REPORT OF THE

DEFENSE SCIENCE BOARD

TASK FORCE

ON

INFORMATION WARFARE - DEFENSE

(IW-D)

November 1996

OFFICE OF THE UNDER SECRETARY OF DEFENSE
FOR ACQUISITION & TECHNOLOGY
WASHINGTON, D.C. 20301-3140

II 834

This report is a product of the Defense Science Board (DSB). The DSB is a Federal Advisory Committee established to provide independent advice to the Secretary of Defense. Statements, opinions, conclusions, and recommendations in this report do not necessarily represent the official position of the Department of Defense.

This report is UNCLASSIFIED.

OFFICE OF THE SECRETARY OF DEFENSE
3140 DEFENSE PENTAGON
WASHINGTON, DC 20301-3140

DEFENSE SCIENCE
BOARD

25 NOV 1996

MEMORANDUM FOR UNDER SECRETARY OF DEFENSE (ACQUISITION & TECHNOLOGY)

SUBJECT: Report of the DSB Task Force on Information Warfare (Defense)

I am pleased to forward the final report of the DSB Task Force on Information Warfare (Defense), which was chaired by Mr. Duane P. Andrews. You asked the Task Force to focus on protection of information interests of national importance through establishment and maintenance of a credible information warfare (IW) defensive capability in several areas, including deterrence and to make recommendations regarding the creation and maintenance of specific aspects of a national information warfare defense capability.

The Task Force recommends a series of over 50 actions designed to better prepare the Department for this new form of warfare beginning with identification of an accountable focal point within the Department for all IW activities and ending with the allocation or reallocation of approximately $3 billion over the next 5 years to implement these recommended actions.

Craig I. Fields
Chairman

PREFACE

The Defense Science Board Task Force on Information Warfare (Defense) was established at the direction of the Under Secretary of Defense for Acquisition and Technology. By USD(A&T) Memorandum for the Chairman, Defense Science Board, dated October 4, 1995, the Task Force was directed to "focus on protection of information interests of national importance through the establishment and maintenance of a credible information warfare defensive capability in several areas, including deterrence." Specifically, the Task Force was asked to:

- Identify the information users of national interest who can be attacked through the shared elements of the national information infrastructure.
- Determine the scope of national information interests to be defended by information warfare defense and deterrence capabilities.
- Characterize the procedures, processes, and mechanisms required to defend against various classes of threats to the national information infrastructure and the information users of national interest.
- Identify the indications and warning, tactical warning, and attack assessment procedures, processes, and mechanisms needed to anticipate, detect, and characterize attacks on the national information infrastructure and/or attacks on the information users of national interest.
- Identify the reasonable roles of government and the private sector, alone and in concert, in creating, managing, and operating a national information warfare-defense capability.
- Provide specific guidelines for implementation of the Task Force's recommendations.

For the purpose of this report, the terms national and national-level are assumed to include Federal, state and local governments, academia, associations, public interest organizations, and the private sector.

This report presents the conclusions and recommendations of the Task Force based on study efforts of the Task Force and Panels created by the Task Force to address specific areas of interest. The report is organized as follows:

- Executive Summary.
- Section 1, Introduction, provides background information.
- Section 2, Environment, describes factors pertinent to the study effort.
- Section 3, Observations, provides the major findings of the Task Force.
- Section 4, What Should We Defend?, identifies the information users of national interest and scope of interests to be defended.
- Section 5, How Should We Defend?, suggests processes and procedures necessary to defend the users against the threats. It includes a discussion of required indications

and warning, tactical warning, attack assessment, and continuity of operations organizations and procedures.

- Section 6, Recommendations, presents recommendations, and provides specific guidelines for implementing the recommendations. It includes a discussion of the reasonable roles of government and the private sector and concludes with resources, in addition to current INFOSEC budgets, required to implement the recommendations.
- Section 7, Summary, briefly summarizes the report and suggests some immediate actions.

Appendices are provided as background and resource information. ***They <u>do not</u> represent a consensus view of the Task Force and recommendations contained in the Appendices <u>are not</u> Task Force recommendations to the Department.*** Some of the appendices were used in part as input to the main body of this report. Other appendices are provided because they contain useful information for further discussion of matters addressed in the main body of the report.

At about the same time that the Task Force was created, the President signed a major policy directive regarding the protection of critical infrastructures such as telecommunications, electric power, and transportation. This directive resulted in the creation of a Critical Infrastructures Working Group (CIWG) to address the manner in which the directive should be implemented. The CIWG recommendations were implemented with some modification in Executive Order 13010, Critical Infrastructure Protection which was signed by the President on July 15, 1996. E.O. 13010 establishes a President's Commission to, in part,

- Assess the scope and nature of the vulnerabilities of, and threats to, critical infrastructures,
- Determine what legal and policy issues are raised by efforts to protect critical infrastructures, and
- Recommend a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats and assuring their continued operation.

Given these parallel and closely related activities, the Task Force elected to address information warfare (defense) issues and provide conclusions from both the national and Department of Defense perspectives. However, the Task Force recommendations are specifically oriented on the Department of Defense. Department of Defense dependencies on national level activities for information warfare (defense) are provided to the Secretary of Defense for possible transmittal to the President's Commission for use in their deliberations.

TABLE OF CONTENTS

Section			Page
EXECUTIVE SUMMARY			ES-1
1.0	INTRODUCTION		1-1
2.0	ENVIRONMENT		2-1
	2.1	Growing Dependency, Growing Risk	2-1
	2.2	Information Warfare	2-4
	2.3	The Infrastructure	2-6
	2.4	Threat	2-11
3.0	OBSERVATIONS		3-1
4.0	WHAT SHOULD WE DEFEND?		4-1
5.0	HOW SHOULD WE DEFEND?		5-1
	5.1	Procedures, Processes and Mechanisms	5-1
	5.2	Strategy	5-2
6.0	RECOMMENDATIONS		6-1
	6.1	Designate an Accountable IW Focal Point	6-1
	6.2	Organize for IW-D	6-3
		6.2.1 Establish a Center for Intelligence Indications and Warning, Current Intelligence, and Threat Assessments	6-4
		6.2.2 Establish a Center for IW-D Operations	6-6
		6.2.3 Establish a Center for IW-D Planning and Coordination	6-8
		6.2.4 Establish a Joint Office for System, Network and Infrastructure Design	6-9
		6.2.5 Establish a Red Team for Independent Assessments	6-12
	6.3	Increase Awareness	6-15
	6.4	Assess Infrastructure Dependencies and Vulnerabilities	6-17
	6.5	Define Threat Conditions and Responses	6-18
	6.6	Assess IW-D Readiness	6-19
	6.7	"Raise the Bar" with High Pay-Off, Low-Cost Items	6-21
	6.8	Establish and Maintain a Minimum Essential Information Infrastructure	6-22
	6.9	Focus the R&D	6-24
	6.10	Staff for Success	6-26
	6.11	Resolve the Legal Issues	6-27

TABLE OF CONTENTS (Continued)

Section		Page
	6.12 Participate Fully in Critical Infrastructure Protection	6-28
	6.13 Provide the Resources	6-33
7.0	SUMMARY	7-1
APPENDIX A:	Threat Assessment	A-1
APPENDIX B:	National Intelligence Exploitation Architecture	B-1
APPENDIX C:	A Taxonomy for Information Warfare?	C-1
APPENDIX D:	Organizational Models	D-1
	D.1 Centers for Disease Control and Prevention	D-2
	D.2 Federal Emergency Management Agency Federal Response Plan	D-17
	D.3 National Drug Intelligence Center	D-34
APPENDIX E:	Think Pieces	E-1
	E.1 Information Infrastructure Assurance Principles	E-2
	E.2 "Raise the Bar" Exercise	E-7
APPENDIX F:	Technology Issues	F-1
APPENDIX G:	List of Acronyms	G-1
APPENDIX H:	Glossary	H-1

LIST OF EXHIBITS

Exhibit		Page
ES-1	Observations	ES-2
ES-2	Recommendations	ES-4
1-1	Terms of Reference	1-1
1-2	Additional Items of Interest	1-2
1-3	Task Force Members	1-2
2-1	A Fragile Foundation	2-3
2-2	Infrastructures and Dependencies	2-9
2-3	Vulnerabilities	2-10
2-4	Vulnerabilities/Exploitation Techniques	2-11
2-5	The Threat is Real	2-12
2-6	Threat Assessment	2-12
2-7	The Risk—A Clear and Present Danger	2-17
3-1	Initial Observations	3-1
3-2	Information Warfare is Different	3-2
3-3	Intelligence Community Observations	3-3
3-4	Additional Observations	3-4
3-5	Additional Observations	3-5
3-6	Additional Observations	3-6
3-7	Additional Observations	3-7
3-8	Additional Observations	3-8
4-1	National Goals for Information Warfare (Defense)	4-1
4-2	The National Interests	4-2
5-1	Procedures, Processes and Mechanisms	5-1
6-1	Designate an Accountable IW Focal Point	6-2
6-2	Organize for IW-D	6-3
6-2-1	Establish a Center for Intelligence Indications and Warning, Current Intelligence, and Threat Assessments	6-5
6-2-2	Establish a Center for IW-D Operations	6-7
6-2-3	Establish a Center for IW-D Planning and Coordination	6-9
6-2-4	Establish a Joint Office for System, Network and Infrastructure Design	6-12
6-2-5	Establish a Red Team for Independent Assessments	6-13
6-2-6	Organizational Recommendation - DoD Aspects	6-14
6-2-7	Organizational Recommendations - Functional Aspects	6-15
6-3	Increase Awareness	6-16

LIST OF EXHIBITS (Continued)

Exhibit		Page
6-4	Assess Infrastructure Dependencies and Vulnerabilities	6-17
6-5-1	Define Threat Conditions and Responses	6-18
6-5-2	Sample Threat Condition and Response	6-19
6-6	Assess IW-D Readiness	6-20
6-6	Assess IW-D Readiness (Continued)	6-21
6-7	"Raise the Bar" with High-Payoff, Low-Cost Items	6-22
6-8	Establish and Maintain a Minimum Essential Information Infrastructure	6-23
6-9	Focus the R&D	6-25
6-10	Staff for Success	6-27
6-11	Resolve the Legal Issues	6-28
6-12-1	Participate Fully in Critical Infrastructure Protection	6-29
6-12-2	Participate Fully in Critical Infrastructure Protection (Continued)	6-29
6-12-3	Participate Fully in Critical Infrastructure Protection (Continued)	6-30
6-12-4	Participate Fully in Critical Infrastructure Protection (Continued)	6-31
6-12-5	Participate Fully in Critical Infrastructure Protection (Continued)	6-32
6-12-6	Possible IW Target Protection Responsibilities	6-32
6-13-1	Provide the Resources	6-33
6-13-2	Get Started Resources	6-34
7-1	Tie It Together	7-1
7-2	And Start Immediately!	7-2

EXECUTIVE SUMMARY

The Environment

The national security posture of the United States is becoming increasingly dependent on U.S. and international infrastructures. These infrastructures are highly interdependent, particularly because of the inter-netted nature of the information components and because of their reliance on the national information infrastructure. The information infrastructure depends, in turn, upon other infrastructures such as electrical power.

Protecting the infrastructures against physical and electronic attacks and ensuring the availability of the infrastructures will be complicated. These infrastructures are provided mostly (and in some cases exclusively) by the commercial sector; regulated in part by federal, state, and local governments; and significantly influenced by market forces. Commercial services from the national information infrastructure provide the vast majority of the telecommunications portion of the Defense Information Infrastructure (DII). These services are regulated by Federal and state agencies. Local government agencies regulate the cable television portion of the information infrastructure. Power generation and distribution are provided by very diverse activities—the Federal government, public utilities, cooperatives, and private companies. Interstate telecommunications are regulated by the Federal Communications Commission, intrastate telecommunications by the state public utilities commissions. Interstate power distribution is regulated by the Federal Energy Regulatory Commission, intrastate power generation and distribution by the state public utilities commissions.

Observations

Information infrastructures are vulnerable to attack. While this in itself poses a national security threat, the linkage between information systems and traditional critical infrastructures has increased the scope and potential of the information warfare threat. For economic reasons, increasing deregulation and competition create an increased reliance on information systems to operate, maintain, and monitor critical infrastructures. This in turn creates a tunnel of vulnerability previously unrealized in the history of conflict.

Information warfare offers a veil of anonymity to potential attackers. Attackers can hide in the mesh of inter-netted systems and often use previously conquered systems to launch their attacks. The lack of geographical, spatial, and political boundaries offers further anonymity and legal and regulatory arbitrage; this lack also invalidates previously established "nation-state" sanctuaries. Information warfare is also relatively cheap to wage, offering a high return on investment for resource-poor adversaries. The technology required to mount attacks is relatively simple and ubiquitous. During information warfare, demand for information will dramatically increase while the capacity of the information infrastructure will most certainly decrease. The law, particularly international law, is currently ambiguous regarding criminality in and acts of war on information infrastructures. This ambiguity, coupled with a lack of clearly designated

responsibilities for electronic defense hinders the development of remedies and limits response options.

Exhibit ES-1 shows additional observations.

- ***Information warfare has been particularly troublesome for the intelligence community***
- ***We lack a common vocabulary***
- ***Resources are focused on classified content and systems***
- ***It is easy to make the IW-D problem too hard***
- ***Acquisition policy and practices pose dilemmas***
- ***However, a lot can be done***
- ***And DoD must start now!***

Exhibit ES-1. Observations

What Should We Defend?

The current Administration's national security strategy for the United States suggests that the nation's "economic and security interests are increasingly inseparable" and that "we simply cannot be successful in advancing our interests—political, military and economic—without active engagement in world affairs." In the broad sense, then, the scope of national information interests to be defended by information warfare defense and deterrence capabilities are those political, military, and economic interests. These include the continuity of a democratic form of government and a free market economy, the ability to conduct effective diplomacy, a favorable balance of trade, and a military force that is ready to fight and that can be deployed where needed. These interests are supported by the delivery of goods and services that result from the conduct of functional activities such as manufacturing, governing, banking and finance, and the like. Some of these activities are critical to the nation's political, military, and economic interests. These critical functional activities, in turn, depend on information technology and critical infrastructures such as banking and finance, electric power, telecommunications, and transportation.

In general, U.S. infrastructures are extremely reliable and available because they have been designed to respond to disruptions, particularly those caused by natural phenomena. Redundancy and diverse routing are two examples of design techniques used to improve reliability and availability. However, deregulation and increased competition cause companies operating these infrastructures to rely more and more on information technology to centralize control of their operations, to support critical functions, and to deliver goods and services. Centralization and reliance on broadly networked information systems increase the vulnerabilities of the infrastructures and the likelihood of disruptions or malevolent attacks.

