except in one way. By the very nature of the information assurance challenge in a military context, a reasoned response would be designed to detect and react to disruption regardless of the cause. The warning component of an information assurance system provided for the DII should clearly indicate any set of disruptions that appear to be part of a coordinated attack, and help orchestrate a coordinated defense. (See note 15)

2.5.7 DII Information Assurance Standards Are Inadequate

It is enlightening to examine the current US Government standards base upon which open systems are now being acquired. [68] The DoD standards document begins with a list of protection service standards, including some that seem to be information assurance standards needed to fulfill requirements of the DII. Unfortunately, almost none of the list of service standards is currently specified:

Service Standard	Status
Authentication	Not Available- In Process
Access Control	Not Available- In Process
Non-Repudiation	Not Available- In Process
Confidentiality	Not Available- In Process
Integrity	Not Available- In Process
Auditing	Not Available- In Process
Key Management	Not Available- In Process

Most of the 'Not Available- In Process' items are specified as 'This work is still in the early stages and is not yet of practical use. It should not be referenced in a procurement." Further, there is no clear migration path, so there is no defined way for the designers of the DII to even plan for their future inclusion. Notice that "availability of service" is not even on the list of standards to be developed!

By way of reference, the IS0 (International Standards Organization) standard upon which this list was based was in approximately the same incomplete state about 10 years ago, when the protection addendum to the IS0 standard was newly created. To date, no significant progress has been made in these areas, and no current "open system" COTS products provide substantial coverage of these areas.

2.6 Prudence Dictates the DoD Assume the DII Is Targeted

In the October, 1993 crisis in Russia, the members of the dissolved parliament escalated to military action by ordering their supporters to take over the Mayor's office across the street, the television station across town, another major telecommunications center, and the Kremlin a few blocks away, in that order. The takeover of the Mayor's office in downtown Moscow was essentially unopposed (only warning shots were fired), but when it came to the television station, the battle became fierce. The other targets were never even threatened. Can there be any question that the Russian leadership on both sides understood the import of information as the key to victory?

Infrastructure has been a major target at least since WWII, when the allies targeted German ball bearing factories. [69] This was not only because ball bearings were used in tanks, aircraft, and naval craft, but because they were used in the machinery that made machinery.

Information and information systems are the ball bearings of the information age. Both military and civilian operations depend on this technology at almost all levels. Information technology is used to design information systems, to direct telephone calls and data transmission, to control individual radios and building security systems, and to keep accurate time. Each of these information technologies is vital to the DII.

Information infrastructure is a low risk, high payoff target for disruption. (See note 10)

2.6.1 The World Knows the DoD Is Information Dependent

There are many publicly available examples of the US dependency on both military and commercial information technology, including recently published examples from wartime military operations.

The US Army's Chief of Staff called Desert Shield/Storm the "Knowledge war." [8] (p ix) The House Armed Services Committee said ". ..acquiring support systems consistent with high-tech weapons may be more important than buying the next generation plane or tank." [8] (p xxi) According to another author, ". ..it is very surprising that very extensive use had also to be made of the international commercial networks, Intelsat and Inmarsat." [70] Still another author wrote "DISA and CENTCOM learned a valuable lesson: A viable information systems architecture requires the total integration of commercial and military communications systems...". [71]

Logistics data passing over local and wide area computer networks also became vital. Regarding Marine Corps operations: "Supply and maintenance information, . . . soon came to be seen as critical to the success of the operation. . . . these systems had to operate in the same environment as the systems that [performed command and control] functions." [72]

Real US information warfare vulnerabilities are commonly described in both fictional and factual books, articles, and other media (See note 4)

2.6.2 Other Nations and Organizations Have Demonstrated Attack Capabilities

Ideas about the use of software for military and civil infrastructure attack have been published in the military, computer science, and popular press, so this concept is common knowledge among many computer literate people. Many examples include specific mentions of military targeting. Here are two:

- An article in a recent 'Wired' magazine names the 'Top Ten' US infrastructure targets including the Culpeper telephone switch that handles federal fund transfers and the Worldwide Military Command and Control System (WWMCCS). [79] [80]

- In a paper published in 1988, the authors suggest logistics attacks, and suggest that "Software warfare holds promise of emerging as the first truly militarily effective form of economic warfare." [48]

Publicly available sources indicate that well over 30 nations have the capabilities required to launch successful disruption attacks against the DII, that several nations have active programs directed toward understanding and preparing capabilities for information infrastructure attack, and that several relatively small independent organizations have demonstrated substantial attack capabilities. (See note 11)

One paper presented to the Naval Postgraduate School in August, 1993, and available to the public claims that with 20 people and $1,000,000 the author can bring the US to its knees. [81] Other expert claims range from $100,000 and 10 people for large scale DII disruption over a period of weeks, to $30,000,000 and 100 people for total information infrastructure disruption resulting in multi-year recovery time. [109]

Information warfare can be practiced by small private armies, terrorist organizations, drug lords, and even highly motivated individuals of modest means. This may represent a fundamental shift away from the notion that the hostile nation state is the major threat the US has to be concerned with. [128] [21] [113]

2.6.3 Other Nations Are Working on Information Assurance

The People's Republic of China has a group headed by Yue-Jiang Huang that has produced both internal and international hardware enhancements to personal computers for protecting against many forms of disruption. This group is also doing substantial work in the use of non-linear feedback shift registers for both secrecy and integrity applications.

In Russia, there is at least one group working on disruption prevention, detection, and response systems. This Moscow based group at the Central Research Institute "Center" in Moscow is working on new hardware architectures that provide enhanced integrity protection and limited availability against general classes of malicious threats. They seem to have an emphasis on computer viruses, but far more general application can be made of their architecture. [1163

Research groups in Israel regularly publish results on their research in international journals, and several groups have started work on protection of information systems against general classes of malicious corruption. [118] [119]

An Australian research group directed by Bill Caelli and centered at Queensland University of Technology is concentrating a substantial amount of effort in the design of high integrity networks capable of withstanding malicious disruption. They also have people working on cryptographic integrity techniques and key management systems with revocation for use in systems similar to the DII.

At least one Canadian author has published work on limits of testing and coding spaces against malicious disruption attacks as well. [1173

A German research team at the University of Hamburg has gone a step further than most groups in this area by forming a database of parts of computer viruses. They essentially break the thousands of known viruses into component parts (i.e., self-encryption, find file, hide in memory, attach to victim, etc.) and store the partial programs in a database. Many known viruses have common components, but there are on the order of several hundred of each different component part. This gives them both the capability to detect and automatically analyze many viruses in very short timeframes, and the capability to generate on the order of 10^{20} different viruses automatically by mixing techniques together.

Several other countries have started to publish papers in the information assurance areas, and although there is no apparent evidence for massive efforts, it seems that the international interest in this field has increased substantially since the Gulf War.

2.6.4 The Insider Threat Demands Attention

Many publications on computer security identify the most common source of intentional disruption as authorized individuals performing unauthorized activities. The normal clearance procedure has not proven effective in eliminating this threat, and it is therefore prudent to take measures to protect against, detect, and respond to insider attacks.

Accidental disruption is also commonly caused by insiders acting imprudently, and it is sometimes very difficult to differentiate between accidental and intentional disruption in this context. This implies that more stringent techniques may have to be applied to observe insider behavior and reliably trace the specific actions of individuals in order to detect patterns indicative of intent.

3 PREPARING FOR DEFENSIVE INFORMATION WARFARE

Obtaining information assurance will require the application of resources and hard work. It will not come about as a serendipitous feature of the development of an information infrastructure based on open systems. The longer this matter resides on the back burner or is treated as a matter of academic interest, the greater the eventual costs will be to add resiliency to the infrastructure. Ultimately, neglect of this matter could result in major economic loss, the loss of military capability, and military defeat

3.1 Information Assurance Is a Readiness Issue

DISA should strive to ensure that senior decision makers come to understand that the assured availability and integrity of information are essential elements of US military readiness and sustainability so that they will provide adequate resources to meet this looming challenge.

Military capability is: "The ability to achieve a specified wartime objective (win a war or battle, destroy a target set). It includes four major components; force structure, modernization, readiness, and sustainability.

a. force structure--Numbers, size, and composition of the units that comprise our Defense forces; e.g., divisions, ships, air-wings.

b. modernization-Technical sophistication of forces, units, weapon systems, and equipment.

c. readiness-The ability of forces, units, weapons systems, or equipment to deliver the outputs for which they were designed (includes the ability to deploy and employ without unacceptable delays).

d. sustainability-The ability to maintain the necessary level and duration of operational activity to achieve military objectives." [91]

Readiness assessment generally involves such factors as people authorized and on hand, their skills and training; operational status of equipment, the time to repair, degree of degradation; training status of units, recentness of field exercises, command post training; and other more detailed factors. In the age of information warfare, everyone in the military must recognize that the readiness status of forces, units, weapons systems, and equipment depends on the status of the information infrastructure. An assessment of readiness should include such questions as:

- Are there enough information workers and managers on hand?
- Are they properly trained in detecting and reacting to information attacks?
- How recently have they undergone defensive information warfare training?
- What is the readiness status of the DII?
- How much stress can the DII take at this time?

Currently, the DoD appears unable to take comfort in the answers to these questions. Training programs to prepare information workers for the prevention of attack, detection of intentional attacks, differentiation of malicious from mischievous from accidental disruption, and the recovery steps to undertake do not exist. Worse, there is no analysis indicating how many people with what sorts of training and skills are required to operate successfully in an information warfare environment

The DoD depends on the DII at least as much as it depends on the logistics structure for battle readiness, and yet the DoD does not treat them in the same light. The DoD must assess information assurance as a readiness issue, it must incorporate DII readiness into the overall military readiness assessment, and it must treat DII readiness as a component critical to overall battle readiness. DISA should undertake an awareness campaign that brings these concerns to the attention of OSD Principle Staff Assistants, the Military Departments and Services, and Defense Agencies.

3.2 DISA Planning Should Reflect Information Age Warfare

In any conflict against an information warfare opponent, the DII will take battle damage. In order to continue fighting under this sort of attack, the DII must automatically detect, differentiate, warn, respond, and recover from disruption. There must be enough redundancy to meet bandwidth requirements during anticipated levels of disruption, sufficient firewalls to prevent disruption from spreading, sufficient mechanisms to make recovery and reconstitution of the DII feasible in an appropriate time frame, and sufficient training and support to allow that reconstitution to safely take place. In order to meet budget constraints, the DoD must find ways to do this at a tolerable cost. (See'note 14)

It is not reasonable to expect that technicians will be able to detect, differentiate, warn, respond, and devise work-arounds for each attack in real-time, and in the case of remote components, they may be unable to gain access to do these things at reasonable cost For this reason, the designers of the DII must devise mechanisms that are as nearly automatic as feasible, and have built-in resiliency that, at a minimum, puts these mechanisms into known and controllable state sequences when they become ineffective over a period of time. This is very similar to the requirements on remote space exploration vehicles, except that the DII must be designed to behave in this fashion even during hostile attack and at a far lower cost

3.2.1 DISA Must Retain Flexibility

In order to spend money wisely and still be properly prepared, DISA must ensure that the DII retains flexibility to adjust to changes in doctrine and strategy over the next 20 years. Compare US warfighting in 1973 to 1993. Predicting 2013 is not a simple matter. Rather than trying to make a 20 year prediction and hinging enormous amounts of money on being right, DISA should promulgate design guidance that ensures a DII capability that is flexible enough to adapt with the times. Fortunately, information systems are easily made flexible, but unfortunately, that flexibility

leads to vulnerability to disruption. The designers of the DII must devise information assurance techniques that allow flexibility without increasing vulnerability.