The information users of national interest who can be attacked through the shared elements of the national information infrastructure are those responsible for performing the critical functions

necessary for the delivery of the goods and services upon which our political, military, and economic interests depend.

The Department of Defense (DoD) must preserve its ability to fulfill its basic missions. To do that, DoD must be concerned about the ensured operation of the critical functions and the availability of information necessary to fulfill those missions. The intertwined nature of the functions of national interest and supporting infrastructures add to the complexity: there are critical functions which have national security implications and which must be defended; and there are critical portions of the infrastructures which are necessary for the operation of DoD and national functions.

How Should We Defend?

The concept for defending the information infrastructure and the information components of other critical infrastructures includes the following principles:

- Critical functions must be capable of being performed in the presence of information warfare attacks.
- Some minimum essential infrastructure capability must exist to support these critical functions.
- Point and layered defenses are preferable to area defenses.
- The infrastructure must be designed to function in the presence of failed components, systems, and networks. The risk associated with failed components, systems, and networks must be managed since it cannot be avoided.
- The infrastructure control functions should not be dependent on normal operation of the infrastructure.
- The infrastructure must be capable of being repaired.

The concept for defending is as follows. In the information age as in the nuclear age, *deter* is the first line of defense. This deterrence must include an expression of national will as expressed in law and conduct, a declaratory policy relative to consequences of an information warfare attack against the United States, and an indication of the resiliency of the information infrastructure to survive an attack. Technology to conduct information warfare is simple and ubiquitous; some form of infrastructure robustness and protection is essential. It is technically and economically impossible to *design and protect* the infrastructure to withstand any and all disruptions, intrusions, or attacks (or avoid all risk). The risk can be managed, however, by protecting selected portions of the infrastructure that support critical functions and activities necessary for maintaining political, military, and economic interests. An equally important function is to *verify* through independent assessments that the design principles are being followed, that protective measures are being implemented where appropriate, and that the information warfare (defense) readiness posture is as reported.

Tactical warning, damage control, attack assessment, and restoration ensures the continuance of these critical functions and activities in the presence of disruptions or attacks. The essence of *tactical warning* is monitoring, detection of incidents, and reporting of the incidents. Monitoring

and detection of infrastructure disruptions, intrusions, and attacks are also an integral part of the defense against information warfare. Providing an effective monitoring and detection capability will require some policy initiatives, some legal clarification, and an ambitious research and development program. The telecommunications infrastructure will be subject to some form of attack and we should have some capability to limit the damage that results and to restore the infrastructure. Little research has been devoted to the basic procedures necessary to contain "battle" damage, let alone the tools which might provide some automated form of *damage control.* Some form of *attack assessment* is essential to determine the impact of an attack on critical functions and the appropriate response to an attack. Restoration of the infrastructure implies some capability to repair the damage and the availability of resources such as personnel, standby services contracts, and the like. The basic functions of monitoring, detection, damage control, and restoration must begin at the lowest possible operating level. Reports of the activity must be passed to regional, DoD, and national-level organizations to establish patterns of activity and to request assistance as needed in damage control and restoration. Finally, some form of *response* to the intrusions or attacks may be necessary to deter future intrusions or attacks. The response could entail civil or criminal prosecution, use of military force, perception management, diplomatic initiatives, or economic mandates. Because response might also involve offensive information warfare, this report does not address it in detail.

Recommendations

The Task Force makes 13 key recommendations as shown in Exhibit ES-2. The Task Force considers these recommendations as imperatives.

Bottom Line - DoD has an urgent need to:

1. ***Designate an accountable IW focal point***
2. ***Organize for IW-D***
3. ***Increase awareness***
4. ***Assess infrastructure dependencies and vulnerabilities***
5. ***Define threat conditions and responses***
6. ***Assess IW-D readiness***
7. ***"Raise the bar" (with high-payoff, low-cost items)***
8. ***Establish a minimum essential information infrastructure***
9. ***Focus the R&D***
10. ***Staff for success***
11. ***Resolve the legal issues***
12. ***Participate fully in critical infrastructure protection***
13. ***Provide the resources***

DSB has been urging action on this problem for 3 years!

Exhibit ES-2. Recommendations

In addition, the Task Force made over 50 additional recommendations, which are categorized under these key recommendations. (Note that the first recommendation addresses all of

information warfare, not just defensive information warfare.) The Task Force attempted to prioritize these "key recommendations," but in the end decided that portions of all of these key recommendations should be implemented immediately.

The following discussions provide all of the recommendations made by the Task Force. The parenthetical entry following each of the key recommendations identifies the section of the report in which the recommendations are discussed in detail.

1. Designate an accountable IW focal point (6.1). This is the most important recommendation the Task Force offers. The Task Force believes that the Secretary of Defense needs a single focal point charged to provide staff supervision of the complex activities and interrelationships that are involved in this new warfare area. This includes oversight of both offensive and defensive information warfare planning, technology development and resources. The SECDEF should:

1a. Designate ASD(C3I) as the accountable focal point for all IW issues.

1a(1). Develop a plan and associated budget beginning in FY 97 to obtain the needed IW-D capability.

1a(2). Authorize ASD(C3I) to issue IW instructions.

1a(3). Consider establishing a USD(Information).

1b. Establish a DASD(IW) and supporting staff to bring together as many IW functions as possible.

2. Organize for IW-D (6.2). This key recommendation identifies the need for specific IW-D related capabilities and organizations to provide or support the capabilities. While not specifically addressed by the Task Force, virtual organizations that draw on existing assets and capabilities can be established.

2a. Establish a center to provide strategic indications and warning, current intelligence, and threat assessments. The SECDEF should request the DCI to:

2a(1). Establish an I&W/TA center at NSA with CIA and DIA support.

2a(2). Task and resource the Intelligence Community to develop the processes for Current Intelligence, Indications and Warning, and Threat Assessments for IW-D.

2a(3). Encourage the Intelligence Community to develop information-age trade craft, staff with the right skills, and train for the information age.

2a(4). Conduct comprehensive case studies of U.S. offensive programs and a former foreign program to identify potential indicators—collection, funding, training, etc.

2a(5). Establish an organization to examine and analyze probable causes of all security breaches.

2a(6). Develop and implement an integrated National Intelligence Exploitation Architecture to support the organization and processes.

In addition, the SECDEF should:

2a(7). Direct the development of IW Essential Elements of Information.

2b. Establish a center for IW-D operations to provide tactical warning, attack assessment, emergency response, and infrastructure restoration capabilities. The SECDEF should:

2b(1). Establish a DoD IW-D operations center at DISA with NCS, NSA, and DIA support.

2b(2). Develop and implement distributed tactical warning, attack assessment, emergency response, and infrastructure restoration procedures.

2b(3). Interface the operations center with Service and Agency capabilities and I&W/TA support.

2b(4). Establish necessary liaison (e.g., with military and government operations centers, service providers, intelligence agencies, and computer emergency response centers).

2c. The SECDEF should establish an IW-D planning and coordination center reporting to the ASD(C3I) with interfaces to the intelligence community, the Joint Staff, the law enforcement community, and the operations center. This center will: develop an IW planning framework; assess IW policy, plans, intelligence support, allocation of resources, and IW incidents; develop procedures and metrics for assessing infrastructure and information dependencies; and facilitate sharing of sensitive information such as threats, vulnerabilities, fixes, tools, and techniques within DoD and among government agencies, the private sector, and professional associations.

2d. Establish a joint office for system, network and infrastructure design. This office will: develop and promulgate IW-D policies, architectures, and standards; design the information infrastructure for utility, resiliency, repairability, and security; develop and implement an IW-D configuration management process; and conduct independent verification of design and procurement specifications to ensure compliance with the design. The SECDEF should:

2d(1). Establish a joint security architecture/design office within DISA to shape the design of the DoD information infrastructure.

2d(2). Establish a process to verify independently and enforce adherence to these design principles.

2e. Establish a Red Team for independent assessments. The Red Team would assess the vulnerabilities of new systems and services and would conduct "IW-like" attacks to verify the readiness posture and preparedness of the fighting forces and supporting activities. The SECDEF should:

2e(1). Establish a Red Team which is accountable to SECDEF/DEPSECDEF and independent of design, acquisition, and operations activities.

2e(2). Develop procedures for employment of the Red Team.

3. Increase awareness (6.3). The Task Force strongly suggests the need to make senior-level government and industry leaders aware of the vulnerabilities and of the implications. To that end, the SECDEF should:

3a. Establish an internal and external IW-D awareness campaign for the public, industry, CINCs, Services, and Agencies.

3b. Expand the IW Net Assessment recommended by the 1994 Summer Study to include assessing the vulnerabilities of the DII and NII.

3c. Review joint doctrine for needed IW-D emphasis.

3d. Explore possibility of large-scale IW-D demonstrations for the purpose of understanding cascading effects and collecting data for simulations.

3e. Develop and implement simulations to demonstrate and play IW-D effects (USD(A&T) lead).

3f. Implement policy to include IW-D realism in exercises.

3g. Conduct IW-D experiments.

4. Assess infrastructure dependencies and vulnerabilities (6.4). Various infrastructures are vitally needed to support mobilization, deployment, and employment of forces and to control and sustain those forces. Some of these interconnected infrastructures are known to have single points of failure. Therefore, the SECDEF should:

4a. Develop a process and metrics for assessing infrastructure dependency.

4b. Assess/document operations plans infrastructure dependencies.

4c. Assess/document functional infrastructure dependencies.

4d. Assess infrastructure vulnerabilities.

4e. Develop a list of essential infrastructure protection needs.

4f. Develop and report to the SECDEF the resource estimates for essential infrastructure protection.

4g. Review vulnerabilities of hardware and software embedded in weapons systems.

5. Define threat conditions and responses (6.5). Conditions analogous to DEFCON should be developed to provide a common understanding of IW threat conditions. Appropriate responses to these conditions should also be developed using the Task Force suggestions outlined in the report as a starting point. The SECDEF should:

5a. Define and promulgate a useful set of IW-D threat conditions which is coordinated with current intelligence community threat condition definitions.

5b. Define and implement responses to IW-D threat conditions.

5c. Explore legislative and regulatory implications.

6. Assess IW-D readiness (6.6). A standardized process is necessary to enable commanders to assess and report their operational readiness status as it relates to their specific dependency on information and information services. Using the standard vocabulary suggested by the Task Force, the SECDEF should:

6a. Establish a standardized IW-D assessment system for use by CINCs, MilDeps, Services, and Combat Support Agencies.

6b. Incorporate IW preparedness assessments in Joint Reporting System and Joint Doctrine, for example.

7. "Raise the bar" with high-payoff, low-cost items (6.7). There are a number of low-cost activities the Department can undertake to "raise the bar" significantly for potential systems and network intruders. Three specific Task Force recommendations are that the SECDEF should:

7a. Direct the immediate use of approved products for access control as an interim until a MISSI solution is implemented and for those users not programmed to receive MISSI products.

7b. Examine the feasibility of using approved products for identification and authentication.

7c. Require use of escrowed encryption for critical assets such as databases, program libraries, applications, and transaction logs to preclude rogue employees from locking up systems and networks.

8. Establish and maintain a minimum essential information infrastructure (6.8). A strategy and an overall architecture concept employing existing core capabilities such as Milstar must be developed to serve as a means for restoring services for critical functions and adapting to large-scale outages. The SECDEF should:

8a. Define options with associated costs and schedules.

8b. Identify minimum essential conventional force structure and supporting information infrastructure needs.

8c. Prioritize critical functions and infrastructure dependencies.

8d. Design a Defense MEII and a failsafe restoration capability.

8e. Issue direction to the Defense Components to fence funds for a Defense MEII and failsafe restoration capability.

9. Focus the R&D (6.9). While many commercial and approved security products are available to meet some of the Department's needs, these products generally do not meet the Department's needs in large-scale distributed computing environments and generally do not protect against denial of service attacks. Therefore, the SECDEF should focus the DoD R&D program on the following areas.

9a. Develop robust survivable system architectures.

9b. Develop techniques and tools for modeling, monitoring, and management of large-scale distributed/networked systems.

9c. Develop tools and techniques for automated detection and analysis of localized or coordinated large-scale attacks.

9d. Develop tools for synthesizing and projecting the anticipated performance of survivable distributed systems.

9e. Develop tools and environments for IW-D oriented operational training.

9f. Develop testbeds and simulation-based mechanisms for evaluating emerging IW-D technology and tactics.

In addition, the SECDEF should work with the National Science Foundation to:

9g. Develop research in U.S. computer science and computer engineering programs.

9h. Develop educational programs for curriculum development at the undergraduate and graduate levels in resilient system design practices.

10. Staff for success (6.10). A cadre of high-quality, trained professionals with recognized career paths is an essential ingredient for defending present and future information systems. The Task Force recommends that the SECDEF:

10a. Establish a career path and mandate training and certification of systems and network administrators.

10b. Establish a military skill specialty for IW-D.

10c. Develop specific IW awareness courses with strong focus on operational preparedness in DoD's professional schools.

11. Resolve the legal issues (6.11). The advent of distributed computing has and will continue to further blur the boundaries of the systems and networks that the Department uses. Confusion also stems from uncertainty over when or whether a wiretap approval is needed. Government-wide guidance, and perhaps legislation as well, are needed in the areas of Department assistance to the private sector (e.g., Computer Security Act), tracing attackers of unknown nationality (intelligence versus U.S. persons), tracking attackers through multiple systems, and obtaining/requiring reports of computer-related incidents from the private sector owners and operators of critical infrastructures. The SECDEF should:

11a. Promulgate for Department of Defense systems:

- **Guidance and unequivocal authority for Department users to monitor, record data, and repel intruders in computer systems for self protection.**
- **Direction to use banners that make it clear the Department's presumption that intruders have hostile intent and warn that the Department will take the appropriate response.**
- **IW-D rules of engagement for self-protection (including active response) and civil infrastructure support.**

11b. Provide to the Presidential Commission on Critical Infrastructure Protection proposed legislation, regulation, or executive orders for defending other systems.

12. Participate fully in critical infrastructure protection (6.12). The Task Force makes the following recommendations to the SECDEF regarding the activities of the President's Commission on Critical Infrastructure Protection. Detailed suggestions for each of the below recommendations are outlined in Section 6.12.

12a. Offer specific Department capabilities to the President's Commission.

12b. Advocate the Department's interests to the President's Commission.

12c. Request the Commission provide certain national-level capabilities for the Department.

12d. Suggest IW-D roles for government and the private sector.

13. Provide the resources (6.13). The Task Force reviewed all of the individual recommendations categorized under the key recommendations and estimated to $5 million granularity what the implementation costs might be. The cost estimate is $3.01 billion over fiscal years 1997 through 2001. However, the Department should make a detailed estimate.

SECTION 1.0

INTRODUCTION

The Task Force was formed in November of 1995. It met formally eight times. Four individual panels were formed to address specific issues and each met about the same number of times. During the course of the study, the Task Force drew upon previous DSB Task Force efforts. Some recurring themes will be pointed out later in the report.

The objective of the study was to make recommendations regarding the creation and maintenance of specific aspects of a national information warfare defense capability. Exhibit 1-1 shows the specific tasks outlined by the terms of reference.

- **TOR #1 - Identify the information users of national interest who can be attacked through the shared elements of the national information infrastructure. This should include telecommunications, public transportation, financial services, public safety, and the mission essential functions of the Department of Defense.**
- **TOR #2 - Determine the scope of national information interests to be defended by information warfare defense and deterrence capabilities.**
- **TOR #3 - Characterize the procedures, processes, and mechanisms required to defend against various classes of threats to the national information infrastructure and the information users of national interest.**
- **TOR #4 - Identify the indications and warning, tactical warning, and attack assessment procedures, processes, and mechanisms needed to anticipate, detect, and characterize attacks on the national information infrastructure and/or attacks on the information users of national interest.**
- **TOR #5 - Identify the reasonable roles of government and the private sector, alone and in concert, in creating, managing, and operating a national information warfare-defense capability.**
- **TOR #6 - Provide specific guidelines for implementation of the Task Force's recommendations.**

Exhibit 1-1. Terms of Reference

In addition to the Terms of Reference objectives, the Task Force was requested to look at additional items of interest shown in Exhibit 1-2. The National Research Council study was mandated by Public Law 103-160, Defense Authorization Bill for Fiscal Year 1994, November 30, 1993. Pre-publication copies of this report were released May 30, 1996. Because of the potential role of cryptography in information warfare - defense (IW-D), the Task Force was encouraged to review the NRC report in the context of the Task Force deliberations. To avoid duplication and to provide additional focus to the study, the Task Force received briefings on the study of the Global Information Infrastructure sponsored by the Director of Central Intelligence. This excellent study effort provided valuable insights into the global implications of defensive information warfare.

- ***DoD***
  - **Organization for defensive information warfare**
  - **Legislation and enforcement**
  - **Enabling technologies**
  - **Indications and warning/response center**
  - **Intellectual framework/taxonomy**
  - **Intelligence community**
  - **Red teaming**
- ***NRC study on "Cryptography's Role in Securing the Information Society"***
- ***DCI study of the Global Information Infrastructure***
- ***Presidential Commission on Critical Infrastructure Protection***

Exhibit 1-2. Additional Items of Interest

During the Task Force deliberations, the President signed Presidential Decision Directive 39 (late 1995) and Executive Order 13010 (July 15, 1996). These established a President's Commission on Critical Infrastructure Protection. The Commission was tasked to develop a comprehensive national policy and implementation strategy for protecting critical infrastructures from physical and cyber threats. The Task Force was advised that after review and approval of the Task Force report by OUSD(A&T), the Defense Science Board will forward its report to the Commission as a "statement of DoD issues, concerns, requirements, and recommendations."

The sponsors of the study were the Honorable Emmett Paige, Jr., Assistant Secretary of Defense for C3I; and VADM Arthur K. Cebrowski, Director for C4 Systems, Joint Staff.

Task Force members are shown in Exhibit 1-3. A variety of disciplines were represented—academia, the telecommunications, banking, and aerospace industries, systems integrators, former military—and a number of members with former government service. In order to examine the issues more closely, the Task Force organized into four panels.

Mr. Duane Andrews, Chairman	**Mr. Donald C. Latham, Vice Chairman**
Mr. John G. Grimes **Org'n and Mgmt Panel Chairman**	**Gen. Bernard P. Randolph, USAF (Ret.)** **Technology Panel Chairman**
Mr. Paul A. Strassmann, **Policy Panel Chairman**	**Mr. Lawrence T. Wright,** **Threat Panel Chairman**
Mr. Edward C. Aldridge	**Mr. Bob Nesbit**
Mr. Stewart A. Baker	**Dr. Percy A. Pierre**
Dr. Delores M. Etter	**Mr. John P. Stenbit**
Mr. Charles A. Fowler	**Mr. Lowell E. Thomas**
Dr. George H. Heilmeier	**ADM Harry D. Train II, USN (Ret.)**
Mr. John Lane	**Dr. Willis H. Ware**
Mr. Alan J. McLaughlin	**CDR Frank Klein, Executive Secretary**

Exhibit 1-3. Task Force Members

SECTION 2.0

ENVIRONMENT

2.1 GROWING DEPENDENCY, GROWING RISK

The objective of warfare waged against agriculturally-based societies was to gain control over their principal source of wealth: land. Military campaigns were organized to destroy the capacity of an enemy to defend an area of land.

The objective of warfare waged against industrially-based societies was to gain control over their principal source of all wealth: the means of production. Military campaigns were organized to destroy the capacity of the enemy to retain control over sources of raw materials, labor and production capacity.

The objective of warfare to be waged against information-based societies is to gain control over the principal means for the sustenance of all wealth: the capacity for coordination of socio-economic inter-dependencies. Military campaigns will be organized to cripple the capacity of an information-based society to carry out its information-dependent enterprises.

In the U.S. society, over 60 percent of the workforce is engaged in information-related management activities. The value of most wealth producing-resources depends on "knowledge capital" and not on financial assets or masses of labor. Similarly, the doctrine of the U.S. military is now principally based on the superior use of information.

> "The joint campaign should fully **exploit the information differential,** that is, the superior access to and ability to effectively employ information on the strategic, operational and tactical situation which advanced U.S. technologies provide our forces." [Joint Pub. 1, p. IV-9]

The military doctrines shaping U.S. force structure and operational planning assume this information superiority. "Joint Vision 2010 focuses the strengths of each individual Service on operational concepts that achieve Full Spectrum Dominance" This technological view is shared in the Army's "Enterprise Strategy" and "Force XXI Concept of Operations," the Navy's "Forward...From the Sea," the Air Force's "Global Presence," and the Marine's "Operational Maneuver from the Sea."

The capstone Joint Vision 2010 provides the conceptual template for how America's Armed Forces will channel the vitality and innovation of our people and leverage technological opportunities to achieve new levels of effectiveness in joint warfighting. It addresses the expected continuities and changes in the strategic environment, including technology trends and their implications for our Armed Forces. It recognizes the crucial importance of our current high-quality, highly trained forces and provides the basis for their further enhancement by prescribing how we will fight in the early 21st century. This vision of future warfighting embodies the improved intelligence and command and control available in the information age and goes on to develop four operational concepts: dominant maneuver, precision engagement, full dimensional protection, and focused logistics.

It is not prudent to expect the U.S. dependence on information-dominated activities for wealth producing and for national security to go unchallenged. In his book, *Strategy: the logic of war and peace* [1987, Belknap Press, pages 27-28], Edward Luttwak notes:

> The notion of an 'action-reaction' sequence in the development of new war equipment and newer countermeasures, which induce in turn the development of counter-countermeasures and still newer equipment, is deceptively familiar. That the technical devices of war will be opposed whenever possible by other devices designed specifically against them is obvious enough. Slightly less obvious is the relationship (inevitably paradoxical) between the very success of new devices and their eventual failure: *any sensible enemy will focus his most urgent efforts on countermeasures meant to neutralize whatever opposing device seems most dangerous at the time.*

The reality is that the vulnerability of the Department of Defense—and of the nation—to offensive information warfare attack is largely a self-created problem. Program by program, economic sector by economic sector, we have based critical functions on inadequately protected telecomputing services. In aggregate, we have created a target-rich environment and the U.S. industry has sold globally much of the generic technology that can be used to strike these targets.

Despite the enormous cumulative risk to the nation's defense posture, at the individual program level there still is inadequate understanding of the threat or acceptance of responsibility for the consequences of attacks on individual systems that have the potential to cascade throughout the larger enterprise.

A case examined in some detail by the Task Force was the dependence of the Global Transportation Network on unclassified data sources and the GTN interface to the Global Command and Control System (GCCS). GCCS will continue to increase in importance as it becomes the system of systems through which CINCs, JTFs, and other commanders gain access to more and different information sources. Although GCCS has undergone selected security testing, much remains to be accomplished. For example, security testing to date has focused principally upon Oracle databases and applications evaluation. Other GCCS aspects need thorough security testing; e.g., database applications (Sybase), message functions and configuration management. GTN and GCCS are not unique circumstances. The Global Combat Support System and a long series of Advanced Concepts Technology Demonstrations currently shaping the future of C4ISR follow a remarkably similar pattern: Well-intentioned program managers work very hard to deliver an improved mission capability in a constrained budget environment. The operators they are supporting do not emphasize security and neither operators nor developers are held responsible for the contribution their individual program makes to the collective risk of cascading failure in the event of information warfare attack.

To reduce the danger, all defense investments must be examined from a network- and infrastructure-oriented perspective, recognizing the collective risk that can grow from individual decisions on systems that be connected to a shared infrastructure. Only those programs that can operate without connecting to the global network or those that can operate with an accepted level

of risk in a networked information warfare environment should be built. Otherwise, we are paying for the means that an enemy can use to attack and defeat us.

The shift from the industrial age to the information age and the implications are illustrated in Exhibit 2-1.

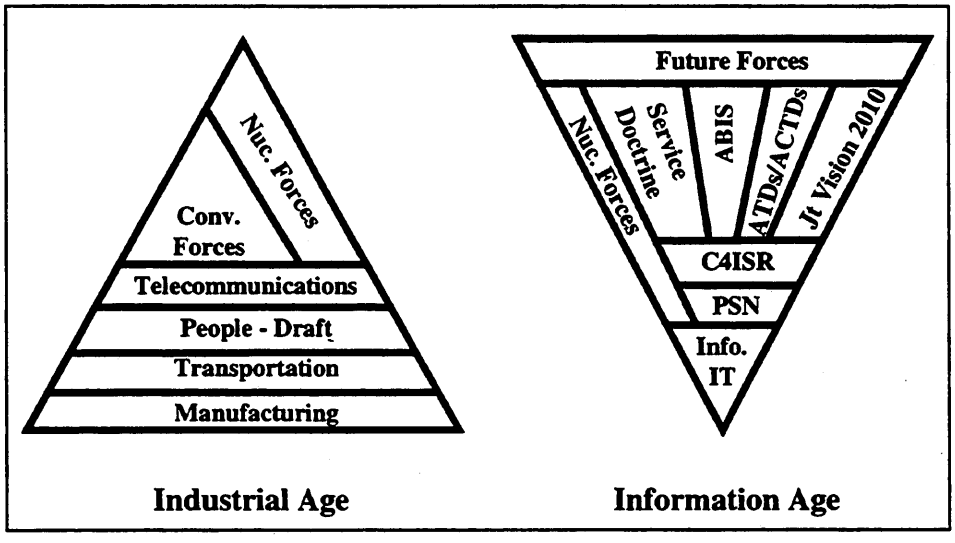


Exhibit 2-1. A Fragile Foundation

The United States formerly enjoyed a broad-based manufacturing foundation to support other infrastructures and conventional and nuclear forces. With the increasing dependence on information and information technology, that broad-based foundation has been reduced to a rather narrow base of constantly changing and increasingly vulnerable information and information technology. Service and joint doctrine clearly indicate an increasing dependence of future forces on information and information technology. However, the doctrine of information superiority assumes the availability of the information and information technology—a dangerous assumption. The published Service and joint doctrine does not address the operational implications of a failure of information and information technology.

By analogy, consider the protection implications of adding an aircraft carrier to our force structure. The carrier does not deploy in isolation. It is accompanied by all manner of ships, aircraft, and technology to ensure the protection of the entire battle group: destroyers for picket duty, cruisers for firepower, submarines for subsurface protection, aircraft and radar for early warning, and so on. The United States must begin to consider the implications of protecting its information-age doctrine, tactics, and weapon systems. It can not simply postulate doctrine and tactics which rely so extensively on information and information technology without comparable attention to information and information systems protection and assurance. This attention, backed up with sufficient resources, is the only way the Department can ensure adequate protection of our forces in the face of the inevitable information war.

2.2 INFORMATION WARFARE

Although this task force specifically examined IW-D, it also considered of a few of the concepts behind offensive information warfare to help define the battlefield upon which the defense must operate.

Offensive information warfare is attractive to many because it is cheap in relation to the cost of developing, maintaining, and using advanced military capabilities. It may cost little to suborn an insider, create false information, manipulate information, or launch malicious logic-based weapons against an information system connected to the globally shared telecommunications infrastructure. The latter is particularly attractive; the latest information on how to exploit many of the design attributes and security flaws of commercial computer software is freely available on the Internet.

In addition, the attacker may be attracted to information warfare by the potential for large non-linear outputs from modest inputs. This is possible because the information and information systems subject to offensive information warfare attack may only be a minor cost component of a function or activity of interest—the database of the items in a warehouse costs much less then the physical items stored in the warehouse.

As an example of why information warfare is so easy, consider the use of passwords. We have migrated to distributed computing systems that communicate over shared networks but largely still depend on the use of fixed passwords as the first line of defense—a carry-over from the days of the stand-alone mainframe computer. We do this even though we know that network analyzers have been and continue to be used by intruders to steal computer addresses, user identities, and user passwords from all the major Internet and unclassified military networks. Intruders then use these stolen identities and passwords to masquerade as legitimate users and enter into systems. Once in, they apply freely available software tools which ensure that they can take control of the computer and erase all traces of their entry.

It is important to stress that strategically important information warfare is not a trivial exercise of hacking into a few computers—the Task Force does not accept the assertions of the popular press that a few individuals can easily bring the United States to its knees. The Task Force agrees that it is easy for skilled individuals (or less skilled people with suitable automated tools) to break into unprotected and poorly configured networked computers and to steal files, install malicious software, or cause a denial of service. However, it is very much more difficult to collect the intelligence needed and to analyze the designs of complex systems so that an attacker could mount an attack that would cause nation-disrupting or war-ending damage at the time and place and for the duration of the attacker's choosing.

This is not to make light of the power of the common hacker "attack" methods reported in the press. Many of these methods are sufficiently robust to enable significant harassment or large-scale terrorist attacks. The Task Force also acknowledges that malicious software can be emplaced over time with a common time trigger or other means of activation and that the effect could be of the scale of a major concurrent attack. While such an attack cannot be ruled out, the

probability of such is assessed to be low. Currently, however, there is no organized effort to monitor for unauthorized changes in operational software even though for the past 3 years unknown intruders have been routinely been penetrating DoD's unclassified computers.

The above assessments do not mean that the threat of offensive information warfare is low or that it can be ignored. The U.S. susceptibility to hostile offensive information warfare is real and will continue to increase until many current practices are abandoned.