3.2.2 Separate Information Assurance Policies And Standards are Needed

Most current information protection policies include requirements for availability and integrity, but these features are always mentioned along with secrecy. When this policy is translated into implementation, the information assurance elements are usually ignored. An example of this is the recent draft versions of the DISN specification. The top level goals include almost equal emphasis of these three elements of information assurance, [60] but in the design process, there is often a de-emphasis of information assurance and an emphasis on secrecy. [61] There seem to be two reasons for this, and top level attention is required in order to resolve them:

- Information assurance is usually brought up in conjunction with protection of' classified information. Even though these areas are distinctly different, they are specified, discussed, and addressed together. In order to assure that information assurance is adequately addressed, policy makers should separate the information assurance requirements from the secrecy requirements, and make it explicit in policy documents that they are separate and different.

- There are no information assurance standards explicitly referenced in top level specifications.. When specifications are translated into implementations, standards influence a large part of the design process. Standards are commonly viewed as checklists that have to be met, and where no standards are specified, there is no checklist, and thus no features are implemented. To assure that information assurance is properly and consistently practiced, DISA should develop a set of information assurance standards for the DII that address disruption. (See note 5)

3.2.3 Infrastructure Level Optimization Should Be Addressed

There are substantial differences between designing a typical information system and designing a good information infrastructure, and the techniques normally used in information system design are often less than ideal in infrastructure design. One of the most glaring examples of these differences is in the tradeoffs between efficiency and effectiveness. (See note 13) In designing typical information systems, good designers almost always choose to do things for efficiency, while good infrastructure designers almost always choose to do things for long term effectiveness.

- A typical system designer will choose to perfect a hardware device or interface rather than use one that has flaws. An infrastructure has to support all manners of devices and interfaces, whether operating perfectly or with flaws, regardless of design mismatches. 'These devices will change over time, and a good infrastructure should support the range of changes over the expected lifetime by being designed to be changed.

- A typical system designer will choose to use components with almost identical electrical characteristics, matched timing limits, and equal reliability. An infrastructure is composed of components with a wide range of electrical characteristics, timing limits, reliability traits, and other design constraints. Over a period of decades, almost everything in an infrastructure will change, but the infrastructure as a whole should be designed to continue operating all along.

- A typical system designer will assume in the design of each component that all of the other components work properly, and repair faulty component designs until this is true over the testing period. An infrastructure should be designed to operate properly when SOME of the components operate properly, not only when they ALL operate properly. A faulty component should not have a significant impact on overall operations, and components should be designed to operate on the assumption that other components work improperly. Infrastructures regularly have components changed, upgraded, removed, or added, and should operate without substantial problems regardless of these changes.

- A typical system designer will implement central control mechanisms, synchronized clocks, duplex bus usage, and other techniques that share resources for efficiency. An infrastructure should not have a central control, an off switch, or a lot of dependency between components. Highly efficient resource sharing should not be critical for infrastructure operations; it's not that efficiency should be ignored, but rather that it should not be depended upon. The DII has a requirement for removing redundancy from data entry in order to increase efficiency. This policy itself may be flawed from an infrastructure standpoint, even though each application using the infrastructure may have this as a design goal. (See note 6)

- A typical system designer will use top-down design to break large problems into smaller, more manageable parts. This reduces design complexity [107] and allows design challenges to be addressed by subgroups. The problem is that technical expertise tends to be grouped near the bottom of the design structure while management tends to be grouped near the top. In infrastructure design, the best designers should be concentrated at the top, because there is a need to design an overall infrastructure that operates regardless of the components that are eventually attached to it, and that requires central technical design oversight.

- In a typical system design, the designer is provided with a description of the range of uses of the system before starting the design process, and designs the system specifically for the purpose. In an information infrastructure design, the designer is faced with designing an infrastructure that will support an unknown mix of current and future applications. A good infrastructure designer must design the infrastructure to be adapted over time to optimize performance for changing needs, and must not limit the utility of the design by making it to specific or too inflexible.

DISA should ensure that the top-level technical managers responsible for designing and operating the DII understand the issues of infrastructure design as opposed to typical system design and can help make design decisions that will satisfy the changing requirements over the lifetime of the infrastructure.

3.3 DISA Should Addresses Current Weaknesses

In order to transition existing systems into the DII while providing appropriate information assurance, DISA must first understand the weaknesses of these legacy systems, and then find ways to provide these systems with the information assurance features required in order to operate in the DII environment.

A key step in this process is performing a threat assessment which can be used as a baseline for vulnerability analysis. If properly done, such a threat assessment will bring to light a variety of new threats and threat sources that have not historically been considered in DoD vulnerability analysis.

Once the threat assessment is completed, vulnerability analysis of the most common classes of system can begin in order to create baseline vulnerability assessments of the major classes of systems without performing an expensive and unnecessary exhaustive analysis of each system on a piecemeal basis.

While vulnerability analysis is underway, mathematical life cycle cost and coverage analyses of potential defensive measures against identified threats in different classes of environments can be performed. As vulnerability assessments become available, the results of these assessments can be used in conjunction with defensive measure analysis to identify minimum cost protective measures required to cover identified threats.

As threats, vulnerabilities, and defensive measures are made available to program managers, they can make risk management decisions and implement appropriate controls in keeping with budget and other constraints.

3.3. Technical Vulnerability Should Be Assessed

DISA should undertake a substantial study of existing and planned DII components in order to understand their vulnerabilities to offensive information warfare and determine appropriate actions to provide information assurance during the interim period before the DII and enhanced components are fully developed. Specifically:

- Perform disruption oriented assessments to identify potential vulnerability.
- Perform safe and authorized experiments to more precisely assess the extent to which accidental and intentional disruption has been addressed in the DII components in place today.

- Analyze the overall DII in conjunction with these analytical and experimental results to assess overall DII vulnerability to disruption today.

- Determine methods by which existing and proposed DII components can or should be cost effectively upgraded or replaced over time to provide enhanced information assurance for the DII.

There are some limited but proven scientific theories about vulnerability to intentional disruption, [39] [92] and these theories can be used to form hypotheses about potential information assurance problems. From these hypotheses, DISA should sponsor the development of experiments to confirm or refute the existence of actual vulnerabilities, provide immediate awareness of their existence to information assurance personnel, and form approaches to removing or reducing their impact on the DII.

Something that should be clear from the start is that it will be infeasible to analyze software in most legacy systems for potential vulnerabilities, because the DoD has over 500 million lines of customized software in operation today, and the vast majority of it has never been examined for information assurance properties. With that much unexamined software, it is prudent to assume that malicious logic weapons have been implanted.

One way to enhance assurance in networked legacy systems at a very low cost is to provide an external misuse detection capability at the network level. These sorts of enhancements can provide substantial protection improvement at minimal cost, remain flexible enough to be adapted as the DII expands, and can provide a backbone for long term automated detection and response.

In the course of assessment, improved procedures, standards, and documents should be generated to capture and disseminate the limited expertise currently available in this field. A mentor program might also be used to develop more expertise in this area.

3.3.2 Human Vulnerability Should Be Addressed

According to one recent report, [94] the root cause of 30-40 percent of failures in digital cross connect systems is human procedural errors and is the cause of more disruption than any other single source. Many industry studies show similar results for other classes of information systems and networks. One report claimed that over 80% of reported intrusions could have been prevented by human procedures. [127] Another author posted to the "risks" forum that the lack of information from the current CERT (Computer Emergency Response Team) caused numerous disruptions to take place and kept them from being prevented, detected, and corrected. [90]

"High reliability organizations are defined as high-risk organizations designed and managed to avoid catastrophic accidents. The organization is high-risk due to the high complexity of the technology. Examples include air traffic control and nuclear reactors. . . . increasing numbers of serious errors will occur in high-reliability organizations, . . . data is lacking on ways to avoid

exceeding human capacity limits, and . . . design and management strategies to allow safe operation are not understood.... These organizations have several distinguishing characteristics in common: hyper-complexity; tight coupling of processes; extreme hierarchical differentiation; large numbers of decision makers in complex communication networks (law of requisite variety is cited); higher degree of accountability; high frequency of immediate feedback about decisions; compressed time factors measured in seconds; more than one critical outcome that must happen simultaneously." Another study is cited to show that designers are often unaware of the human limits to operating such systems. "However, as Perrow points out... Designers tend to believe that automatic controls reduce the need for operator intervention and errors, while operators frequently override or ignore such controls due to the constraints...". [95]

DISA has to assure the resolution of the role of human components of information assurance to properly protect the DII. There are generally three strategies for improving this situation:

- Automate more human functions
- Improve human performance
- Use redundancy for integrity.

It is generally beneficial to automate functions for enhanced reliability whenever automation enhances performance, reduces cost, or provides other desired benefits. Unfortunately, while the DoD spends a lot of money on enhancing automation for other tasks, one of the areas where automation is severely lacking is protection management A simple example is the lack of administrative tools in most timesharing computer systems. Systems administrators are expected to keep systems operating properly, and yet:

- There are typically millions of protection bits that have to be set properly to prevent disruption, and there are virtually no effective or supported tools to help set, validate, verify, or correct them. [92]

- The DoD requires systems administrators of many systems to examine audit trails daily for signs of abuse, but it is virtually impossible for people to detect intentional disruption by this process, and the time and effort consumed in this activity is quite substantial. [120] According to one report, audit records for a system with 7 users executing an average of 1 command per minute over a period of 6 hours results in 75 megabytes of audit data! [126]

- Current audit analysis requirements don't require real-time analysis or response. Even automated audit reduction tools are inadequate in today's environment if they cannot act in near real-time, because disruptions can spread through a network at a very high rate unless response times are very short. For example, one AT&T switching system will disrupt the local central office unless failures are detected and responded to within 1.5 seconds of their occurrence. [45]

- Local area network administration tools are just now emerging, and the few tools that are commercially available open unlimited opportunity for intentional disruption. Some of the most powerful tools for network analysis are available for free, and allow even an unsophisticated user to observe network packets. In most current LANs, this allows passwords to be observed as they are entered.

"Research has shown that performance of certain types of control room tasks increases if the operator has some knowledge of the functioning of the process." [96]

Improving human performance is most often tied to motivation, training, and education, and again, there is woefully little of this in the information assurance area. Educational institutions do not currently provide the necessary background to make training easy, [39] and existing training programs in information assurance are not widely incorporated in the military. These areas must be addressed if DISA is to provide information assurance for the DII.

3.4 Real-Time Prioritization Should Be Addressed

In order for the DII to react properly to malicious disruption, it must be able to prevent disruptions where possible, and detect and respond appropriately to disruptions when prevention is not possible. In plain terms, the operators of the DII must be able to manage the damage. During periods of substantial disruption, there are likely to be more tasks to perform than bandwidth available to perform them. In an economic model of a high demand, low supply situation, the value of services naturally increases, and usage decisions change to reflect the relative values.

DISA should prepare for Joint Chiefs of Staff (JCS) approval, an analogy to this economic theory for warfighting priorities so that, as the network manager, DISA can design a priority assessment and assurance scheme so that the value of information passed through the degraded DII is higher per bit than that passing though the non-degraded DII. The JCS needs to specify metrics for, assess value of, and assign priority to 'information as a function of value at that time and the DII must use these metrics to prioritize its behavior. A sound start in this area could be achieved by developing a military version of the commercially oriented "Guideline for Information Valuation." [104]

If the priority assessment scheme is not a fully automatic process, the DII may have a profound problem in reacting in a timely fashion. The first problem is that if people have to react, they are inherently limited in their reaction time. If the attack is automated, and peoples' reaction times limit the defense, it may be possible to design attacks that vary at a rate exceeding the human ability to respond. A knowledgeable attacker who understands reflexive control may exploit this to create further disruption by misleading the people into reflexive response, and exploiting those responses to further the attack. [103] A fully automatic response may have similar reflexive control problems except that it is potentially more predictable and normally far faster. This is where design flexibility must also come into play.