Practices that invite attack include poorly designed software applications; the use of overly complex and inherently unsecure computer operating systems; the lack of training and tools for monitoring and managing the telecomputing environment; the promiscuous inter-networking of computers creating the potential for proliferating failure modes; the inadequate training of information workers; and the lack of robust processes for the identification of system components, including users. By far the most significant is the practice of basing important military, economic and social functions on poorly designed and configured information systems, and staffing these systems with skill-deficient personnel. These personnel often pay little attention to or have no understanding of the operational consequences of information system failure, loss of data integrity, or loss of data confidentiality.

Information warfare defense is not cheap, nor can it be easily obtained. It will take resources to develop the tools, processes, and procedures needed to ensure the availability of information and integrity of information, and to protect the confidentiality of information where needed. Additional resources will be needed to develop design guidelines for system and software engineers to ensure information systems that can operate in an information warfare environment. More resources will be needed to develop robust means to detect when insiders or intruders with malicious intent have tampered with our systems and to have a capability to undertake corrective actions and restore the systems.

Note that the appropriate investment in an information warfare defense capability has no correlation with the investment that may have been made to obtain an offensive information warfare capability. Information warfare defense encompasses the planning and execution of activities to blunt the effects of an offensive information warfare attack. However, the value of an investment in information warfare defense is not a function of the cost of the information or information system to be protected. Rather, the value of the defense is a function of the value to the defender of an information-based activity or process that may be subject to an information warfare attack.

If the defender leaves unprotected vital social, economic, and defense functions that depend upon information services, then the defender invites potential adversaries to make an investment in an offensive information warfare capability to attack these functions. To provide a robust deterrent against such an attack, an information-dependent defender should invest wisely in a capability to protect and restore vital functions and processes and demonstrate that the information services used are robust and resilient to attack.

Part of the challenge is that the rate of technology change is such that most systems designers and system engineers have their hands full just trying to keep up—never mind learning and applying totally new security design practices. But the lack of such steps can cost. The organized criminals that recently made a successful run at one of the major U.S. banks spent 18 months of preparation, including downloading application software and the e-mail of the software designers, before they started to transfer funds electronically.

It will cost even more, as well as raise significant issues of privacy and the role of the government, to design a warning system for major institutions of society such as the banks or air traffic control. Such a warning system should, as a minimum, provide tactical warning of and help in the characterization of attacks mounted through the information infrastructure.

Probably the biggest obstacle will be the difficulty in convincing people—whether in commerce, in the military, or in government—of the need to examine work functions and operating processes. This examination should uncover unintentional dependencies on the assumed proper operation of information services beyond their control.

2.3 THE INFRASTRUCTURE

What is the National Information Infrastructure (NII)? The phrase "information infrastructure" has an expansive meaning. The NII includes more than just the physical facilities used to transmit, store, process, and display voice, data, and images. It encompasses a wide range and ever-expanding range of equipment: cameras, scanners, keyboards, telephones, fax machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, optical fiber transmission lines, microwave nets, switches, televisions, monitors, printers, and much more.

The NII is not a cliff that suddenly confronts us, but rather a slope—one that society has been climbing since postal services and semaphore networks were established. An information infrastructure has existed for a long time, continuously evolving with each new advance in communications technology. What is different is that today we are imagining a future when all the independent infrastructures are combined. An advanced information infrastructure will integrate and interconnect these physical components in a technologically neutral manner so that no one industry will be favored over any other. Most importantly, the NII requires building foundations for living in the Information Age and for making these technological advances useful to the public, business, libraries, and other non-governmental entities. That is why, beyond the physical components of the infrastructure, the value of the NII to users and the nation will depend in large part on the quality of its other elements:

- The information itself, which may be in the form of video programming, scientific or business databases, images, sound recordings, library archives, and other media. Vast quantities of that information exist today in government agencies and even more valuable information is produced every day in our laboratories, studios, publishing houses, and elsewhere.
- Applications and software that allow users to access, manipulate, organize, and digest the proliferating mass of information that the NII's facilities will put at their fingertips.

- The network standards and transmission codes that facilitate interconnection and interoperation between networks, and ensure the privacy of persons and the security of the information carried, as well as the security and reliability of the networks.
- The people—largely in the private sector—who create the information, develop applications and services, construct the facilities, and train others to tap its potential. Many of these people will be vendors, operators, and service providers working for private industry. Every component of the information infrastructure must be developed and integrated if America is to capture the promise of the Information Age.

We call out domains within this infrastructure by names that reflect the interest of the user: the Defense Information Infrastructure of the defense community; the National Information Infrastructure of the United States; the complex, interconnected Global Information Infrastructure of the future described so well to the Task Force by the representatives of the Central Intelligence Agency. The reality is that almost all are interconnected.

DoD has over 2.1 million computers, over 10,000 LANs, and over 100 long-distance networks. DoD depends upon computers to coordinate and implement aspects of every element of its mission, from designing weapon systems to tracking logistics. In field testing, DISA has determined that at least 65 percent of DoD unclassified systems are vulnerable to attack. Consider how this state come about.

The early generations of computer systems presented relatively simple security challenges. They were expensive, they were isolated in environmentally controlled facilities; and few understood how to use them. Protecting these systems was largely a matter of physical security controlling access to the computer room and of clearing the small number of specialists who needed such access.

As the size and price of computers were reduced, microprocessors began to appear in every workplace, on the battlefield and embedded in weapons systems. Software for these computers is written by individuals and firms scattered across the globe. Connectivity was extended, first to remote terminals, eventually to local- and wide-area communications networks, and now to global coverage. What was once a collection of separate systems is now best understood as a dynamic, ever-changing, collection of subscribers using a large, multifaceted information infrastructure operating as a virtual utility.

These legacy computer systems were not designed to withstand second-, third-, or "n"-order-level effects of an offensive information warfare attack. Nor is there evidence that the computer systems presently under development will provide such protection. The cost for "totally hardened" systems is prohibitive. Security criteria at present presume that computing can be protected at its perimeter, primarily through the encryption of telecommunications links. However, internal security may be more important than perimeter defense.

It is not necessary to break the cryptographic protection used to protect telecommunications and data to attack classified computing environments. The legacy protection paradigm used by DoD was based upon the classification of information. However, most classified computer systems

contain, and often rely on, unclassified information. This unclassified information often has little or no protection of the data integrity prior to entry into classified systems. The expected interaction between GCCS and GTN is an example of this. An increasing number of DoD systems contain decision aids and other event driven modules that, unless buffered from unclassified data whose integrity cannot be verified, are at risk.

To cope with this new reality, the approach for managing information security must shift from developing security for each individual system and network to developing security for subscribers within the worldwide utility; and from protecting isolated systems owned by discrete users to protecting distributed, shared systems that are interconnected and depend upon an infrastructure that individual subscribers neither own nor control.

Successful protection policies within this global structure must be sufficiently flexible to cover a wide range of systems and equipment from local area networks to worldwide networks, and from laptop computers to massively parallel processing supercomputers. They must take into account threat, both from the insider and the outsider, and must espouse a philosophy of risk management in making security decisions.

These protection challenges are made more difficult by the rapid technological and regulatory changes under way in the distributed computing environment. The Telecommunications Act of 1996 is reshaping all aspects of interconnected communications in the United States. Similar movements toward deregulation are under way across the globe. Into this regulatory turmoil technology is introducing new services based on a bevy of competing waveforms and protocols for use over copper, coaxial, glass, and wireless mediums. To date, it is not possible to predict how fragile or how robust the communications infrastructure will be in the near term—let alone the far future.

New computing technologies are being integrated into distributed computing environments on a large scale even though the fragility of these technologies is not understood. Recent examples include the post-deployment security flaws found in Netscape Navigator and in Java applets; the ongoing market struggle to dominate the building blocks for World Wide Web applications formed from collections of objects distributed across clients and servers that is under way between the Object Management Group's Common Object Request Broker Architecture and Microsoft Corporation's Distributed Common Object Model (each with a different approach to security); and a proposed future where Microsoft would automatically deliver and install software updates onto the customer's desktop without the customer's active involvement.

These environmental factors have serious implications for information warfare defense. Within this rapidly changing, globally interconnected environment of telecomputing activities it is not possible for a person to identify positively who is interconnected with him or her or know the exact path a message and voice traffic takes as it transits the telecommunications "cloud." It is not possible to know technically or at the logical level how the various software components on a computer— including the distributed applets downloaded, used, and discarded—interact together. It is not possible to know for sure if the various components installed in the computer hardware only do what is asked of them. Finally, it is certainly not possible to know for certain if

a co-worker who shares authorized access to a telecomputing environment is behaving appropriately.

In sum, we have built our economy and our military on a technology foundation that we do not control and which, at least at the fine detail level, we do not understand.

A few words about the environment are important to set the stage for later discussions. DoD's information infrastructure is a part of a larger national and global information infrastructure. These interconnected and interdependent systems and networks are the foundation for critical economic, diplomatic, and military functions upon which our national and economic security are dependent. Exhibit 2-2 shows a few examples of those functions, the importance of information and the information infrastructure to each, and the criticality of functions such as coalition building in responding to a regional crisis.

- ***DoD's information infrastructure is part of an interconnected set of military, commercial, national and international interdependent networks and systems***
- ***Critical functions are heavily dependent on the infrastructures and information***
  - **Economic**
    - **Manufacturing and distribution**
    - **Free trade**
  - **Diplomatic**
    - **Coalition building**
    - **Crises stabilization**
  - **Military**
    - **Deployment**
    - **Coalition warfare**
    - **Sustainment**

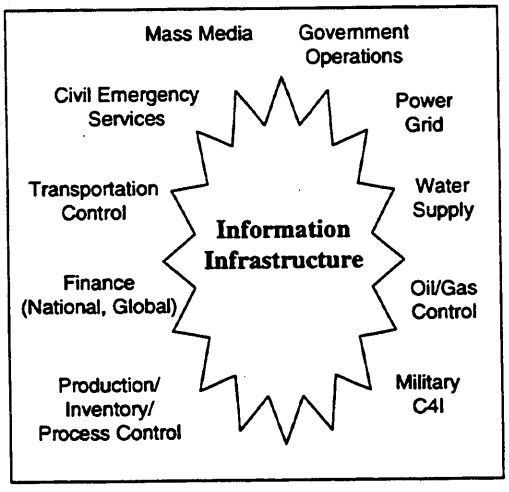


Exhibit 2-2. Infrastructures and Dependencies

The United States is an information and information systems dominated society. Because of its ever-increasing dependence on information and information technology, the United States is one of the most vulnerable nations to information warfare attacks. The United States and its infrastructures are vulnerable to a variety of threats ranging from rogue hackers for hire to coordinated trans-national and state-sponsored efforts to gain some economic, diplomatic or military advantage. Exhibit 2-3 depicts some of the vulnerabilities.

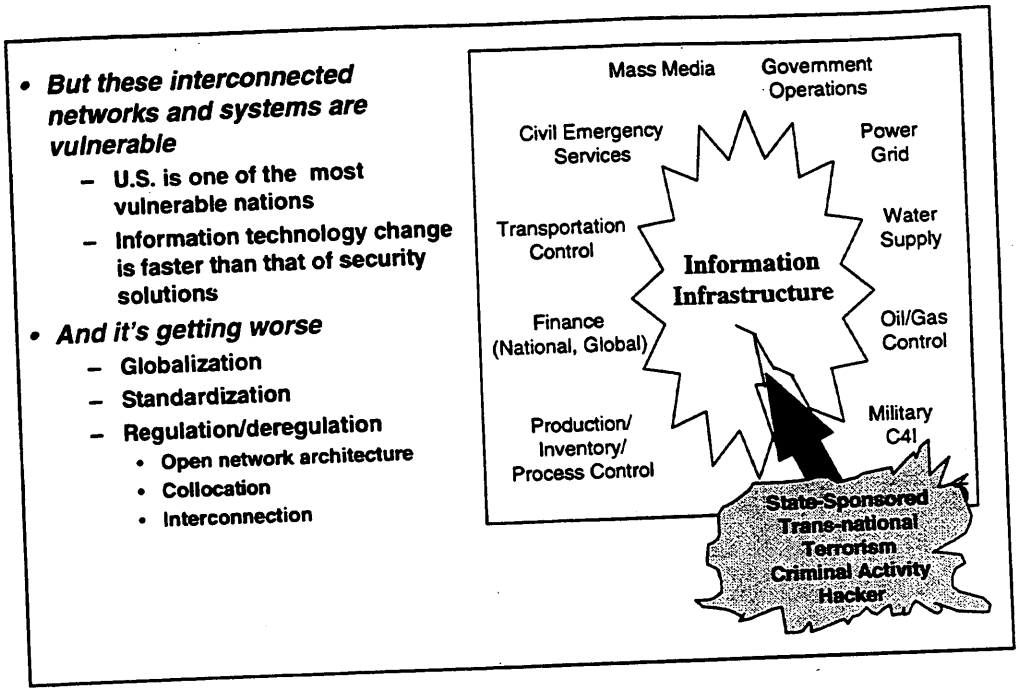


Exhibit 2-3. Vulnerabilities

The military implications of this dependency was made abundantly clear when it was suggested in one of the briefings presented to the Task Force that points of failure had been identified for each of three infrastructures (telecommunications, power, transportation) supporting a key port city in the United States. If these individual locations were attacked or destroyed, or in the case of power and telecommunications, if the resident electronics were disturbed, it would impact the ability of military forces to deploy at the pace specified in the Time Phased Force Deployment List.

And it is getting worse. Globalization of business operations brings with it increased information and information system interdependence. Standardization of technology for effectiveness and economies tends to standardize the vulnerabilities available to an adversary. Regulation and deregulation also contribute to growing vulnerability. For example, the Federal Communications Commission has mandated an evolution toward open network architecture—a concept which has as its goal the equal, user-transparent access via public networks to network services provided by network-based and non-network enhanced service providers. However, in execution, the concept makes network control software increasingly accessible to the users—and the adversaries. Implementation of the Telecommunications Act of 1996 will also require the carriers to collocate key network control assets and to increase the number of points of interconnection among the carriers. The Act also mandates third-party access to operations support systems, providing even more possible points of access to the critical infrastructure control functions. Similarly, the Federal Energy Regulatory Commission's recent Orders 888 and 889 directed the deregulation of the electric power industry. As part of Order 889, the electric utilities are required to establish an Open Access Same-time Information System (OASIS) using the Internet as the backbone.

Exhibit 2-4 illustrates the variety of network and computer system vulnerabilities which can be exploited, starting with simply making too much information available to too many people. The number of holes is mind-boggling—an indication of the complexity and depth of defensive information warfare task!

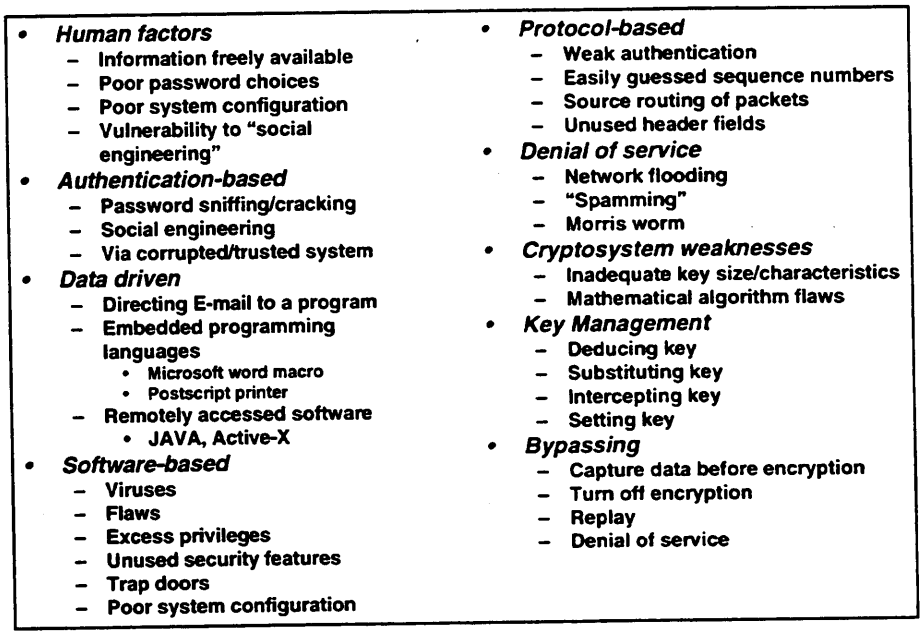


Exhibit 2-4. Vulnerabilities/Exploitation Techniques

Take, for example, "Remotely accessed software," which is found in the left column under "Data Driven." Distributed software objects, such as JAVA and Active-X, are the wave of the future. Rather than having software reside permanently in workstations or desktop computers, the Internet will make applications and data available as needed. The applications and data are deleted from the workstations or desktop computers after use. The danger of this just-in-time support is that the user has no idea as to what might be hidden in the code. Another aspect of distributed computing is that the definition of system boundaries becomes very blurred. This suggests considerable future difficulty in defining what can and cannot be monitored for self-protection, an implication discussed in Section 6.11, Resolve the Legal Issues, with legal recommendations.

The implication s that a risk management process is needed to deal with the inability to close all of the holes. Since this subject has been treated extensively by other study efforts (e.g., the Joint Security Commission) the Task Force elected not to examine risk management.

2.4 THREAT

There is ample evidence from the Defense Information Systems Agency and the General Accounting Office of the presence of intruders in DoD unclassified systems and networks. Briefings and reports to the Task Force have reinforced the DISA experience. Exhibit 2-5 shows some of the threats involved.

- ***Unknown intruders are in DoD networks and computers***
  - Services and DISA experience
  - GAO report
- ***U.S. networks and computers are of significant interest***
  - CIA, DIA, and NSA briefings
- ***FBI survey – "There is a serious problem"***
- ***Threat to the public switched network is significant***
  - NCS and NSTAC
- ***Growing interest in sharing sensitive information***
  - Government and industry Network Security Information Exchanges
  - DoJ Industry Information Center
  - Etc.
- ***We can't let our confidence in technological superiority blind us to a growing threat***

Exhibit 2-5. The Threat is Real

The "1996 CSI/FBI Computer Crime and Security Survey," released to the public earlier this year, concluded that "there is a serious problem" and cited a growing number of attacks ranging from "data diddling" to scanning, brute-force password attacks, and denial of service. The National Communications System and the President's National Security Telecommunications Advisory Committee have been warning since 1989 that the public switched network is growing more vulnerable and is experiencing a growing number of penetrations. There is also a growing interest in sharing sensitive vulnerability information among private sector companies, among government agencies, and between government and the private sector. However, sometimes the technology success we have achieved and our faith in our technological superiority blinds us to the growing threat and to our own vulnerabilities. Exhibit 2-6 depicts the Task Force view of the threat.

	Validated* Existence	Existence Likely but not Validated	Likely by 2005	Unlikely before 2005
Incompetent	W			
Hacker	W			
Disgruntled Employee	W			
Crook	W			
Organized Crime	L		W	
Political Dissident		W		
Terrorist Group		L	W	
Foreign Espionage	L		W	
Tactical Countermeasures		W		
Orchestrated Tactical IW			L	W
Major Strategic Disruption of United States				L

* Validated by DIA

W = Widespread; L = Limited

Exhibit 2-6. Threat Assessment

The incompetent threat is an amateur that by some means (perhaps by following a hacker recipe or by accident) manages to perform some action that exploits or exacerbates a vulnerability. This category could include a poorly trained systems administrator who assigns privilege groups incorrectly, which would then allow a more nefarious threat to claim more privileges on a system than would be warranted.

The hacker threat implies a person with more technical knowledge who to some degree understands the processes used and has the intent to violate the security or defenses of a target to one degree or another. The hacker threat is broad in motivation, ranging from those who are mostly just curious to those who commit acts of vandalism.

The disgruntled employee threat is the ultimate insider threat: the individual who is inside the organization and trusted. This threat is the most difficult to detect because insiders have legitimate access.

When examining the potential for information warfare activities, the potential for a criminal or non-governmental attack for economic purposes must be considered. Information is the basis for the global economy. Money is information; only approximately 10 percent of the time does it exist in physical form. As information systems are increasingly used for financial transactions at all levels, it is natural to expect all levels of criminals to target information systems in order to achieve some gain.

The increasing interconnectivity of information systems makes them a tempting target for political dissidents. Activities of interest to this group include spreading the basic message of their cause by a variety of means as well as inciting others to actions. An example is the political dissident in this country who sent out e-mails urging folks to send e-mail bombs to the White House server.

By attacking those targets in a highly visible way, the terrorist hopes to cause the media to provide a great deal of publicity of the action, thereby further disseminating the message of fear and uncertainty.

A significant threat that cannot be discounted includes activities engaged on behalf of competitor states. The purpose behind such attacks could be an attempt to influence U.S. policy by isolated attacks; foreign espionage agents seeking to exploit information for economic, political, or military intelligence purposes; the application of tactical countermeasures intended to disrupt a specific U.S. military weapon or command system; or an attempt to render a major catastrophic blow to the United States by crippling the National Information Infrastructure.

It is necessary to distinguish between what a layman might consider a "major disruption," such as the three New York airports simultaneously being inoperable for hours; and a "strategic" impact in which both the scope and duration are of dramatically broader disruptions. The latter is likely to occur at a time in which other contemporaneous events make the impact potentially "strategic," such as during a major force deployment.

The Task Force struggled with the issue of what would truly constitute a "strategic attack" or "strategic" impact upon the United States. The old paradigms of "n" nuclear weapons, or threats to "overthrow the United States per se," were marginally helpful in understanding the degree to which we are vulnerable today to Information Warfare attack in all of its dimensions. Couple this issue with the difficulty in assessing the real impact of cascading effects through our infrastructures; on the one hand as being major nuisances and inconveniences to our way of life, or on the other hand, as literally threatening the existence of the United States itself, or threatening the ability of the United States to mount its defenses.

The Task Force concluded that, in this new world, an event or series of events would be considered strategic either because the impact was so broad and pervasive, or because the events occurred at times and places which affected (or could affect) our ability to conduct our necessary affairs. One example we used to illustrate this latter point was a disruption in the area phone, power, and transportation systems coincident with our attempts to embark and move major military forces through that area to points abroad.

Few members of the Task Force felt that the power failures in several contiguous Southwestern states this summer were a "major disruption" or of "strategic impact" on the United States. Clearly they were inconveniences. However, had we reason to believe that the outages had been knowingly orchestrated by adversaries of the United States, this nation would have been outraged.

An issue related to our perceived vulnerabilities is the ability of an adversary to actually plan and execute Information Warfare so that it creates the desired impact. Our Task Force had many enlightening discussions about the potential for effects to cascade through one infrastructure (such as the phone system) into other infrastructures. This example is particularly important because most of our other infrastructures ride on the phone system. No one seems to know quite how, where, or when effects actually would cascade; nor what the total impact might be. The Threat and Vulnerabilities Panel concluded that if, with all the knowledge we have about our own systems, we are unable to determine the degree to which effects would multiply and cascade; an adversary would have a far more difficult task of collecting and assessing detailed intelligence of literally hundreds, if not thousands, of networked systems in order to plan and successfully execute an attack of the magnitude which we would consider to be "strategic." The very complexity and heterogeneity of today's systems provide a measure of protection against catastrophic failure, by not being susceptible to the same precise attacks. Presumably, the more kinds of attacks required, the harder it would be to induce cascading effects that would paralyze large segments of this nation. This is not to say that significant mischief is unlikely. It does suggest that the risk of an adversary planning and predicting the intended results at the times and places needed to truly disrupt the United States is considered low for approximately the next decade.

The trade and news media regularly report on the penetration of businesses and financial institutions by organized crime to steal funds, the theft of telecommunications services, the theft of money via electronic funds transfer, and the theft of intellectual property to include foreign

government-sponsored theft and transfer to offshore competitors of intellectual property from U.S. manufacturing firms.

The media also reports instances of disgruntled employees, contract employees, and ex-employees of firms using their access and knowledge to destroy data, to steal information, to conduct industrial espionage, invade privacy-related records for self-interest and for profit, and to conduct fraud. (An MCI employee electronically stole 60,000 credit card numbers from an MCI telephone switch and sold them to an international crime ring. MCI estimated the loss at $50 million.) Malicious activity by "insiders" is one of the most difficult challenges to information assurance.

DISA reported that it responded to 255 computer security incidents in 1994 and to 559 incidents in 1995. Of these, 210 were intrusions into computers, 310 were virus incidents, and 39 fell into another category. This is probably just the tip of a very large iceberg. Last year, DISA personnel used "hacker-type" tools to attack 26,170 unclassified DoD computers. They found that 3.6 percent of the unclassified computers tested were "easily" exploited using a "front door" attack because the most basic protection was missing and that 86 percent of the unclassified computers tested could be penetrated by exploiting the trusted relationships between machines on shared networks. Worse, 98 percent of the penetrations were not detected by the administrators or users of these computers. In the 2 percent of the cases where the intrusion was detected, it was only reported 5 percent of the time. This works out to be less than one in a thousand intrusions are both detected and reported. These detection and reporting statistics suggest that up to 200,000 intrusions might have been made into DoD's unclassified computers during calendar year 1995.

Whatever the number, unknown intruders have been routinely breaking into unclassified DoD computers, using passwords and user identities stolen from the Internet, since late 1993. Once the intruders enter the computers masquerading as the legitimate users, they install "back doors" so that they can always get back into the computer. These intruders have gained access to computers used for research and development in a variety of fields: inventory and property accounting, payroll and business support, supply, maintenance, e-mail files, procurement, health systems, and even the master clock for one-fourth of the world. They have modified, stolen, and destroyed data and software and have shut down computers and networks.

Such intrusions are not limited to DoD. Information age "electronic terrorists" have penetrated commercial computers and data-flooded or "pinged" network connections to deny service and destroy data to further their cause: an environmental group sponsored such attacks to call attention to their message and to punish a business with which they disagreed.

In the early 1980s an intruder required a high level of technical knowledge to successfully penetrate computers. By the early 1990s automated tools for disabling audits, stealing passwords, breaking into computers, and spoofing packets on networks were common. These tools are easy to use and do not require much technical expertise. Most have a friendly graphical user interface (GUI); automated attacks can be initiated with a simple click on a computer mouse.

Such tools include:

RootKit — a medium technology software command language package which, when run on a UNIX computer, will allow complete access and control of the computer's data and network interfaces. If this computer is attached to a privileged network, the network is now in control of the RootKit tool set user.

SATAN — a medium technology software package designed to test for several hundred vulnerabilities of UNIX-based network systems, especially those which are client/server. However, the tool goes beyond the testing and grants access to privileged information and control using any of the vulnerabilities found.

WatcherT — a high technology Artificial Intelligence engine, which is rumored to have been created by an international intelligence agency. It is designed to look for several thousand vulnerabilities in all kinds of computers and networks including PCs, UNIX (client/server) and mainframes.

More sophisticated attacks include plain text encryption of programs and messages, that is using plain text to hide malicious code; disabling of audit records; mounting attacks that are encrypted and that come from multiple points to defeat security detection mechanisms; hiding software code in graphic images or within spreadsheets or word processing documents; the insertion, over time and by multiple paths, of multi-part software programs; the physical compromise of nodes, routers, and networks; the spoofing of addresses; the eavesdropping (installing "sniffers" on Internet routers) on telecommunications and networks to obtain addresses and passwords for subsequent downstream spoofing; and the modifications of packet transmissions on networks.

Hackers with a bent to cyber crime are actively recruited by both organized crime and unethical business men, including private investigators who want to access privacy-protected information. Such recruiting was intense at the hacker convention DEFCON III, held August 4 to 6, 1995, in Las Vegas. Such conventions also serve as a clearing house for hacker tradecraft. At DEFCON III sessions were held on hacking the latest communications protocols (ATM and Frame Relay); the development and distribution of polymorphic software code (code that dynamically changes and adapts to the computer it is installed on); the penetration of health maintenance organizations and insurance companies; and the vulnerabilities of telephone systems. New services such as electronic commerce, cyber cash, mobile computing, and personal communications services are already areas of intense criminal interest.

The hackers and the cyber criminals are very efficient. The current state of technology favors the attackers, who need only minimal resources to accomplish their objectives. They have accumulated considerable knowledge of various devices and commercial software by examining unprotected sites. This know-how and tradecraft is transportable and is shared on the 400-plus hacker bulletin boards, worldwide. This includes hacker bulletin boards sponsored by governments (for example, the French intelligence service sponsors such a board). These boards are also used to distribute very sophisticated user-friendly "point-and-click" hacker tools that enable even amateurs to attack computers with a high degree of success.

A CD-ROM entitled *The Hacker Chronicles, Vol II*, produced by P-80 Systems and available at hacker shows for $49.95, contains hundreds of megabytes of "hacker" and information security information including automated tools for breaking into computers. The package carries this warning notice:

> The criminal acts described on this disk are not condoned by the publishers and should not be attempted. The information itself is legal, while the usage of such information may be illegal. The Hacker Chronicles is for information and educational purposes only. All information in this compilation was legally available to the public [readily available on the Internet] prior to this publication.