3.4.1 Priorities Should Be Properly Addressed Over Time and Circumstance

Information assurance issues must be flexibly prioritized and adapted as needed in order for the DII to behave properly over the range of operating and disrupted conditions. The metrics associated with information should be evaluated differently in different situations, and should include such factors as time, value, criticality, locality, and redundancy. Each of these values should have an effect on the manner in which the DII prioritizes activities, while each should be controlled by different mechanisms to assure that an attacker cannot circumvent a single mechanism and exploit this to dominate activities.

Even in the most dire of circumstances, unconditional preemption should not be the method of choice for prioritizing scarce services. The problem is that preemption results in service denial for the preempted, and if the assessment of priorities is not accurate, it may be highly desirable to apply some, albeit reduced, bandwidth toward all legitimate needs. It would be preferable to have a scheme whereby higher priorities have a higher probability of domination of resources at any given time, but over any significant period of time, even the lowest priority process has a reasonable expectation of some limited service. This concept is often called 'graceful degradation.'

3.4.2 Criticality of Function Should be Properly Addressed

A more fundamental issue that must be resolved is how to prioritize between the basic information assurance measures. If better to have wrong information than no information, then availability is more important than integrity. If it better to have no information than wrong information, then integrity is more important than availability. The former appears to be the case from a standpoint of infrastructure recovery, where even low integrity information may assist in service restoration. The latter appears to be more appropriate when making strategic or tactical decisions where a decision based on corrupt information can be fatal.

In most modern databases, it is a simple matter to make undetected modifications. Whereas an outage would be noticed and cause a response, and modern database techniques detect inconsistencies in a database, there is no protection provided -in most modem databases for erroneous data entered through the legitimate database mechanism or malicious modification by a knowledgeable attacker. Subtle corruption's typically produce a different sort of failure, such as a missile defense system detecting hostile missiles as friendly, or an airplane flipping upside down as it enters the southern hemisphere. In DoD logistics, command and control, and medical databases, such an error can not only be fatal, but can cause the DoD's automated information systems to be used as a weapon against it.

3.4.3 Priorities Should Interact Properly Across Components

Prioritization in the DII will involve both communication and computation, and the prioritization schemes must meld together in a suitable fashion across these boundaries. Furthermore, many of the computation components of DII will not be under the operational

control of DISA. For example, embedded systems interacting with the DII will have to interact in specific ways in order to assure that no mismatch occurs, and the DII will have to be able to deal effectively with intentional mismatches created to disrupt interaction between communication and computation resources.

Most current rietwork protection strategies are based on the concept that all of the systems in the network behave properly, and many local area network protocols are based on well behaved hardware devices and software products in all of the nodes. When connecting these networks to global systems, imperfectly matched protocols or processes can snowball causing widespread disruption. The priority assessment scheme must not be based on trusting the network components and must be designed to detect and react properly to limit the spread of network wide disruptions regardless of their specific characteristics. There are some theories for addressing protocol inconsistencies, but new basic understandings are needed at the process and infrastructure levels. DISA must promulgate standards that provide assurance based on the assumption of malicious components, and not based solely on lists of known attacks.

3.5 · DoD Components Should Train for Defensive Information Warfare

Information workers cannot be expected to react properly in combat unless they are properly prepared for defensive information warfare. ‘Ibis involves several key actions:

- DoD components must act in conjunction with DISA to develop proper policies and procedures, to define specific defensive information warfare tasks to be carried out, and to specify the manner in which they are to be performed.

- DoD components must train information workers in how to properly carry out their duties under stress, so that they are able to effitiently carry them out as required under “information warfare” battle conditions.

- DoD components must hold readiness drills and regular exercises so that the skills developed and honed in training do not decay with time.

- DoD components must hold war games in order to determine weaknesses in strategies and improve them over time.

In the long term, education and training for defensive information warfare must rest upon a well conceived, articulated, implemented, and tested body of strategy, doctrine, tactics, techniques, and procedures. In turn, this body of knowledge must be based, in large measure, on a fairly detailed knowledge of the offensive capabilities available to potential adversaries and the nature of possible attacks on the information infrastructure. In the short term, however, there are several actions that should be undertaken to mitigate disruptions of the information infrastructure.

As a first priority, DISA should make everyone associated with the operation, management, and maintenance of the DII familiar with the concept of information assurance and the nature of likely disruptions, and should undergo regular training and awareness drills to reinforce this training. Primary emphasis should be given to proper prevention, detection, differentiation, warning, response, recovery, analysis, and improvement.

The operators of the elements of the DII must be trained to consider, as a matter of course, the possibility that there are hostile disruptions being undertaken, and that the DoD is unaware of them. Without awareness, advanced training, and education, the human elements of the DII are unlikely to be able to detect attacks unless and until advanced technology-based warning enhancements are implemented. Even then, awareness, advanced training, and education play a vital role in installing, maintaining, and using the automation.

As a second priority, DISA should ensure the provision of similar training and awareness to DII users. While this training may be more narrow in scope, it is essential that the users of the DII be aware of the information assurance issues, how their function can be impacted by DII disruption, what they should do to avoid causing disruption, and what they should do in the event of disruption.

The Defense Agencies, CINCs, and Military Services should make extensive use of simulation capabilities in training individuals and units. This training should be reinforced through the conduct of frequent readiness drills and exercises. These drills and exercises may initially be conducted as stand-alone events, but must eventually be integrated into command post and field exercises involving the forces that use the information processed and disseminated by the DII.

DISA should undertake efforts to include information assurance in the curricula of technical and professional courses of instruction offered throughout the DoD. Information assurance should be embedded in all courses related to information systems, sciences, and management, and courses concentrating on information assurance should be 'offered as a part of the required curriculum for military students concentrating on computer or information science or engineering.

3.6 Information Assurance Impacts the National Information Infrastructure

Another area to which these results can be readily applied is the current effort to implement the NII. There is considerable overlap between the DII and the NII. Both depend in large part on the public switched telecommunications network and on the telecommunications and computer manufacturing sector. The primary difference is on focus; the DII is focused on the national security mission and the NII is focused on national economic progress, itself an element of national security.

'The benefits of the NII for the nation are immense. An advanced information infrastructure will enable US firms to compete and win in the global economy, generating good jobs for the American people and economic growth for the nation. As importantly, the NII can transform the lives of the American people - ameliorating the constraints of geography, disability, and economic

status giving all Americans a fair opportunity to go as far as their talents and ambitions will take them." [13] But this will only be true if the NII can get the right information to the right place at the right time. Recent studies have shown that US industries lose billions of dollars per year because of disruptions in their information systems, [14] [15] and the loss is increasing year by year.

'In addition, it is essential that the FEDERAL government work with the communications industry to reduce the vulnerability of the nation's information infrastructure. The NII must be designed and managed in a way that minimizes the impact of accident or sabotage. The system must also continue to function in the event of attack or catastrophic natural disaster." [13]

The US economy now depends for its very survival on the information infrastructure. With the inclusion of new services including national health care, access to state and local government information, financial records, and health records, under the promise of the NII, that dependence will grow.

As a nation, the US not only gets involved in military struggles with other nations, but with the emergence of a global economy, the US is in a constant economic struggle with the rest of the world. Even though economic opponents may not be as likely to use physically destructive methods to win the economic war, they already use information weapons against us, and are increasingly pursuing national policies to this end.

Many of the same techniques that will provide information assurance to the DII will be directly applied to the NII to help assure the availability and integrity of the national infrastructure. Just as standards for secrecy have promulgated to industry, it is likely that the standards for information assurance applied to the DII will become de-facto industry standards, and will have a positive impact on national competitiveness for many years to come.

3.7 Cost Factors Call for Selective Immediate Action

Without careful analysis, it would be easy to bankrupt the Department of Defense in an attempt to 'armor-plate' the DII with ad-hoc after-the-fact enhancements. For example, according to industry sources about 20% employee overhead is required for systems administration of integrity protection in a typical banking operation. If the DoD were to add 20% to all staff that use computers just to maintain integrity, the cost would run into billions of dollars per year, and this would not provide availability of services or cover the overall integrity of the DII. DISA should undertake a careful analysis to determine the cost-effectiveness of information assurance techniques on a class-by-class basis. This effort should be undertaken at the earliest possible time in order to afford the greatest cost savings.

There is a great deal of historical data that strongly supports the contention that the DoD should spend money on information assurance now rather than waiting until the DII is widely implemented and operational. Many experts in information protection indicate that after-the-fact protection is much less effective, much more expensive, rarely adequate, and hard to manage.

The data from several significant studies indicates that the costs associated with addressing information assurance now may be as much as several orders of magnitude less than addressing it once the integrated DII is widely operating. (See note '7)

Most DoD legacy systems were not designed to provide information assurance in an environment like the DIS. Substantial data supports the conclusion that the costs of retrofit for information integrity in most DoD legacy systems would be a factor of 100 more than it would have been during the original system specification. [37] This implies that for the same cost as providing information assurance to one legacy system, the DoD can provide information assurance to 100 systems of the same scale now in the specification phase. A conclusion of this study is that except in situations where a high cost retrofit is deemed vital or low-cost enhancements are possible, automated information assurance features should only be implemented by altering the specifications and designs of systems still in development, and by implementing network-based information assurance that can cover numerous legacy systems at reasonably low cost.

Under this plan, automated information assurance features would be phased in over a 5-10 year period, based on normal system replacement cycles. Substantial immediate improvement will be attained by implementing network-based protection features and training DoD'S information workers in defensive information warfare, and over the long term, information assurance will reach desired levels at reasonable cost. 'This time lag in technical enhancement will also give DISA time to sponsor much needed research and development that will lead to far better and more cost effective information assurance technologies than those available today.

As this study pointed out earlier, designing 'perfect' information assurance for the DII is infeasible. In the opposite extreme, providing minor information assurance enhancements can be quite inexpensive, even in legacy systems. For example, adding a cryptographic checksum to database records to assure that they have not been externally tampered with costs almost nothing, and substantially mitigates risks from all but the most serious attackers. An important subject for further study should be determining the 'knee point' in the cost vs. protection tradeoff for both legacy systems and systems still in the design phase. By doing this analysis, the DoD will be able to implement the most cost effective protections first, and only implement very expensive and marginally beneficial enhancements in cases where very high integrity and availability requirements are called for.

Based on these cost factors, it is the conclusion of this study that the most cost effective overall approach to providing information assurance in the DII will be for DISA to:

- Immediately create a minimum information assurance standard for systems currently beiig specified and designed, and work to improve that standard over time.

- Immediately support cost-analysis studies of classes of existing information assurance technologies and provide the results of these studies to designers as they become available.

- Support substantial research and development to improve design standards and create increasingly cost effective technologies for information assurance.

- Support the analysis of cost vs. protection tradeoffs for information assurance features, incorporating new research results as they become available.

- Promptly apply network-based tools and techniques to detect and respond to disruptions as they become available.

- Implement low-cost high-benefit information assurance features in legacy systems which lend themselves to these enhancements as suitable technologies become available and time and money permit.

- Plan on achieving overall DII information assurance commensurate with criticality over a 5-10 year period.

The cost to the US of a DII with inadequate information assurance that sustains significant battle damage in a war can be as high as military defeat. But the cost of implementing information assurance frivolously could bankrupt the nation. The DoD must make prudent financial decisions about information assurance, while implementing as much cost-effective protection as feasible over a reasonable period of time.