Attacks are not just based on the use of smart tools. Simple social engineering—impersonation and misrepresentation to obtain information—remains very productive. The ruses are many: "cyber friend," providing a free software upgrade that has been doctored to circumvent security, a "customer" demanding and receiving support over the telephone from a customer-oriented firm.

Additional details on the Task Force assessment of the threat are provided in Appendix A, Threat Assessment.

The nature of the danger is evident in an assessment of the current risk, which is based on the presence of a threat; the vulnerabilities of our networks and computing systems; the measures available to counter an attack; and the impact resulting from the loss of critical information, information systems, or information networks. This is depicted in Exhibit 2-7.

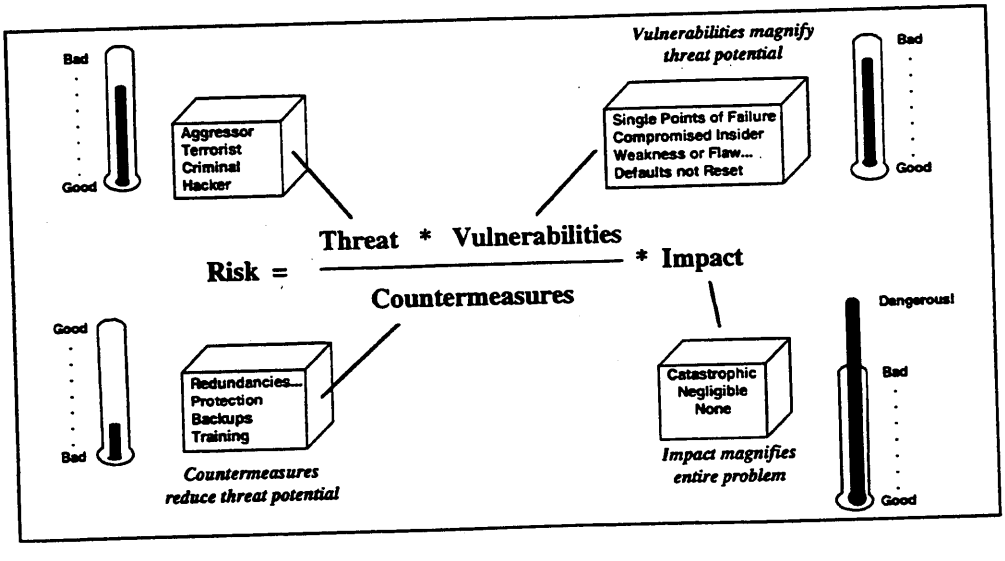


Exhibit 2-7. The Risk — A Clear and Present Danger

The Task Force believes that the overall risk is significant because of the following factors:

- The current threat is significant
- The vulnerabilities are numerous
- The countermeasures are extremely limited
- The impact of loss of portions of the infrastructure could have catastrophic effects on the ability of the Department to fulfill its missions.

SECTION 3

OBSERVATIONS

The Task Force agrees with the observation of the Deputy Secretary shown in Exhibit 3-1 below. This section discusses several areas in the Department and in the larger national security environment where we can make rapid progress on responding to this challenge.

- ***"This is not a problem we will solve. It is one we can get a handle on." – DEPSECDEF White***
- ***While information warfare is a national security issue that goes beyond DoD, it is warfare and DoD must play a major role.***
- ***Information warfare is different***
  - **IW attack objective is generally a critical function or a process - targets include**
    - **Information**
    - **Computers**
    - **Systems**
    - **Networks**
    - **Facilities**
    - **People**
  - **It's adaptive**

Exhibit 3-1. Initial Observations

The threat posed by information warfare is not limited to the realm of national defense, and the effort to control the problem must encompass broader national security interests, including Congress, the civil agencies, regulatory bodies, law enforcement, the Intelligence Community, and the private sector.

Unlike an attacker in conventional war, an attacker using the tools of information warfare can strike at critical civil functions and processes such as telecommunications, electric power, banking, or transportation and other centers of gravity or even at the stability of the social structure, without first engaging the military. Such a strategic information warfare attack can occur without forewarning or escalation of other events. In addition, attacks on the civil infrastructure could impede the actions of the military as much as a direct attack on the military's force generation processes or command and control.

However, we should not forget that information warfare is a form of warfare, not a crime or act of terror. The Secretary of Defense individually and the Department of Defense collectively, have two basic responsibilities—to provide for the "common defense" of the United States, and to be "ready to fight ... with effective representation abroad" [A National Security Strategy of Engagement and Enlargement, The White House, February 1996]. By first focusing on improving its ability to manage the information warfare challenge to the defense mission, the

Department can meet its national defense responsibilities while also enhancing its ability to play a significant role in defending against and countering a strategic information warfare attack on national centers of gravity.

Keep in mind that information warfare is not limited to attacks on computers: The potential targets of information warfare attacks can include information, information systems, people, and facilities that support critical information-dependent functions. The means of attack can be both cyber and physical. Finally, information warfare is adaptive and the practitioners learn from their experiences. While this phenomenon is not unique to information warfare, the speed at which the learning process takes place has no parallel in other forms of warfare.

Exhibit 3-2 suggests some additional ways in which information warfare is different from conventional warfare. Information warfare offers a veil of anonymity to potential attackers. Attackers can hide in the mesh of inter-networked systems and often use previously conquered systems to launch their attacks. The lack of geographical, spatial, and political boundaries in cyberspace offers further anonymity. Information warfare is also relatively cheap to wage as compared to conventional warfare, offering a high return on investment for resource-poor adversaries. The technology required to mount attacks is relatively simple and ubiquitous. During an information warfare engagement, the demand for information will dramatically increase while the capacity of the information infrastructure to provide information may decrease. The law, particularly international law, is currently ambiguous regarding the definition of criminality in and acts of war on information infrastructures. This ambiguity, coupled with a lack of clear designated responsibilities for defense, hinders the development of remedies and limits response options. Finally, deterrence in the information age is measured more in the resiliency of the infrastructure than in a retaliatory capability.

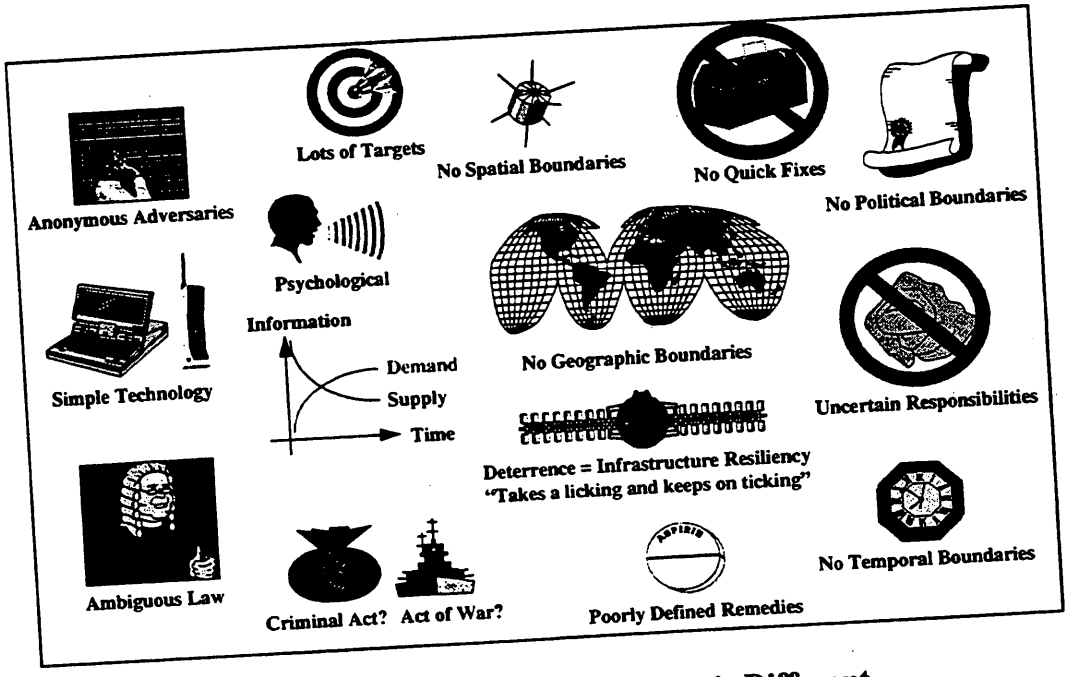


Exhibit 3-2. Information Warfare is Different

Exhibit 3-3 shows that information warfare has been particularly troublesome for the Intelligence Community because IW is a non-traditional intelligence problem. It is not easily discernible by traditional intelligence methods. Formerly, capabilities were derived from unique observables and indicators of military capability open to our sensors, amenable to cataloging in databases, and understandable by classic analytic techniques. With information warfare, however, the following elements come into play:

- **Relevant questions**
  - **What do we need to know? What should we look for? Where do we look?**
- **Traditional methods are not effective**
  - **Observables, indicators, experience, databases, analysis techniques, ...**
  - **Suggesting intent will be extremely difficult**
- **Key commercial technologies have lethal possibilities**
- **Technology is ubiquitous and relatively simple**
- **"Business" processes are complex**
- **HUMINT is still extremely important**
- **Required skill set much broader and deeper in educational level**
  - **Computer scientists, network engineers, electronics engineers, business process engineers**
  - **More MSs and PhDs**

Exhibit 3-3. Intelligence Community Observations

- The physical attributes of conventional and nuclear forces can be observed and quantified. The alert posture and movement of forces provided indications of potential threat. Our understanding of such patterns gained from long experience in observing known adversaries, the orders of battle stored in our databases, and the related analytic skills were well suited for understanding historic threats and from such insights we derived "intent." These skills are largely irrelevant in the information warfare environment.
- Now, key technologies designed for completely innocent applications can be used as weapons. For example, software used to test systems can also be used to penetrate systems.
- The technology required for information warfare is available everywhere.
- However, the "business" or "war" processes that must be penetrated to determine capabilities and intent are relatively complex, which means that human intelligence and counter-intelligence will continue to play a vital role. It is not easy to identify sources of attacks, intent, etc. in the information age.
- Finally, the technical skills required by our intelligence collectors and analysts in order to deal with these new challenges are much broader and deeper and more sophisticated than those required in the past. The intelligence community will require more personnel with advanced scientific degrees and a deep technical understanding of process, computer, and network design and of leading-edge technologies to meet the challenge adequately.

The Task Force derived a taxonomy of information warfare that describes information warfare. Unfortunately, as shown in Exhibit 3-4, in those cases where both objects and processes are present, this taxonomy would not scale in a linear manner beyond three levels. This is the result of the number of permutations and combinations by which the attacks could be mounted against a particular process, over variable time periods. The derivation of the taxonomy is discussed in Appendix C, A Taxonomy for Information Warfare?

However, by adopting concepts from Joint Pub sources and inputs of the Threat and Policy Panels of the Task Force, we developed a standard vocabulary for use in threat alerting and for the assessment and reporting of defensive preparedness, tied to specific information dependent processes. This vocabulary is discussed in Section 6, Recommendations.

- ***We lack a common vocabulary***
  - **Task Force could not find or derive a useful IW taxonomy**
    - **Scale, time factors, sequence of attacks, non-linear effects**
  - **Task Force proposes a standard vocabulary for IW-D readiness assessment and reporting and for threat warning**
- ***Resources are focused on classified content and systems***
- ***It is easy to make the IW-D problem too hard***
  - **Focus too broadly (GII/NII versus DII) or narrowly (definitions, legal)**
  - **Focus on solving political or social problems before addressing IW-D**
- ***Acquisition policy and practices pose dilemmas***
  - **Current practices trade off security**
    - **Functionality, performance, number of systems**
  - **Policy is clear**
    - **DoDD 5000.1 and DoDD 5000.2-R emphasize IW**

Exhibit 3-4. Additional Observations

Resources have been focused historically on protecting classified content and systems. These classified systems constitute only a very small percentage of the challenge.

Sometimes, we just make the problem too hard by failing to focus on what can and should be done. We can focus too broadly, too narrowly, or on the wrong problem set.

The reality of limited resources has fostered the current acquisition practice of trading off functionality, performance, and numbers of systems delivered to the operating forces at the expense of security. On a positive note, recent policy updates clearly state the need for attention to the information warfare aspects of systems acquisition. For example, DoDD 5000.1 indicates that acquisition programs should consider how systems security procedures and practices will be implemented and how the system will be able to respond to effects of information warfare. The Directive also calls for a C4I Support Plan for each system. The Task Force was disappointed to note, however, that the Support Plan does not include information warfare considerations. DoDD 5001.2-R also specifies that the operational requirements documents must include the characteristics the system must have to defend against and survive an information warfare attack.

Bottom line—policy exists, it is not yet uniformly implemented or enforced, and it requires resources in implementation.

Exhibit 3-5 suggests that infrastructure resilience has been demonstrated repeatedly during natural disasters, but overall robustness against a major IW attack is untested. Thus, national infrastructure recovery must be considered uncertain. Given the complexity and interconnected nature of our infrastructures, we really do not know the extent of our vulnerability. The possibility of cascading effects occurring throughout and between infrastructures certainly exists. This was adequately demonstrated in the 1991 regional long-distance telephone failures (attributed to a simple programming error), the recent West Coast power failures, and the 1988 Morris worm propagation throughout the Internet (damage was limited to UNIX systems demonstrating the value of system diversity). The Morris worm example is noteworthy in that warnings of the worm were often sent over the Internet because emergency response personnel did not have the telephone numbers of colleagues in other organizations to whom the warnings needed to be sent. In many cases, these electronic warnings carried the worm with them and aided the propagation of the worm.

- ***Cascading effects have occurred, are difficult to predict***
  - **Infrastructure robustness untested**
  - **Infrastructure recovery uncertain**
- ***Area and perimeter defenses are not sufficient!***
  - **Resiliency and repairability are critical to information survivability**
  - **Information domains are essential**
  - **Scale of IW-D for a distributed computing environment not well understood**
- ***Easy technical solutions are not apparent***

Exhibit 3-5. Additional Observations

The concept of protecting large portions of the information infrastructure is not valid. It is economically and technically impossible to close every possible vulnerability. We need to focus on designing a resilient and repairable information infrastructure. Our experience in designing highly reliable computer systems does not scale to a large, distributed information infrastructure. Our design practices are not based on the possibility of malicious events. We need to focus on establishing information domains within the information infrastructure, which will minimize cascading effects and which will enable us to contain the battle damage which might result from an information warfare attack. And, since we cannot yet effectively employ area and perimeter defenses, we do not really know what the implications of scale are in establishing an effective information warfare (defense) capability.

The Task Force does not want to imply that the various actions taken over the years by the information security or INFOSEC community do not have roles in IW defense. INFOSEC is an important contributor to achieving a robust information warfare defense capacity. Unfortunately, to many, INFOSEC has become shorthand for protecting the confidentiality of information.