4 ACTIONITEMS

This study points out the many areas that have to be considered in order to achieve the level of information assurance required for the DII. Specifically, the following action items are critical, and to keep costs as low as possible, they should be pursued in all haste.

- DISA should take steps to ensure that information assurance is recognized and treated as a critical readiness issue: The DoD should make information assurance issues a more central component of its readiness evaluation process in order to get a realistic appreciation of its impact on the ability of the US military to prevail in conflict

- DISA should oversee the development of information assurance policy, doctrine, strategy, tactics, techniques, and procedures.

- Infrastructure design should be considered differently than systems design: DISA should support efforts to understand the differences between infrastructure design and standard information system design, and use these understandings to improve DII design decisions.

- DISA should ensure that existing technical and human vulnerabilities are addressed: The current situation is one where inadequately trained people operate inadequately protected equipment, and are unaware that attacks are taking or have taken place. This is a recipe for disaster, and it must be addressed to have any reasonable expectation of the availability or integrity of information that is critical to the defense of the nation.

- DISA should ensure that new standards, technologies, and tools to protect against disruption are developed: In the information age, information infrastructure will be the target of attacks just as industrial infrastructure was the target of attacks in the industrial age, and the information infrastructure of potential adversaries is already a primary target in US military doctrine. If the US military is to defend itself against this sort of attack, it must develop new standards for dealing with intentional disruption. The benefits of this will extend far beyond information warfare defense, and will ultimately make the US stronger as an economic force in the world, because in an economic war, the national information infrastructure is also a major target.

- DISA should recommend activities to strengthen top level technical management of information assurance: In order to deal with the problem of horizontal consistency and integration and to prevent unnecessary duplication, it is necessary to have top level technical management that considers and addresses the implications of interconnecting diverse information infrastructure components. Current management is essentially limited to addressing individual systems and their compliance with standards. This is inadequate and costly.

- DISA should sponsor the development of real-time control mechanisms to enhance information assurance: When disruption takes place, a unified, coordinated, management and operational control capability must be in place to detect attack, differentiate attack from accident or mischief, and warn the affected DoD components that an attack is underway, limit the spread of damage through responses, and manage the recovery process.

- DISA should create testing programs and assure that they are used to enhance information assurance: Current testing programs do not address disruption, and this is a root cause for the current inadequacies in this area. To this end, the DoD should establish a suitable clearinghouse mechanism to ensure the developers of these testing programs have a comprehensive technical understanding of the full range of offensive information warfare techniques that have been encountered or that have been postulated.

- DISA should ensure that flexible, automated, prioritized responses to disruption are implemented: In the current and anticipated information warfare environment, human reaction times are not adequate to make moment to moment decisions about the control of information in a global network, and even if they were, the decision processes are far too complex for people to do right.

- DISA should sponsor the reduction of information assurance knowledge to a usable and teachable form: This should include the creation of technical books and course materials, manuals for managers and operators, and other similar educational and training materials. As a high priority, these materials should be used to ensure that the architects, designers, and system engineers responsible for developing and fielding the component elements of the DII are trained in information assurance design principles and practices.

- DISA should provide training materials and requirements so that information workers can begin to train as defensive information warriors: The first line of defense today is the people operating and using the existing information systems, and they are inadequately prepared for information warfare. The DoD must begin in earnest to train its information workers in the area of information warfare, or they will continue to be inadequately prepared to handle the task at hand.

- DISA should work with the Joint Staff and the Joint Warfighting Center to ensure that readiness exercises and war games for defensive information warfare begin: Training alone is not enough. In order for training to be effective in a battle situation, readiness exercises must drive that training home. The DoD must train as it will fight so that it can fight as it trains. In the same way as readiness exercises prepare the warrior for tactical operation, war games prepare planners for strategic and doctrinal decision making. War games are a necessary component in the high level decision processes that will lead to long term success on the information battlefield.

5 NOTES

Note 1:

Let's look at what a typical text says on the subject: "The noise analysis of communications systems is customarily based on an idealized form of noise called 'white noise,' the power spectral density of which is independent of the operating frequency. The adjective 'white is used in the sense that white light contains equal amounts of all frequencies within the visible band of electromagnetic radiation.... " [35] 'The reason cited for the random noise models is the ease of analysis, [36] but ease and adequacy of analysis are not always compatible.

One of the most common techniques for detecting corruption in memory and transmission is the use of a 'parity' bit associated with each byte. The parity bit is set to 1 or 0 to make the total number of 'l's even (or odd, depending on whether the even or odd parity convention is being used). This technique detects ALL single bit errors, which is quite effective against particular sorts of random noise that cause transient faults. It is not effective against an intentional attacker who can change sets of bits collectively while maintaining parity, thus keeping the parity the same while corrupting the information and avoiding detection.

On disk storage, LAN packets, and in some satellite transmission, CRC (Cyclical Redundancy Check) codes are used to detect classes of faults that result in errors to linear sequences of bits of at most some pre-defined length. [29] Again, these codes are ineffective against an intentional attacker, because it is easy to determine the constant coefficients of the coding equations by watching packets, and from this it is easy to forge packets at will undetected. [39]

Note 2:

This work is essentially oriented toward designing a perfect system wherein all inputs, states, outputs, and state transitions are specified in full detail, and mathematical proofs are provided to show that the design is properly implemented. [30] [31] Although this type of solution may be applicable to certain limited control problems in embedded systems, these sorts of solutions are computationally infeasible for any large system, cover ONLY sufficiency and not necessity [49], only cover limited function systems against disruption, [39] and are beyond current and anticipated capabilities over the next 20 years for the sorts of systems desired in the DII.

An alternative path to a similar solution is the use of automated program generating programs. In this technology, a small number of programs are designed to automatically write the rest of the programs. Designers spend a-great deal of time and effort in perfecting the design automation system which, in turn, designs other systems. [32] This technology is far from perfected, and even if it were perfected, it leaves the problem of writing perfect specifications, which is at least as hard as writing a perfect programs.

In the hardware realm, design automation has been highly successful, but this does not imply that it will be successful in the software realm. There are substantial differences between hardware and software. For example, the complexity of current software is many orders of

magnitude higher than the most complex automated hardware design; the physical properties of hardware are abstracted out of most software design; software is designed based on a finite but unbounded randomly accessible space, while hardware is designed based on a relatively small finite and bound space with only local access as provided by explicitly created wires. Furthermore, hardware design automation takes substantial amounts of computer time, still leaves design flaws such as data dependencies that have resulted in disruption, and is based on specifications that are vulnerable to errors.

Another alternative is the use of extremely intensive testing to detect the presence of errors and correct them. The problem with this approach is that testing for 100 percent coverage is as complex as perfect design. Imperfect testing leaves systems that fail when 'rare' events occur. In one study, the combination of two events characterized as low probability caused 50 percent of systematically designed, well tested, small control programs to fail. [34] If this is the current state of the art for low probability events in small programs, extremes in testing are not likely to be successful against intentional attacks on large globally networked infrastructures.

Note 3:

Gateways, terminal servers, and routers are commonly used to control traffic in networked environments, and they are quite effective against random or accidental misrouting-routing of information, but in a hostile environment, they commonly fall prey to disruptive attacks. General purpose computers used as gateways are easily overwhelmed and corrupted* Terminal servers are commonly accessible by users logged into any computer in the network and can be altered to remove usage restrictions, connect users to wrong systems, or even lock out legitimate terminal server administrators. [41] Routers designed to control network traffic and prevent overloading in large networks are also easily bypassed by using the administrative mechanisms which permit remote control of the router or forgery of machine Identifications (IDs) with authorized access. [42]

The public telecommunications networks are a critical part of the current DII, and are likely to be a major component of the DII into the future, but they lack the information assurance features required for military operations. Service assurance features are designed into these systems at every level, [43] and yet they still fail to meet even the challenge of accidental errors and omissions. As an example, in 1991, there was a major failure in telephone switches in several large US cities that lasted for several days, and was finally traced to a 3 bit error (a 'D' instead of a '6') in one byte of a software upgrade. [93] This is the simple sort of mistake that even minimal software change control detects. This change was apparently never tested at all, was put into widespread uses and caused widespread harm. In 1990, AT&T's long distance network shut down due to a protocol error that impacted millions of customers nationwide for over four hours. [44]

In many cases, telecommunications disruptions must be resolved in very short timeframes. For example, some telephone switching systems must be repaired within 1.5 seconds or the circuit failure errors passing through the network will cause a propagating positive feedback which may

deadlock more of the network, [45] eventually cascading into a major problem An attacker only needs to disrupt two sites for 1.5 seconds to cause such a cascading effect.

One quarterly report of large scale disruption incidents for the fall of 1993 includes an Federal Aviation Administration (FAA) computer systems failure delaying regional traffic for 90 minutes (cause unknown), an FAA weather computer system failure for 12 hours due to a time activated logic bomb, a programming error in an X-ray system that resulted in wrong dosages to about 1,045 cancer patients, and a software 'bug' that crashed the Hamburg Integrated Services Digital Network (ISDN) telecommunications services for over 11 hours, and this is only one of several similar publications that report different incidents. [121]

Similar lapses in policies and procedures seem to be common for major software manufacturers. As an example, in 1992, Novell released a virus to tens of thousands of customers when it was noticed **after quality control was completed** that a key file was missing from the master distribution disks then being transported to the disk duplication facility. Instead of returning to the quality control process, the person transporting the disks for duplication loaded the file from the most convenient computer, which by chance contained a virus that was transferred to the floppy disk. The disk was sent to duplication, packaged, and shipped to customers. [46] The disks were apparently never tested at random after duplication for problems, the disks en-route to the duplication facility were not sealed or permanently write protected, the personnel were not properly trained, and the initial quality control process never detected that the correct file was not on the disk!

Note 4:

Five books on computer viruses, including two that are tutorials on writing viruses, discuss military use of this type of software. [73] [74] [75] [76] [77] A recent popular novel has the central theme of tippling attacks on US computers by means of viruses, computer terminal eavesdropping, high energy radio frequency 'guns,' and electromagnetic pulses. The author's virus examples are not as subtle or malicious as a real attack by experts. [78] An interactive movie on CD-ROM, released in October, 1993, illustrates information and infrastructure warfare against the US. It includes details about crippling and corrupting time standards, which affect precision weapon targeting and long distance telephone switches. [80]

The Chaos Computer Club in Germany, maintains an annotated list of the Internet addresses of US DoD command, control, supply, and logistics computers on one of their computer accounts in Germany. [89] Apparently selected from hundreds of publicly available military computer Internet addresses, listed systems are primarily Army, Navy and Air Force logistics, computer, communications, and research sites. This listing is not kept in publicly available bulletin boards throughout the world, but access to it was attained via an international connection. To demonstrate one possible utility of this list in attacking the DII, during this study two simple, safe, legal, and well controlled experiments were performed.

In the first experiment, e-mail was sent to the 'root' user at each of 68 sites chosen from the Chaos Computer Club listing in order to establish that mail sent to most of them would be received and stored in their computers. The following table describes the results:

Number	Response
10	refused the mail
1	no root user, identified self as 'TSO'
2	no such user ID, listed other user IDs
2	no user called 'root' on their system
7	not found by the mail system
6	got the mail - personal response
40	got the mail - no response

The second experiment consisted of sending mass quantities of mail into one site (done on an isolated computer designated for that purpose) to see how it affected operations. The first effect was a slight slowing of other processes on the system, presumably due to the disk writes and paging required to process and store all of the mail. The second effect was consumption of all available disk space in the '/usr' partition of the disk. The target system had about 18 megabytes of free space on that partition, and it took only 4.5 minutes to exhaust it, at which point the system started having severe problems because it could not create or add to files in that area. The system console indicated that no disk space was available on that disk partition.

It typically takes about 30 minutes to find the specific problem in such an incident (in this case, the file consuming all of the disk space) once the systems administrator is able to login to the system. On some systems, the administrator cannot login properly without adequate disk space, but either way, the net effect is a half an hour or more of denial of services, corruption, and repudiation. The lack of disk space causes many programs to fail, and if you are unable to write a file to disk, it is hard to do much useful work. Files being written when there is no space left typically end up in an inconsistent state. Most programs dealing with file input and output (IO) do not detect and properly handle these conditions, so the corruption goes unnoticed for the moment. The audit trails take disk space, and since there is none available, they cannot write. Depending on details of the implementation, the audit program may even stop operating entirely. After the problem is found, there is an even bigger problem How does the administrator prevent this attack and still allow legitimate mail to pass? It turns out that this is not so simple in most modern computer mail systems.

After posting this information to the 'risks' forum on the Internet, numerous replies asserted that this attack was not properly defended on existing systems. [90] One respondent pointed out that electronic FAX and news transmissions had similar problems, and are not adequately addressed by many current systems.

In 1993, the quarterly 'hacker' magazine 2600 had the following table of contents: [88]

Title	Subject
A Guide to the 5ESS	AT&T telephone switch
British Credit Holes	How to subvert and take over a person's credit and identity
High School Hacking	Breaking into high school administrative files
Meeting Advice	Frustration of law enforcement activities at hacker meetings
More Acronyms	Acronym Dictionary
Printable Letters	self explanatory
. AT&T Pages	AT&T Addresses
Government bulletin boards	bulletin board phone numbers
Video Review	Critiques of security training videos
2600 Marketplace	want/sale ads
Toll Fraud Device	Plans for a 'red box' to use on pay phones
2600 Meetings	hacker meetings .
ANSI Bomb	How to build a logic bomb for use on DOS machines

Note 5:

Standards usually involve many components, and this task order doesn't address standards per-se, but in the process of this work, some ideas that may be worth considering in future standards came up.

The first idea is that there should be information assurance labels associated with processes and objects, and that those labels should be used to make decisions about how to behave during operation.

As a trivial example, suppose we label information with an availability integer in the range of O-255, where 0 indicates the lowest priority and 255 indicates the highest priority. We attach this integer (stored as 1 byte of header information) to all processes, files, and packets used throughout the DII, thus creating a tagged architecture [125] reflecting this availability parameter. When decisions have to be made about which information is to pass through limited bandwidth, higher values are given higher probabilities. Similar labels can be associated with other factors, and rules can be made for the treatment of different values in different situations. The ability to interpret these sorts of rules can then be designed into systems, so that they automatically operate to reflect the rules, but are flexible enough to be programmed with new rules as design requirements change.

While this is only a trivial example of one element of a standard and how it could impact the ultimate operation of the DII, it points out the need and the value of creating an appropriate set of standards for information assurance requirements, and how doing this will directly impact the ultimate fulfillment of the information assurance goals in the DII. There is a precedent for this approach in the 'High Probability of Call Completion" standard developed for the public switched telephone networks in support of National Security and Emergency Preparedness (NS/EP)

telecommunications. This standard uses a "traveling class mark" to provide the capability for preemption of calls and other priority treatment for NS/EP calls within the network. [54]

. A second idea about standards for information assurance is that risk analysis for many other areas is fundamentally different than the techniques that apply to malicious disruption. Specifically, if an attacker knows how to disrupt a system, in most cases, the likelihood of success in an attack is 1. The probabilistic approach to analyzing defenses and attacks may not be appropriate for considering human agents with malicious intent. An alternative approach that has been tried with some success is a coverage approach in which we [illegible] techniques which cover different vulnerabilities for their coverage and costs, and provide a minimal cover for the desired level of redundancy. [122] 'Ibis optimizes costs for the specified goal but does not depend on assessing probabilities of attack, or expected losses.

A third idea about standards for information assurance relates to common mode failures and correlated events. [123] It seems that several major incidents per year involving common mode failure in redundant systems now occur, and there seems to be a strong correlation between these events and inadequate standards or capabilities for redundancy. The White Plains telephone cable incident in December of 1986 involved seven redundant circuit connections for the Advanced Research Projects Agency network (ARPAnet) intended to assure that no single (or multiple up to six) failure could disable the network connection. Unfortunately, the telephone company ended up routing all seven connections through the same optical fiber, and when that cable was cut, all seven redundant connections were disrupted.

It seems critical that redundant connections be explicitly specified in a manner that identifies them as redundant with respect to each other to all levels of implementation, and that mechanisms be put in place so that identified redundancies are implemented with redundant physical mechanisms at all levels. For example, a set of co-redundant telephone lines identified to the telecommunications provider should result in the routing of those lines through separate switching centers, switches, tunnels, pipes, cables, and wires.

A more stringent requirement might also demand that the redundant connections operate in different media, (i.e. fiber, metal, microwave, etc.) go through different hardware components controlled by different software (i.e. 3b2s running Unix, Intel based processors running OS/2, 68000 based processors running Apple System 7, etc.), and be controlled by different telecommunications providers.

The automation systems that control the implementation of telecommunications and other aspects of systems would likely have to be redesigned to reflect this change, since most current designs only address efficiency, and when efficiency is less important than resiliency, they tend to do the wrong thing.

The same principles that apply to telecommunications apply to all components of the DII. For example, the movement toward megacenters makes the risks associated with a megacenter failure more severe and thus dictates more consideration. For critical applications, there should be

separate and different implementations that share the same data between geographically diverse locations, and perform redundant processing using different techniques to assure that disruptions don't result in failure. Similarly backups must be performed and stored redundantly, (i.e. separately and differently) and must be tested by restoration into a separate and different environment to assure that they are free of defects.

Note 6:

In many cases where redundant input is required, it isn't exploited for error detection and correction, which is the worst of both worlds. An example may help clarify this point. In the US, postal zip codes directly imply the state. Why then ask for the state? For efficiency reasons, we should not! On the other hand, by asking for the state and zip code, we can detect inconsistency and act to correct the error before it creates a larger problem (e.g., sending a paycheck to the wrong place). In most current systems, we have the worst of both worlds. We ask for both zip code and state, but never compare them to find errors. Thus we have both extra data entry and inadequate coverage of errors.

Note 7:

Compared to finding and correcting problems in the analysis phase, the average cost of a change (i.e., correcting a software fault) according to one study is increased by a factor of 2.5 in design, 5 in testing, and 36 in system integration. [100] In another study of large high assurance software designs with high quality specifications and extensive testing, the cost impact of a change after a system is in operation is calculated to be 100 times the cost of a change during the specification phase. [37] The same study showed that the larger the system, the more cost advantage there was to making changes earlier, and for' similar sized systems, correlated to the factor of 36 given in the other study. According to one software engineering text (that we feel may be less reliable than the previous two extensive studies), the cost of fixing an error rises as more work is built upon that error before it is found and fixed. "The cost to catch a mistake and make a change at the time of writing the requirements specifications may be $10, and during the design $300. While the product is being built, the error may cost $3000; after the product has been delivered, the mistake could cost as much as $15,000 to fix, and possibly much more in losses to the client because the product didn't work." [101] The costs of extensive testing alone for high assurance can double the overall system costs [100] while producing little. advantage against malicious attacks.

Covering intentional disruption is a more stringent requirement than covering random events, but the costs of added coverage are not always substantial. The study of node destruction in a uniformly connected network demonstrated that a factor of 10 increase in the number of available links was required in some circumstances to withstand intentional attack to the same extent as random destruction. But that study was based on design assumptions that do not have to be true. [36] On the other end of the spectrum, cost analysis of fairly strong proactive integrity protection techniques proved more than a factor of 50 more cost effective over the lifecycle of a system than defenses based on a reactive approach to attacks (which most DoD sites have chosen for

protection against virus attack). [40] It appears that making early design decisions can save more than an order of magnitude in information assurance costs.

The potential cost differences between intentional and random disruption protection can reach a factor of at least 50 depending on early design decisions, and the costs of changes during system integration for large systems is on the order of 100 and increases with the size of the system. In the case of the DII, the overall system is more than an order of magnitude larger than the previous systems studied, which implies an even greater increase in the costs of making assurance enhancements later in the process.

It appears from the historical data that several orders of magnitude in savings may be attained by making proper information assurance decisions early in the process, but perhaps more realistically, we will not be able to afford adequate information assurance unless we design it into the DII from the start.

Another issue in cost analysis that must be considered is the difference between life-cycle costs and procurement costs. Perhaps no area demonstrates the lack of attention to this difference more clearly today than the area of computer virus defenses. Many DoD elements have purchased virus scanning programs as a defense against computer viruses on the basis that the cost per system is only about a dollar. Unfortunately, this is only the purchase cost and not the usage cost. The factor of 50 cost increase described above represents the difference between using a virus scanner every day and using a more cost effective protection technique. [40] The cost of the scanner may be only $1 per year, but the two or more minutes per day consumed by performing scans at system startup brings the lost time to over 600 minutes (10 hours) per system per year. Even at only $10 per hour of downtime, the costs of using the scanner are 100 times more that the cost of purchase in this example. Other factors in virus scanners make them far more expensive to use than alternative technologies, and more recent analytical results show that using imperfect scanners (which all scanners are) may lead to the spread of harder to detect viruses just as the use of antibiotics have led to the so called 'superbugs' which resist antibiotics. [39]

Note 8:

- Protection of individual devices operating point-to-point is well within modem technology, but the overall end-to-end communication requirement is far more complex. Most commercial networks have little or no coverage against intentional disruption and commonly fail from software errors, mischievous, and malicious attacks- [94] [44] [38] [54]

- 95 percent of DoD telecommunications capability is provided by public networks owned and operated by common carriers. [1 10] These are the same networks that will be used in the National Information Infrastructure (NII). [10]

- DISA's current plan has no specific contingency for providing information assurance under conditions of substantial disruption or in the presence of substantial battle damage. [55]

Note 9:

Major concerns about network assurance come from several sources. The listing below is incomplete, but worth considering.

- Current network management infonnation assurance standards are incomplete, and have only addressed authentication requirements. [56]

- The Government Network Management Profile's (GNMP) primary goal is to develop interoperable products [56] to allow network managers to remotely monitor and control network resources residing on network components developed by different vendors. This interoperability goal makes the network management system vulnerable to disruption, and from that location, the entire network could potentially be disrupted.

- The consolidation of the DISN network management into 'a hierarchical network management system was originally designed to make it possible for a network management center in one domain to 'cut through,' monitor, and directly control another domain. This could potentially be done without the authority or knowledge of any intervening network managers despite the authentication between sites. [57] Unless specifically addressed, this may allow a single attacker to disrupt the whole network. [58] More recent designs have moved toward a system of centralized monitoring and decentralized control via authenticated messaging to vendor-supplied data centers.

- The DISN network management center software will be made up of COTS products. [59] While this is the lowest initial cost approach, it also provides potential enemies with the opportunity to procure low-cost, readily available network management products that. are compatible with, and capable of functioning as, a network manager for DISN communication elements. This allows them to experiment with and practice attacks until they are perfected before launching them against the DII.

- Current network assurance standards only address authentication. [62] This is inadequate.

- The Government Open System Interconnection Profile (GOSIP) specifies standards that provide interoperability in a heterogeneous environment This interoperability of network services will provide the ability to disrupt and simultaneously damage services from any location in the network unless we specifically design information assurance features into the system

- There is no current plan for creating a separate and different network management capability that can operate when the network itself is not functioning. This lack of external control capability has historically proven inadequate, as the Internet virus of 1988 clearly demonstrated. [64] [65]

- Current network management systems typically address known faults in known ways. [97] Some systems recover from high probability errors, [98] while others detect and recover from large numbers of CRC errors, [99] but intentional attack is simply not treated in the available literature.