Although important, the steps needed to ensure confidentiality are not adequate to achieving information assurance in an information warfare environment.

Encryption may be an example of trying to make the problem too hard, as shown in Exhibit 3-6. The nation has focused a lot of attention and energy on the encryption policy debate. Encryption simply does not solve all of the information security problems. The Task Force believes the policy debate has been a distraction from efforts to enhance the resiliency of the critical national information services.

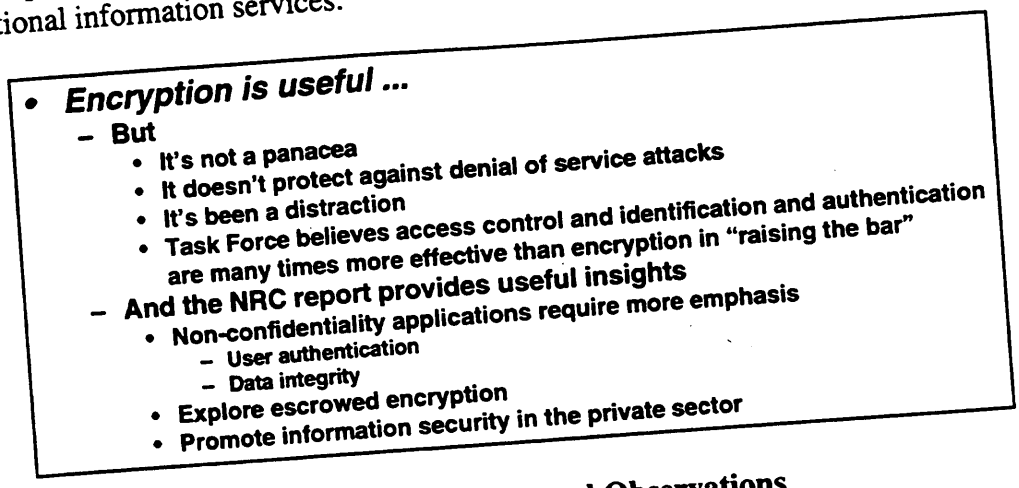


Exhibit 3-6. Additional Observations

The Task Force reviewed the NRC report and was briefed on the study effort. While the Task Force felt that the report provided some useful insights, namely that the non-confidentiality applications of encryption provide significant benefit for user authentication and data integrity, the Task Force also believes that access control and identification and authentication are more efficient than encryption in "raising the bar." It also suggests that escrowed encryption be explored and that attempts be made to promote information security in the private sector. On the basis of the review and briefing, the Task Force determined that a further detailed examination of the encryption issue would probably not yield any additional major insights.

The Computer Security Act of 1987, the recent Clipper debate, and the continuing encryption policy debate highlight the private sector and civil agency reservations about the role of DoD in the area of national information protection. Exhibit 3-7 shows this role.

Market forces are extremely powerful, but will not alone provide the capability desired. The market simply does not perceive the possibility of a strategic information warfare attack against information centers of gravity. The market is not sufficiently informed about the vulnerabilities and threat to make rational national security judgments. Further, there may be little economic motivation to invest in security or even strong market incentives to resist adding security. Where there is commercial awareness, it is focused on protecting against theft of data and services (e.g., credit card numbers, telephone service) and alteration of data (e.g., financial accounts). Denial of service attacks are not an area of major concern for commercial entities. Managing the problem will require some legislation, some additional regulation, some indemnification of the private

sector to achieve desired assurance goals, and some incentives (such as revisions to the tax structure).

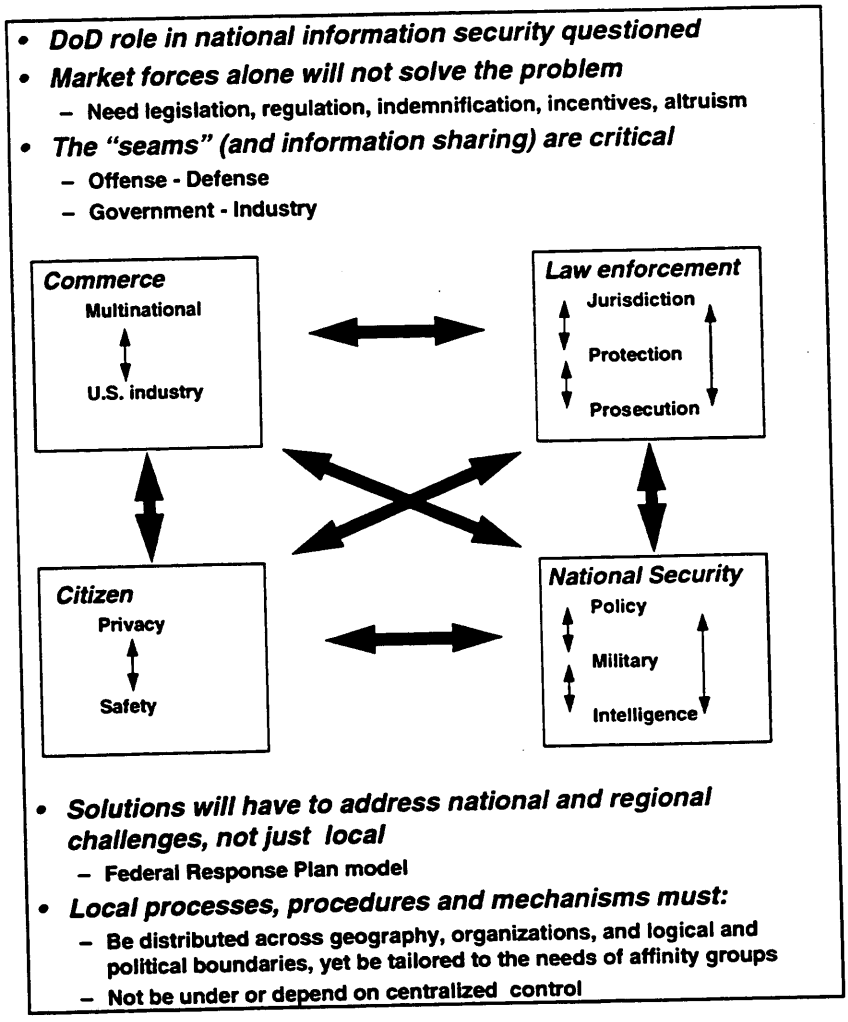


Exhibit 3-7. Additional Observations

The seams are critical. Currently, information necessary for an effective information warfare (defense) capability is not shared effectively across the seams. Information warfare (offense) is highly compartmented in spite of the fact that it shares common technology and operating environment with the information warfare (defense) community. In some cases, the military, law enforcement and intelligence communities are restricted by law, executive order, or regulation from sharing certain information. Historically, these communities are notoriously bad at sharing information. There are very few mechanisms for government and industry to share sensitive information such as vulnerabilities and intrusions. This lack derives primarily from the competitive sensitivity of information that is required for an effective information warfare (defense) capability.

In addition, at the national level, there are competing equities at stake in nearly every information warfare issue. Not only do these interests compete among each other, there are competitive

forces within each of the sectors. Some examples are shown for each of the four equities. Resolution of the information warfare (defense) issues at the national level will be a time-consuming and laborious process. While it may not be possible to balance the equities, the key is to provide a mechanism to discuss rationally and deal with the legitimate equities of the participants. Grappling with this problem on the national level will require a very broad perspective if we are to ensure that national, regional, and local interests are served.

While information warfare (defense) is an extremely complex problem set, there is a lot that can be done with a limited number of resources quickly. Many of the Task Force recommendations identify these possibilities, some of which are shown in Exhibit 3-8.

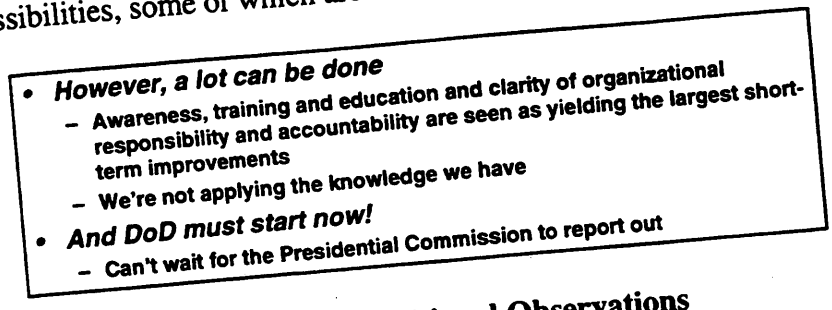


Exhibit 3-8. Additional Observations

Finally, DoD must start now to implement the recommendations of the Task Force. This is the third year in a row that a task force of the Defense Science Board has issued a call for action. The President's Commission will be occupied with issues that transcend the Federal government and the private sector. DoD cannot afford to wait for all of these higher level issues to be resolved before embarking on a concerted effort to grapple with those issues that are within the authority of the Secretary of Defense to address..

SECTION 4

WHAT SHOULD WE DEFEND?

Determination of what to defend should follow from our nation's vital interests as documented in the current national security strategy. On the basis of these interests, the Task Force postulated the goals shown in Exhibit 4-1. Given the available time, it was not possible for the Task Force to address each of these goals in detail. However, the Task Force did develop a set of national-level defensive information warfare interests based on these goals.

- ***Vital interests (A National Security Strategy of Engagement and Enlargement, The White House, February 1996)***
  - **Enhance our security with military forces that are ready to fight and with effective representation abroad**
  - **Bolster America's economic revitalization**
  - **Promote democracy abroad**

- ***Goals***
  - **Stable monetary, financial and banking systems which enjoy public confidence**
  - **Free trade**
  - **Continuity of government and constitutional authority**
  - **Personal privacy**
  - **Ability to deploy, employ and support military forces**
  - **Protected intellectual property**
  - **Venue for resolution of policy issues among government, individuals and the private sector**
  - **Availability of emergency services for any emergency, natural or man-made**
  - **National standards for "reasonable" protection regimes for public and private networks**
  - **Stimulate research, development and application of technologies for IW-D**

Exhibit 4-1. National Goals For Information Warfare (Defense)

Exhibit 4-2 indicates the national interests that must be defended. The emphasis is on defending critical functions and processes, not on defending forces, platforms, or geography. As was the case in developing an ensured means of control for the strategic nuclear deterrent, some critical information infrastructure capabilities must be isolated from the interconnected national and global information infrastructure to ensure it is available to support and manage the restoration of critical functions.

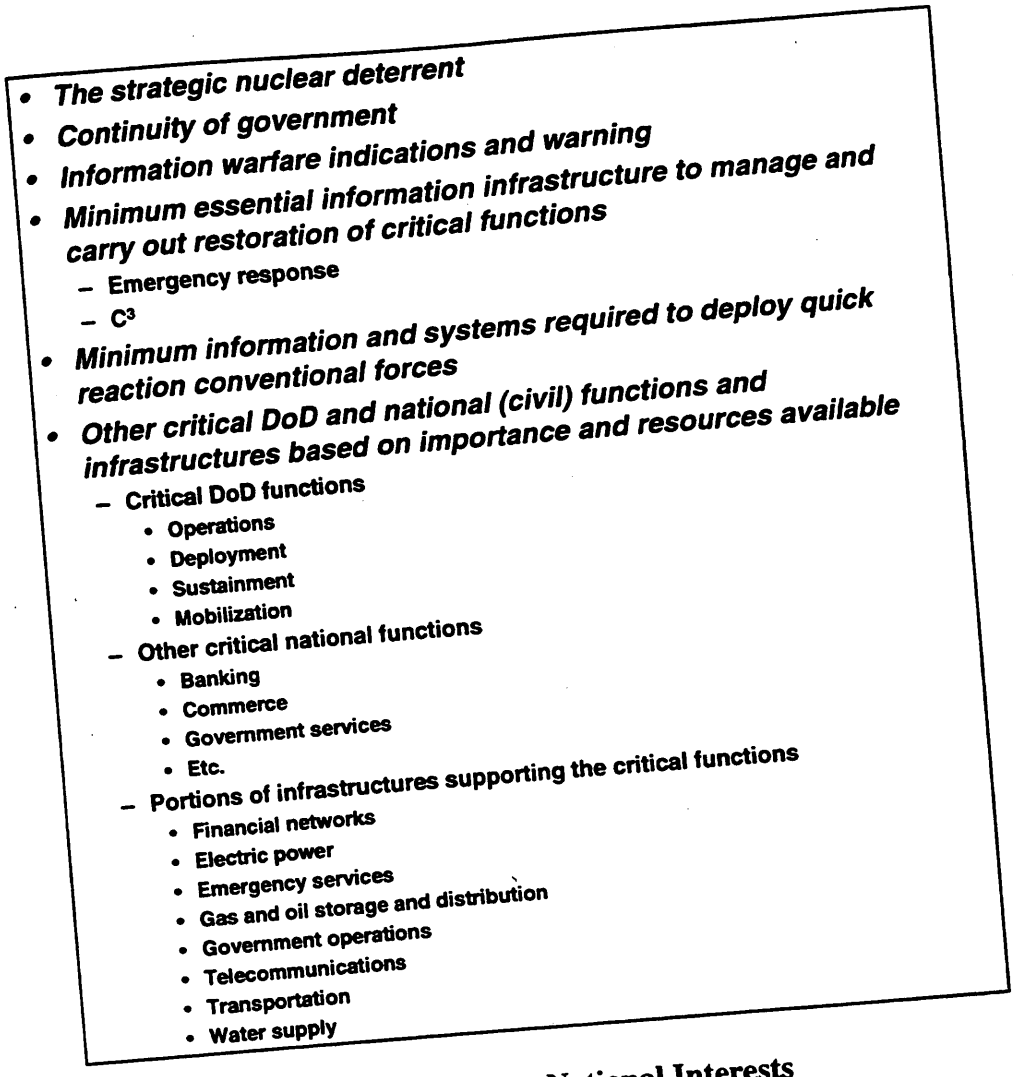


Exhibit 4-2. The National Interests

The Department must preserve its ability to fulfill its basic missions. To do that, DoD must be concerned about the ensured operation the critical functions and availability of information necessary to fulfill those missions. The intertwined nature of the functions and infrastructures make this very complex. Critical national functions that have possible national security implications must be defended, and those portions of the infrastructures that are necessary for the operation of critical DoD and national functions must also be defended.

SECTION 5

HOW SHOULD WE DEFEND?

5.1 PROCEDURES, PROCESSES AND MECHANISMS

Exhibit 5-1 depicts the essential procedures, processes, and mechanisms for IW-D. They are based on the defensive information warfare implementation model developed by the Information Assurance Division of the Joint Staff J6. An essential step in preparing an information warfare defense is the identification of critical national information functions and the information, information services, and infrastructures upon which these functions depend.