Note 10:

- The nature of a worldwide ubiquitous network could allow an opponent the ability to launch attacks over the wire on the DII without going "behind enemy lines." For instances a terrorist group could attack the DII by gaining access to the global network through a third nation's public network.

- The availability of open system technology and COTS products makes attack inexpensive. A well funded, determined military or civilian organization could easily purchase products and use them at their leisure to find flaws in the COTS products and test attacks before launch.

- The risks can be very low, since a failed DII attack does not commit many troops or resources or have to be followed up by a hot war, while a successful DII attack makes hot war much more likely to succeed.

- The reprisals the US can take against a DII attack may be limited. It may be hard to identify the attacker or even the location from which the attack was launched, and even if attackers were found, what could the US claim as damages without revealing DII weaknesses to the world? What would a proportionate response be? How would the US justify its response to its citizens and the rest of the world?

- A large low-tech military that could disrupt the DII could eliminate the US information advantage and thus greatly reduce the DoD's ability to act as a joint force.

- An attack on the DII would provide the attacker the advantage of surprise. To eliminate us from an engagement, the attacker first disrupts the DII, and then uses a conventional attack to achieve their objective. Since DoD response is so highly dependent on information capabilities, we might be partially or completely blinded and paralyzed.

- The deterrent and/or delaying effect of a preemptive strike against the DII by one country aggressing against another may give the aggressor enough time to consolidate a position and keep the US out of the fray.

- "...any sensible enemy will focus his most urgent efforts on countermeasures meant to neutralize whatever opposing device seems most dangerous at the time." [114](pp 27-28)

Note 11:

A number of countries have computer security groups, and some of these are working to certify operating systems, hardware, and software. This demonstrates that these countries are working to discover flaws in existing COTS products, and that these countries are aware of specific techniques by which these systems can be disrupted. European participants in Information Technology Security Evaluation Criteria (ITSEC) include England, Netherlands, France, and Germany, [38](app E, p283.) with Italy beginning to join in. Russia, Japan, China, Australia, New Zealand, Singapore and South Africa are also countries with certification and/or active computer security interest.

A number of countries participate in the world market for telephone and data switching systems, and can be assumed to have the knowledge to disrupt telephone and data networks based on their design, manufacturing and deployment expertise. Companies marketing Private Branch Exchange (PBX) or Central Office (CO) equipment in the US and elsewhere include Hitachi, Nippon Electric Company (NEC) and Fujitsu (Japan), Ericsson (Sweden), Alcatel (France), and Siemens (Germany). [85] The DII may depend on systems from these manufacturers for information assurance.

One paper published in 1989 compares computer viruses to traditional electronic counter measures and states that computer viruses are uniquely qualified to disrupt tactical operations; that several recent trends in military electronic systems make them more vulnerable, including standard computers, software, and data links, and that protective measures must be initiated before viruses are used by an adversary. [47]

Limited direct evidence exists for associating virus discovery locations with virus origins (e.g., language particulars, programming styles) and there is a substantial body of indirect evidence in the form of discovery location statistics that suggests that disruption technology and expertise exists in many nations. One study associating virus discoveries with countries gave the following results:

Country	Virus Discoveries	Country	Virus Discoveries
Former USSR	76	Canada	23
united states	68	England	22
Bulgaria	61	Taiwan	16
Poland	38	Sweden	16
Germany	30	Israel	15
Netherlands	26	Spain	14
Italy	23	Australia	14

From 3-10 viruses were first discovered in Argentina, Austria, Finland, France, Greece, Hungary, India, Indonesia, Malaysia, New Zealand, Portugal, Republic of South Africa, Switzerland, and Turkey. [82]

Vendors of anti-virus software normally have detailed knowledge of computer operations and large collections of viruses to study. Anti-virus software vendors are in place in the US(5), Israel(3), United Kingdom(3), New Zealand(3), Holland(3), Australia(3), Thailand, Iceland, Canada, Colombia, Sweden, and Ukraine. [83]

Another indicator is the countries of residence of speakers at the "International Computer Virus and Security Conference," held in New York City each March. In 1992, technical talks were given by representatives from Germany(3), Bulgaria, Belgium, England(2), Iceland, Russia, Australia, Mexico, and Israel. [84] Authors of anti-virus hardware and software can also be found in China, India, Taiwan, Japan, Malaysia, several CIS (the former Soviet Union) countries, and others.

It is clear from computer virus information alone, that many countries of security interest to the US have knowledge and technology in the computer virus arena that could be directed specifically to disrupt the DII.

In one recent paper, over 30 countries are given excellent ratings in computer-communications espionage, meaning they almost certainly have sufficient expertise to corrupt computer and network data and disrupt operations. Among these countries are India, Taiwan, Republic of Korea, China, Japan, and South Africa. [86]

A talk by Wayne Madsen presented at IFIP SEC '90 (International Federation of Information Processing Societies Annual Computer Security Conference in Finland) in 1990 provided a rating of various countries' ability to engage in computer 'hacking,' and the information that intelligence services were apparently becoming engaged in economic intelligence for business organizations. [87]

Project Rehab, operated by Germany beginning in 1988, is a computer and network intrusion research effort which has accessed computer systems in the US and other countries. The project depends on 'hacker' techniques and other research, and has approximately 36 computer specialists and senior intelligence officials assigned. A primary focus is on cataloging network addresses and establishing pathways for later use. [87]

More details regarding potential adversaries and their capabilities would be helpful in performing assessments in this area, but that is beyond the scope of this effort.

Note 12:

In many cases, disruption is not detected at all. For example, in over 100 legitimate computer virus experiments, no user has ever noticed the presence of a computer virus. [39]

The vast majority of known information system attacks were first detected by attentive users noticing unusual behavior. This is widely known in the computer security community and is supported by virtually every source that discusses the issue. For example, over 2,000 computer viruses have been detected in the last 2 years by the research community, and almost all of them were detected by users noticing anomalies. The Internet virus of 1988 was detected when users noticed dramatic network slowdowns. [64] [65] Hundreds of other failures in national telecommunications networks and individual systems are first detected by user complaints. [94] [38] [54] In major bank frauds involving electronic funds transfers, it is common for the first detection to be at the next bank audit, typically several months later.

Indirection between cause and effect dramatically increases the time required to track an attack to the source. Whereas total denial of services to an entire system is generally noticed quickly and total denial of services to an infrastructure is widely noticed almost right away, business disruption caused by subtle denial of services or corruption may be far harder to detect and associate with a cause. For example, suppose a disruption in the form of subtle denial of services caused orders placed for certain replacement parts to be ignored by the output routines in the order fulfillment subsystem in the supply and logistics system Orders would be placed, and the computer would indicate that the orders had been processed and shipped, but no shipments would arrive. Similarly, disruption in the form of subtle corruption could transform airplane engine part numbers into similar part numbers indicating different components, perhaps canteen cups. The order would be processed, but the resulting shipment would contain the wrong parts. It would probably be blamed on a data entry error, and if it only happened 10% of the time, the cause might go unnoticed for a long time.

Another subtle disruption approach is to slowly increase the level of denial of services over time so that the operators become acclimated to the slower and slower pace over a long period of time.

Differentiating natural disaster from other causes is generally not too difficult because natural disasters are easily detected on any wide scale. Differentiating accident from mischief from malice is yet another problem. The Internet virus was apparently an accident, and yet clearly many believe it was mischief and a few still believe it was malicious. Many disruptions are treated as accidental to avoid investigation. Almost no current organization has a way to tell one sort of disruption from another.

Limiting damage often takes too long to be effective. In the case of the International Business Machines (IBM) Christmas card virus of 1987, several days after the attack was launched, it was widely noticed, and over the next several days, IBM staff members tried unsuccessfully to disconnect their internal networks from the global networks. [108] [39] A defense against the Internet virus was only devised after over a full day of effort by people nationwide, and implementation of the work-around took several days. [64] [65]

Recovery is sometimes impossible, while in other cases it takes from days to weeks. For example, a company in Germany was the subject of extortion from a hacker (1988-89), who showed them a few lines of program code which would have caused the gradual corruption of all inventory records. They did not find the altered code for several weeks. [53] The Chicago telephone center fire in 1989 took months to recover from, and tens of thousands of customers were without service for extended periods. [38]

If the recovery process is improperly performed, many other problems can result. Audit trails may be lost thus preventing accurate determination of cause. The 'recovered' system may be more vulnerable to disruption than the original. The recovery process may itself cause disruptions.

Note 13: .

It may seem contradictory that efficiency and effectiveness do not always act in concert, but there is a very strong case to be made for introducing inefficiency into systems in order to make them more effective, particularly against disruptions.

- The entire field of fault tolerant computing, for example, is based on introducing redundancy of various sorts into otherwise more efficient systems in order to reduce the impact of accidental corruption.

- The adaptive file compression techniques commonly used in modem personal computers reduce space consumption, but if a single bit is in error, decompression will be unable to recover the remainder of the file accurately.

In war, efficiency is even more counter to effectiveness, especially in the area of technology. It is precisely the standards we use to make technology efficient that make it easy to. attack. [112](pp 316-320)

Note 14:

Based on observations made during this study, the authors believe that response to attacks is characterized by thresholds of detection and response capacity.

By lowering thresholds of detection, the defender is likely to detect more attacks, but the number and likelihood of false positives will also increase, and so will the cost of responding to the relatively minor incidents. By increasing the threshold of detection, response resources may be concentrated on the most important incidents, but a small incident with widespread impact may not be noticed until the damage becomes severe.

This leads to the issue of attack and defense. Given the option of a directed attack against a specific target or a more general attack which increases the overall 'noise' level, the threshold scheme employed for defense has a substantial impact on the optimal attack decision. It is always

possible for an attacker to remain below the threshold of detection for any imperfect detection system, so a tied threshold system leaves the defender open to noise-based attack. Similarly a substantial directed attack will sound off any capable detection system and generate a response, but it may also be possible to create the appearance of substantial attacking order to force the defender to respond more strongly than necessary, this creating an environment where the defender constantly 'cries wolf'. In either situation, a fixed response level is easily exploited, so a flexible and adaptive response is necessary in order to be effective.

In addition to detection thresholds, there is a response capacity inherently limited by the available response resources. In a human-based response system such as the one currently in place in the DoD, response time lags further and further behind as the number of incidents increase, eventually leading to a situation where important attacks are not noticed for a substantial amount of time. Increasing human resources is quite expensive and is only effective when the level of attack warrants the number of respondents. It takes a long time to train experts in this field, and there are relatively few of experts available and woefully few places where new experts can be trained.

An attacker can alternatively create and not create attacks SO as to force a defender to waste resources with an overblown defensive capability, or an attacker can use attacks to determine response characteristics and work out ways to overwhelm the defense.

This area is particularly amenable to analysis based on reflexive control. To form a strong defense, the flexibility must be designed so as to prevent this sort of analysis.

Note 15:

Physical attacks are widely varied and cannot be adequately covered here, but certain recent technologies are particularly important to understanding the nature and scope of emerging physical threats.

Cars parked about 300 meters from an electromagnetic pulse (EMP) generator test had coils, alternators, and other controls disabled. The former Soviet Union developed an EMP weapon before its breakup, and nuclear EMP hardening has proven ineffective against this weapon. [129] In the US, a Los Alamos EMP generator produced a 12-16 million amp pulse, with a rise time of 400 nanoseconds. Some 16 X 40 inch generators have produced about 30 million amps of current. [130]

FAA Federal Aviation Administration measurements at one high density US airport peaked at 14,000 volts per meter from surveillance and satellite tracking radars. The FAA set a 200 v/meter no adverse effects limit for one aircraft, partly due to rapid movement of both aircraft and radar beam [131]

The Ground Wave Emergency Network is the only US strategic defense communications system hardened to survive a high-altitude electromagnetic pulse (HEMP). [132]

There is some difficulty in deciding whether enough shielding has been used against electromagnetic interference (EMI). EMI was suspected in Army Blackhawk helicopter crashes, since the Navy version has more shielding and fewer crashes. [133]

In an extreme example, one US patent describes a means and method for altering noise levels which is capable of disrupting atmospheric communications over vast areas of the Earth. Experiments performed in Alaska and elsewhere appear to demonstrate the ability to disrupt all ground-based , airborne, and space-based communications using signals transmitted through the air. [134]

6 ACRONYMS

ADP	Automatic Data Processing
AIS	Automated information Systems
ANSI	American National Standards Institute
ARP Anet	Advance Research Projects Agency network
AT&T	American Telephone and Telegraph
C3I	Command, Control, Communications, and Intelligence
CD ROM	Compact Disk - Read Only Memory
CENTCOM	United States Central Command
CERT	Computer Emergency Response Team
CINC	Commander-in-Chief
CIS	Commonwealth of Independent States
CJCS	Chairman of the Joint Chiefs of Staff
c o	Central Office
COTS	commercial off-the-shelf
CRC	Cyclical Redundancy Check
DEC	Digital Equipment Corporation
DII	Defense Information Infrastructure
DISN	Defense Information Systems Network
DITSO	Defense Information Technology Services Organization
DoD	Department of Defense
DOS	Disk Operating System
DSS	DISN Switched Services
FAA	Federal Aviation Administration
GNMP	Government Network Management Profile
GOSIP	Government Open System Interconnection Profile
GOT	Government off-the-shelf
H-P	Hewlett - Packard
IBM	International Business Machines
ID	Identification
IEEE	Institute of Electrical and Electronic Engineers
IFIP SEC '90	International Federation of Information Processing Societies Annual Computer Security Conference in Finland
INMS	Integrated Network Management System
IO	file output and input .
ISDN	Integrated Services Digital Network
IS0	International Standards Organization
ISSA	Information Systems Security Association
ITSEC	Information Technology Security Evaluation Criteria
JCS	Joint Chiefs of Staff
MIL-STD	Military Standard
MOP	Memorandum of Policy
NEC	Nippon Electric Company

NII	National Information Infrastructure
NIST	National Institute of Standards and Technology
NMSD	National Military Strategy Document
NS/EP	National Security and Emergency Preparedness
OS	Operating System
OSD	Office of the Secretary of Defense
OSE	Open Systems Environment
OSF	Open Software Foundation
oss	Operational Support System
PBX	Private Branch Exchange
POSIX	Portable Operating System Interface Exchange
Pub	Publication
RFI	Request for Information
SAIC	Science Application International Corporation
SEW	Space and Electronic Warfare
SONATA	See Glossary
TSO	Technical System Officer
u s	United States
WCCS	Wing Command and Control System
WWMCCS	Worldwide Military Command and Control System

7 GLOSSARY

Access Control
A means of preventing the unauthorized use of a resource or the use of a resource in an unauthorized manner.

Accountability
The property that enables activities on an automated information system to be traced to individuals who may then be held responsible for their actions.

Assurance
1. The act of assuring or the condition of being assured....
2. A statement of indication that inspire confidence...; guarantee....
3 a. Freedom from doubt. ..,, b. Self-confidence . . . .
4. Boldness.... [135]

Assure
1. To inform confidently, with a view to removing doubt...
2. To cause to feel sure; convince....
3. To give confidence to; reassure....
4. To make certain....” [135]

Authenticate
To establish the validity of a claimed identity.

Availability of Services
An assured level of service, capacity, quality, timeliness, and reliability.

Corruption of Information
The opposite of information integrity.

Data Integrity
1. The state that exists when data is unchanged from its source and has not been accidentally or maliciously modified, altered, or destroyed.
2. The state that exists when computerized data is the same as that in the source documents and has not been exposed to accidental or malicious alteration or destruction.

Defense Information Infrastructure (DII)
The Defense Information Infrastructure is the worldwide aggregation of mobile and fixed DoD information systems organized to provide collection, production, storage, dissemination, and display of information.

Denial of Services
The opposite of availability of services.

Disruption
1. Denial of service or corruption of information resulting from a single event, cause, or source; whether direct or indirect, accidental or intentional, rare or common.
2. Uncertainty - denial of services, information corruption.

Heterogeneous Networks
Networks composed of hardware and software from multiple vendors usually implementing multiple protocols.

Information
Knowledge such as facts, data, or opinions, including numerical, graphic, or narrative forms, whether oral or maintained in any medium.

Information Assurance
The availability of services and information integrity.

Information Integrity
Complete, sound, unaltered, and unimpaired information.

Information System
The organized collection, processing, transmission, and dissemination of information in accordance with defined procedures, whether automated or manual.

Infrastructure
The basic personnel, facilities, equipment, procedures, and installations needed for the function of a system, network, or integrated networks.

Integrity
1. Strict personal honesty and independence....
2. Completeness; unity....
3. The state of being unimpaired; soundness.... [135]

Legacy
Existing.

Open Systems
A system which can be interconnected to others according to established standards. Systems which use stable, publicly-defined, vendor-independent interfaces and allow interoperation between various computers, regardless of make or model. Current examples include AT&T Unix, Open Software Foundation (DEC, H-P, and IBM) OSF/1, POSIX, and GOSIP.

Precedence

A rank ordering assigned to indicate the degree of preference given in processing and protecting communications traffic.

SONATA

US Navy articulation of three themes (global perspective, *The Copernicus Architecture, and* conventional wisdom of the future at birth) for the Navy to succeed in the Information Age.

Stovepiped Systems

Vertically integrated systems that perform the whole range of functions required for a particular application.

8 REFERENCES

[1] Joint Pub 1, "Joint Warfare of the US Armed Forces," Nov. 11, 1991, p57.

[2] ". . .FROM THE SEA: Preparing the Naval Service for the 21st Century," Sept. 1992.

[3] "SONATA" COP-094 booklet] SEW designated by the Chief of Naval Operations as a Navy warfare mission in 1989.

[4] "Army Enterprise Strategy: The Vision," April, 1993.

[5] Testimony of Gen. Charles A. Homer, Commander, Air Force Sapce Command, before the Senate Appropriations Committee Defense Subcommittee, May 26,1993.

[6] DISA, "The Defense Information Infrastructure Architectural Guidance," Draft, February 1, 1993.

[7] DISA, "Defense Information System Network (DISN) Architecture," (Coordination Draft), May 12, 1993.

[8] Alan D. Campen, ed. "The First Information War" AFCEA International Press, 1992.

[9] Lt. Leo S. Mackay, "Naval Aviation, Information, and the Future," Naval War College Review, Vol. XLV, #2, sequence 338, spring 1992

[10] 'National Military Strategy Document" (NMSD) FY 1994-1999, Annex C (Command, Control, Communications, and Computer Systems).

[11] Defense Management Report Decision 918, Defense Information Infrastructure, September 1992.

[12] The Bottom Up Review of the US DoD, 1993.

[13] R. H. Brown, Chair, The "National Information Infrastructure Agenda for Action," Information Infrastructure Task Force, September 15,1993.

[14] Melinda-Carol Ballou, "Survey Pegs Computer Downtime costs at S4 Billion," Computerworld, August 10, 1992, p53

[15] Barton Crockett, "Manhattan Blackout Cripples User Nets," Network World, 8-20-90,p1

[16] Karen D. Loch, Houston H. Carr, and Merrill E. Warkentin, "Threats to Information Systems: Today's Reality, Yesterday's Understanding," MIS Quarterly, June 1992, ppl73-186.

[17] Mary E. Thyfault, Stephanie Stahlwith, and Joseph C. Panetteri, "Weak Links," Information Week, August 10,1992, pp26-31

[18] Bob Violino and Joseph C. Panetteri, "Tempting Fate," Information Week, October 4, 1993 pp42-52.

[19] David Kahn, "The Codebreakers," Macmillan, 1967 p266.

[20] F. Cohen, "Information Warfare Considerations," SAIC's Strategic Assessment Center under a contract for OSD/Net Assessment's study on Information Warfare.

[21] Tofler, Alvin and Heidi, "War, Wealth, and a New Era in History," World Monitor, May 1991.

[22] C. Powell, "C4I for the Warrior," June 12, 1992

[23] CJCS MOP 30, "Command and Control Warfare," March 8, 1993.

[24] D. Clark and D. Wilson, "A Comparison of Commercial and Military Computer Security Policies," Proc. IEEE Symp. on Security and Privacy, Oakland, CA, April, 1987, ppl84-194

[25] "BOC Notes on the LEC Networks- 1990," SR-TSV-002275, Bellcore, Issue 1, March 1991
[26] NCSD 3-8, "Provisioning of Emergency Power in Support of NS/EP Telecommunications," April 2,199 1
[27] MIL-HDBK-419, "Grounding, Bonding, and Shielding for Electronic Equipment and Facilities," V2, January 2 1, 1982.
[28] RS-252-A, "Standard Microwave Transmission Systems," Electronic Industries Association, 1972
[29] IS0 IS 8208, "Information Processing Systems-Data Communications-X.25 Packet Layer Protocol for Data Transmission"
[30] "Safety Criteria and Model for Mission-Critical Embedded Software Systems," IEEE CH30338/91/0000-0069, 1991.
[31] H. 0. Lubbes, "High Assurance Computing Software Technology Requirements," COMPASS 91 (Proceedings of the Sixth Annual Conference on Computer Assurance: System Integrity, Software Safety, and Process Security), pp87-88, IEEE, 1991.
[32] Daniel P. Siewiorek, M. Y. Hsiao, David Rennels, James Gray, and Thomas Williams, "Ultradependable Architectures," Annual Review of Computer Science 1990 4:503-15.
[33] Jim Gray and Daniel P. Siewiorek, "High-Availability Computer Systems," IEEE Computer, September, 1991 pp39-48.
[34] Herbert Hecht, "Rare Conditions-An Important Cause of Faults," IEEE 0-7803-1251-1/93,1993.
[35] S. Haykin, "Communication Systems," J. Wiley & Sons, Inc., 2nd ed., c1983.
[36] D. Minoli, "Cost Implications of Survivability of Terrestrial Networks Under Malicious Failure," IEEE Transactions on Communications, V28#9, September, 1980, ppl668-1674.
[37] Barry W. Boellm, "Software Engineering Economics," Prentice Hall, 1981.
[38] "Computers at Risk: Safe Computing in the Information Age," National Research Council, National Academy Press, 1991.
[39] F. Cohen. "A Short Course on Computer Viruses," 2nd edition, John Wiley and Sons, 1994.
[40] F. Cohen, "A Cost Analysis of Typical Computer Viruses and Defenses," IFIP-TC-ll, Computers and Security, 1991.
[41] Some unpublished results of a small study by F. Cohen, 1993.
[42] Many administrators have found and reported examples of this, and some unpublished experiments by F. Cohen and S. Mishra at Queensland University of Technology, Brisbane, Australia, in 1992 confirmed these results.
[43] W. Falconer, "Service Assurance in Modern Telecommunications Networks," IEEE Communications Magazine, June, 1990
[44] M. Alexander, "Computing Infosecurity's Top 10 Events," Infosecurity News, Sept/Oct 1993.
[45] Bob Pekarske, "Restoration in a flash-using DS3 cross-connects," Telephony, September 10,1990.
[46] R. Lefkon ed., "Data Processing Management Association Annual Computer Virus and Security Conference," New York, NY, 1992.

[47] Myron L. Cramer and Stephen R. Pratt, "Computer Virus Countermeasures-A New Type of Electronic Warfare" Defense Electronics, October, 1989.
[48] Scott A. Boorman and Dr. Paul R. Levitt, "Software Warfare and Algorithm Sabotage" Signal, May, 1988.
[49] F. Cohen, "Computer Virus," PhD Dissertation, University of Southern California, 1985, ASP Press.
[50] B. W. Lampson, "A Note on the Confinement Problem," Communications of the ACM V16(10) pp613-615, October, 1973.
[51] Robery Molloy and Raja Parasuraman, "Monitoring Automation Failures: Effects of Automation Reliability and Task Complexity," Proc Human Factors Society, Annual Meeting, 1992.
[52] F. Cohen, "Computer Viruses-Theory and Experiments," IFIP-TC11 Conference, Toronto, 1984
[53] Ronald D. Ginn, "Continuity Planning," Elsevier, 1989, p9.
[54] "Growing Vulnerability of the Public Switched Networks: Implications for National Security Emergency Preparedness," National Research Council, National Academy Press, 1989.
[55] DISA, Instruction 630-230-19, "Security Requirements for Automated Information Systems (AIS)," August, 1991
[56] NIST, Government Network Management Profile (GNMP), Version 1, December 14, 1992.
[57] DoD, MIL-STD-2045-3800, Network Management for DoD Communications (Draft), January 4, 1993.
[58] OSD(C3I) Letter, "Review of Multilevel Security Capabilities," October 25,1992.
[59] DISA, Draft Specification/Statement of Work for the Integrated Network Management Systems (INMS) Program, August 31, 1992.
[60] DISA, "DISN Concept of Operations," (Coordinating Draft), August 2,1993.
[61] DISA, "DISN Security Policy," Draft, March 18,1993.
[62] NIST, 'The Industry/Government Open System Specification," (Draft) January 1993.
[63] DISA, DISN and DISN Switched Services (DSS) Request for Information (RFI), February 12,1992.
[64] E. Spafford, "Crisis and Aftermath," Communications of the Association for Computing Machinery, V32#6, June, 1989.
[65] J. Rochlis and M. Eichin, 'With Microscope and Tweezers: The Worm from MIT's Perspective," Communications of the Association for Computing Machinery, V32#6, June 1989.
[66] F. Cohen, "Protection and Administration of Information Networks Under Partial Orderings," IFIPTCll Computers and Security, V6(1987) pp118-128.
[67] F. Cohen, "Design and Administration of Distributed and Hierarchical Information Networks Under Partial Orderings," IFIP-TCll Computers and Security, V6(1987)
[68] "Open Systems Environment (OSE) Profile for Imminent Acquisitions (Part 10 of 10 parts) Security Services," - Draft.
[69] R. Ernest Dupuy and Trevor N. Dupuy, "The Encyclopedia of Military History," Harper and Row, 1970,p1021, doctrine, p1093 Schweinfurt Raid

[70] Sir Peter Anson and Dennis Cummings,p125 of 'The First Information War," 'The First Space War: The Contribution of Satellites to the Gulf War'
[71] Jean M. Slupik, p148 of "The First Information War," 'Integrating Tactical and Strategic switching
[72] Merrill L. Pierce, Jr., p153, "The First Information War," 'Established Architecture Keys Marine Data'
[73] Lance J. Hoffman, ed. "Rogue Programs: Viruses, Worms, and Trojan Horses," VNR, 1990
[74] Mark Ludwig, "The Little Black Book of Computer Viruses," American Eagle Publications, 1991
[75] John McAfee and Cohn Haynes, "Computer Viruses, Worms, Data Diddlers, Killer Programs, and Other Threats to Your System," St. Martin's Press, 1989
[76] Ralf Burger, "Computer Viruses-a high tech disease," Abacus, 1988
[77] David Ferbrache, "A Pathology of Computer Viruses," Springer-Verlag, 1992
[78] Winn Schwartau, "Terminal Compromise," InterPact Press, 199 1. also available via Internet
[79] Wired Magazine, "Top Ten US Infrastructure Targets," Nov, 1993.
[80] "Soft Kill," (Interactive CD-ROM), Xiphias, 1993.
[81] Robert D. Steele, "War and Peace in the Age of Information," Superintendent's Guest Lecture, Naval Postgraduate School, August, 1993
[82] C. Preston, "Computer Virus Protection," 1993, pp9-6.
[83] Robert M. Slade, "Antiviral Contact List," (computer file) 1993
[84] "Secure Networks"-Proceedings of the Fifth International Computer Virus and Security Conference, March 1993
[85] Data communications trade magazines.
[86] Wayne Madsen, "The Intelligence Agency threat to Data Privacy and Security," pending publication in The Journal of Intelligence and Counter-Intelligence, 1993.
[87] Peter Schweizer, "Friendly Spies," The Atlantic Monthly Press, 1993 (Note - while some elements of this book have been questioned by other reporters, other elements are strongly supported by written sources both before and since publication.) 1993 and Computers and Security, Vol 9, No 6, p515
[88] 2600, The Hacker Quarterly, Middle Island, NY V10, #2, Summer 1992.
[89] Frank Simon, "Liste der militaerischen Rechner im ARPA-Internetn," from the Chaos Computer Club directory, University of Ulm, Germany, system date 4-19-91. Shown in directory of Chaos Computer Club files titled LIES-MICH, system date 5-14-91.
[90] Internet File, risks@csl.sri.com
[91] JCS Pub l-02, "DoD Dictionary of Military and Associated Terms," Dec. 1,1989.
[92] F. Cohen, "A Short Course on Systems Administration and Security Under Unix," ASP Press, 1991
[93] "FCC Preliminary Report on Network Outages," Common Carrier Bureau, July, 1991
[94] "Network Reliability: A Report to the Nation," Compendium of Technical Papers, FCC's Network Reliability Council, June 1993

[95] Roberts, K. H. and Rousseau, D. M., "Research in Nearly Failure-Free, High-Reliability Organizations: Having the Bubble," IEEE Transactions on Engineering Management, 5-89, pp132-139

[96] Toni Ivergard, "Handbook of Control Room Design and Ergonomics," Taylor & Francis, 1989, Chapter 8.

[97] Lundy Lewis, "A Case-Based Reasoning Approach to the Management of Faults in Communications Networks," Proceedings of IEEE INFOCOM, Vol 3, 1993, pp1422-1429.

[98] Teresa Cochran and Joseph M. Mellichamp, "AUTOREC: An Automated Error Recovery System for Network Management," IEEE Network Magazine, March 1990.

[99] Seyhan Civasllar and Bharat T. Doshi, "Self-Healing in Wideband Packet Networks," IEEE Network Magazine, Jan. 1990.

[100] R. W. Wolverton, "Software Costing," TRW Systems, found in Handbook of Software Engineering, ed Vick, C. R. and Ramamoorthy, C.V., Van Nostrand Reinhold, 1984, pp469-493 cites R. 0. Lewis, "The Cost of an Error: A Retrospective Look at Safeguard Software," Science Applications International Corporation, Inc., prepared under Contract DA660-76-C-0011, Huntsville, AL, March 1977.

[101] Donald V. Steward, "Software Engineering with Systems Analysis and Design," Brooks/Cole Publishing Company, 1987, p26.

[102] Moses, et. al., Gensis 11:7 (The Tower of Babel); Numbers 13:17-19 (The Twelve Scouts); Joshua 2:1 (Spies saved by Rahab); Judges 20:37-41, (War with Benjamin), The New American Bible, Thomas Nelson, Publishers, 1971,

[103] Fred Giessler, "Reflexive Control," SAIC's Strategic Assessment Center, 13 July, 1993.

[104] ISSA, "Guideline for Information Valuation," International Systems Security Association, April 21,1993.

[105] Lauren D. Kohn and Kerry A. Blount, "Information Warfare Issues for Distributed Interactive Simulation," September 14, 1993.

[106] John Arquilla and David Ronfeldt, "Cyberwar is Coming!," Comparative Strategy, V12, ppl41-165.

[107] H. Simon, "Sciences of the Artificial," MIT Press, 1981.

[108] Personal conversations with IBM personnel 4 months after the Christmas Greeting incident.

[109] Personal conversations with several well known experts on this subject.

[110] Unclassified extract of "1979 Project SECA," 1979.

[111] DoD Directive TS3600.1, "Information Warfare (U)," (unclassified extract), December 21,1992

[112] Martin van Creveld, "Technology and War," McMillan, Inc. 199 1. (revised and expanded from 1989)

[113] Martin van Creveld, "The Transformation of War," Free Press, 1991.

[114] Edward Luttwak, "Strategy:The Logic of War and Peace," Belknap press, 1987.

[115] October 2, 1992 Audit Report No. 93-002 Project IFD-0043, Office of the Inspector General.

[116] M. A. Titov, A. G. Ivanov, and G. K. Moskatov, "An Adaptive Approach to Designing Antivirus Systems," unpublished paper, 1992.

[117] Bhumip Khasnabish, "A Bound of Deception in Multiuser Computer Networks," IEEE Journal on Selected Areas in Communications, V7#4, May, 1989.
[118] Goldreich, O., Herzberg, A., Mansour, Y., "Source to Destination Communication in the Presence of Faults," Proceedings of the Eighth Annual ACM Symposium on Principles of Distributed Computing, pp85- 101.
[119] Feige, U.; Shamir, A.; Tennenholtz, M., "The Noisy Oracle Problem," Advances in Cryptology CRYPT0 '88 Proceedings, pp284-296.
[120] DoD Directive 5200.28, "Security Requirements for Automatic Data Processing (ADP) Systems."
[121] "EDPACS"(EDP Audit Control and Security Newsletter), Dec, 1993.
[122] SAIC, "Threats and Defenses for WCCS," August, 1993.
[123] Perter G. Neumann, "The Computer-Related Risk of the Year: Weak Links and Correlated Events," COMPASS '91 (Computer Assurance), MST, June 25-27,1991.
[124] Dorothy Denning, "An Intrusion-Detection Model," Proceedings of the 1986 IEEE Symposium on Security and Privacy, p118-131.
[125] E. A. Feustal, "On the Advantages of Tagged Architecture," IEEE Transaction on Computers, Vol. C-22 #7, July, 1973, pp644-656.
[126] SAIC, 'White Paper to Implement Computer Misuse Detection on the Operational Support System (OSS) ," 1993.
[127] Bellcore, "Unix Security Awareness Alert," May 1990, Bellcore Technical Education Job Aid.
[128] Peter F. Drucker, "Post-Capitalist Society," Harper Business, 1993.
[129] D. A. Fulghum, "ALCMS Given Nonlethal Role," Aviation Week & Space Technology, February 22, 1993, pp20-22.
[130] D. A. Fulghum, "EMP Weapons Lead Race for Non-Lethal Technology," Aviation Week & Space Technology, May 24, 1993, p61.
[131] "Business Flying," Aviation Week & Space Technology, October 2, 1989, p85.
[132] "Ground Wave Emergency Network Should Be Operational Next Spring," Aviation Week & Space Technology, July 16, 1992, pp78-79.
[133] R. Brewer, "Design Tips for EMI Shielding," Machine Design, March 23, 1989, pp85-88.
[134] Bernard J. Eastlund, US Patent #4,686,605, "Method and Apparatus for Altering a Region in the Earth's Atmosphere, Ionosphere, and/or Magnetosphere," August 11, 1987.
[135] The American Heritage Desk Dictionary, Houghton Mifflin Company, Boston, MA, 1981.