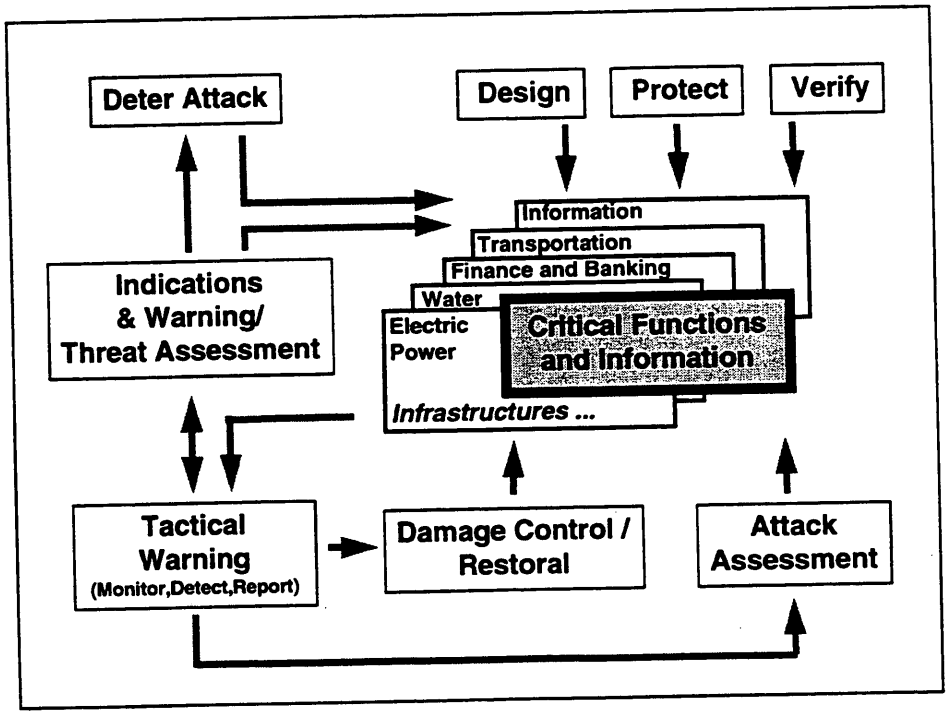


Exhibit 5-1. Procedures, Processes, and Mechanisms

The first order of business is to deter information warfare attacks. This deterrence must include a national will as expressed in law and conduct, a declaratory policy on consequences of an information warfare attack against the United States, and an indication of the resiliency of the information infrastructure to survive an attack.

The most immediate need is to provide some form of protection. This protection might include physically isolating information, providing some form of access control and authentication of personnel performing critical functions or accessing information, or encryption of the information. As time permits, the information infrastructure supporting critical functions should be designed for utility, resiliency, repairability, and security. An equally important function is to verify through independent assessments that the design is being followed, that protective

measures are being implemented where appropriate, and that the information warfare (defense) readiness posture is as reported.

As suggested in the Task Force observations, the importance of intelligence support to information warfare (defense) cannot be overemphasized. This support must include strategic indications and warning of potential information warfare attack, timely and accurate threat assessments, and current intelligence support in the event of an information warfare attack.

The essence of tactical warning is monitoring, detection of incidents, and reporting of the incidents. Monitoring and detection of infrastructure disruptions, intrusions, and attacks are also an integral part of the information warfare (defense) process. Providing an effective monitoring and detection capability will require some policy initiatives, some legal clarification, and an ambitious research and development program, all of which will be addressed later in the report. All intrusions and incidents should be reported so that patterns of activity can be established to aid in strategic indications and warning. The FCC requirement to report telephone outages of specified duration affecting more than a specified number of customers serves as a model in this regard.

It is probable that the telecommunications infrastructure will be subject to some form of attack. We should have some capability to limit the damage that results and to restore the infrastructure. Little research has been devoted to the basic procedures necessary to contain "battle" damage, let alone to the tools which might provide some automated form of damage control. Restoration of the infrastructure assumes some capability to repair the damage and the availability of resources such as personnel, standby services contracts, and the like.

Finally, information warfare (defense) should include some form of attack assessment to aid in determining the impact of an attack on critical functions and in determining the appropriate response to an attack.

A key point not reflected in the exhibit is that this process must be a distributed process. The basic functions of monitoring, detection, damage control, and restoration must begin at the lowest possible operating level. Reports of the activity must be passed to regional and DoD-level organizations to establish patterns of activity and for assistance as needed in damage control and restoration.

5.2 STRATEGY

We will use the following strategy to achieve this capability for the Defense Information Infrastructure:

- Address infrastructure, not just system or network, protection. The design of systems an networks is generally based on efficiency considerations. Infrastructure protection must be based on effectiveness considerations.
- Manage DII risk. It is impossible to pay the cost of avoiding risk to the DII. Protection of the DII must be based on both effectiveness and efficiency considerations.

- Protect information commensurate with its intended use. In certain circumstances, unclassified but sensitive information (weather and terrain data) may have more tactical significance than classified information (e.g., outdated intelligence estimates).
- Integrate policy, technical, operational, and personnel aspects. Each of these aspects is treated separately for the various communications, information, and security disciplines. They must be integrated for both efficiency and effectiveness.
- Use Service/Agency core competencies. All ongoing relevant activities must be reviewed to preclude reinventing the wheel.
- Build on current programs and initiatives. Use the ongoing information security activities and programs and those of related security disciplines as the foundation for achieving an IW-D capability.
- Emphasize solutions to the traditional weak link—the person. Nearly all espionage convictions are based on an inside threat. IW-D activities must address this issue head on.
- Harmonize IW-D, OIW, INFOSEC, and intelligence support functions. These closely related functions are based on many common technologies and processes and must be mutually supporting.
- Harmonize activities to protect the NII, the GII, and the DII. Work toward a consistent approach and economies of scale in protecting these highly interconnected infrastructures.
- Conduct vigorous interagency coordination. The rapidly evolving and highly complex DII requires proactive measures to preclude duplication of effort and contradictory goals.

SECTION 6

RECOMMENDATIONS

The key recommendations are those which can be implemented by the Secretary of Defense. Other recommendations are included which the SECDEF should make to the Director of Central Intelligence, and those which relate to the President's Commission on Critical Infrastructure Protection or the Infrastructure Protection Task Force.

6.1 DESIGNATE AN ACCOUNTABLE IW FOCAL POINT

This is the most important recommendation the Task Force has to offer. Multiple lead organizations with no clear principal staff assistant have led to confusion and slow progress to date. Boards and councils are important for discussing the issues, but have not and cannot provide the needed focus. Although many of the tools used to carry out information warfare have been around for a long time, the nature of information-dominated societies and activities makes it appropriate to view information warfare as a new warfare area. Information warfare is not the sole responsibility of the Chief Information Officer, the Assistant Secretary of Defense for C3I, the Director of Central Intelligence, the Chairman of the Joint Chiefs of Staff, the Secretaries of the Military Departments, or the Service Chiefs. Each of these is, however, responsible for a portion of this new warfare area. The Secretary of Defense, however, needs a single person and office to plan and coordinate this complex activity, as well as to serve as a single focal point charged to provide staff supervision of the complex activities and interrelationships involved. This includes oversight of both offensive and defensive information warfare planning, technology development, and resources. Given the interconnected nature of the information infrastructures, it is critical that the left hand knows what the right hand is doing and that these complex activities are coordinated.

This single focal point should be required to report regularly on the state of the areas shown and provide the informed interaction to other interagency and intergovernmental IW-related activities as shown in Exhibit 6-1.

- *Confusion and slow progress to date*
- *Boards and councils have not provided a focus*
- *Information warfare is a new warfare area*
  - It is not Intel, C2, CIO
- *Charge focal point to "pull it all together"*
  - Staff supervision of both offensive and defensive IW
  - Promulgate integrated policy
  - Ensure development of information warfare theory, doctrine and practice
  - Assess and report regularly to the SECDEF/DEPSECDEF on
    - Policy and plans
    - Preparedness
    - Intelligence support
    - Allocation of resources to IW
  - Interface to interagency/intergovernmental activities

Action:

- Designate ASD(C3I) as the accountable focal point for all IW issues
  - Develop a plan and associated budget beginning in FY 97 to obtain needed IW-D capability
  - Report annually to the SECDEF on IW status
  - Authorize issuing of instructions
  - Long view suggests USD(Information)
- Establish a DASD(IW) and supporting staff (ASD(C3I) lead)
  - Bring together as many functions as possible

Exhibit 6-1. Designate an Accountable IW Focal Point

The Task Force recommends that the Secretary of Defense designate a focal point for the coordination of information warfare. While the focal point could be any of the existing Under Secretaries or Assistant Secretaries, the Task Force recommends that the focal point be the Assistant Secretary of Defense for C3I. The first order of business for the focal point should be to develop a plan of action to obtain the needed capabilities. The focal point should also report the Department's IW status annually to the SECDEF. The focal point should be given authority to issue instructions. The long view suggests the eventual need for an Under Secretary of Defense for Information. While the Task Force does not make such a recommendation at this time, there was strong sentiment within the Task Force in support of organizing for the long view. The Task Force also recommends that a Deputy Assistant Secretary reporting to the ASD(C3I) be named and provided an adequate supporting staff to assist in providing the necessary staff oversight and coordination of information warfare activities. The Task Force hope is that as many IW-related functions as possible would be consolidated under this individual.

6.2 ORGANIZE FOR IW-D

Before discussing specific organizational recommendations, this section briefly discusses what the Task Force views as necessary capabilities for IW-D. Exhibit 6-2 shows the capabilities the Task Force determined are necessary for an effective information warfare (defense) and which are not adequately addressed in the Defense Department's current information warfare (defense) planning.

1. ***Intelligence indications and warning, current intelligence and threat assessment***
2. ***Operations (911)***
3. ***Planning and coordination (411+)***
4. ***System, network and infrastructure design***
5. ***Independent assessments***

Exhibit 6-2. Organize for IW-D

Section 3, Observations, addressed the need for intelligence indications and warnings, current intelligence, and threat assessment. A specific recommendation which addresses the needed improvements in intelligence support to information warfare (defense) follows.

"Operations" as used in Exhibit 6-2 is shorthand for those time-sensitive activities necessary for dealing with an actual intrusion or attack. While not fully analogous, the Task Force sometimes refers to these capabilities as 911 or emergency response capabilities. Remember that these operations capabilities must be distributed throughout the Department—down through the Military Departments and Services and the Defense Agencies and through the CINCs to the operating forces.

"Planning and coordination" is shorthand for preparedness activities. The Task Force has taken to referring to these capabilities as enhanced 411 or 411+ capabilities. Once again, the analogy is not completely accurate since it does not convey what will certainly be a broader interactive capability, but it does help to make quick associations with intended capabilities.

One of the more critical needs is a continued capability to obtain an independent assessment of our information warfare (defense) posture. While these assessments can be carried out at any level, it is felt that there should be a capability established which is accountable directly to the SECDEF/DEPSECDEF. In addition, the organization established to provide this capability should be staffed with people who are knowledgeable of all types of threats and of both the DoD and private sector environments.

6.2.1 Establish a Center For Intelligence Indications and Warning, Current Intelligence, and Threat Assessments

Current intelligence resources and processes are not optimized to provide an understanding of threats and potential adversary capabilities to conduct Information Warfare; nor are they presently capable of providing either Indications and Warning or Attack Assessment of Information Warfare. An understanding of the IW process and indications of an IW attack will most probably require an unusual amalgamation of otherwise seemingly unrelated sets of data. The lack of previously identified and validated indicators for IW creates several additional difficult dimensions to the problem facing the Intelligence and Defense communities' efforts to understand all aspects of IW.

The United States has, over nearly four decades, identified many sets of data comprising indicators of activities by potential adversaries (communist-bloc). These indicators have provided the foundation of our intelligence assessment and indications and warning processes. Examples of these include known and understood development processes and cycles for military equipment's ranging from ICBMs to submarines to bomber aircraft. Thus, if we observed earth spoil on overhead imagery indicating a possible new heavy ICBM silo was under construction, we could adjust our threat understanding accordingly. Similarly, we might observe Soviet Missile Range Instrumentation Ships moving toward areas of the Pacific Ocean known (from prior observations) to be used by Russia as an impact area for ICBM tests; and we would conclude that a missile test was in the offing. Or, if a Mediterranean nation began to import chemicals which could be used either in fertilizer or in chemical agents for war; we could be on the alert for other indications of chemical gas production such as special buildings, storage facilities or personalities known to possess technical knowledge necessary to produce chemical weapons.

In a more operational vein, over time, we began to understand communist-bloc strategy, doctrine, and tactics as well. All of this knowledge was gained from a series of observations over several years. We were able to use this knowledge as we planned for combat and designed and executed wargames. Over four decades, with the expenditure of billions of dollars for collection, analysis, and reporting systems were optimized to deal with these known, discrete indications of activity. These "known indicators" permitted us to conduct intelligence assessments, Indications and Warning, and in some cases, attack assessments.

There were several factors involved in our gathering these data sets. The first is that we (and others) have made enough similar observations to establish "patterns of activity." Secondly, these observations have either caused us, or permitted us, to identify a number of discrete activities that we conclude are indicative of the "entire pattern," or significant segments of the pattern. Thirdly, having noted one or more of the discrete indicators, we know what other indicators to look for to corroborate our suspicions.

Information Warfare is a whole new game from the Intelligence dimension. We have precious few real data from which to derive "patterns of activity." This is made all the more difficult because so many of the "indicators" we have used in the past have involved some physical

phenomena. In IW, at least in the computer and networked components of it, evidence of IW is fleeting at best and is usually not physically observable. The Intelligence Community is working hard to address some of these issues; but progress is hampered by organizations, processes, and systems optimized for situations found in the past, not the future. Evidence of IW preparations or attacks is most likely to come from a wide variety of sources and venues: from the more than 50 Computer Emergency Response Teams (CERT) around the world, from nodes of different segments of our National Information Infrastructure, from academia, from the Internet, from law enforcement agencies, from FEMA, and of course from traditional Intelligence Community resources such as human, signals, and open source intelligence. The Defense Science Board believes that some new approaches to collection and analysis are urgently needed.

The intelligence community understands as well as any that they face a tremendous challenge in developing information-age intelligence support activities. Some of the Task Force observations regarding these challenges were discussed earlier in the report and are shown in Exhibit 6-2-1. It is no easy matter to pinpoint the requirements, identify observables, establish patterns and indicators of the patterns, identify sources of the indicators, or determine how the sources will be exploited to collected information necessary to develop the indicators.

- ***Functions***
  - **Identify requirements, observables, patterns, indicators, sources, collection methods**
  - **Develop analysis techniques, data bases, threats**

Action: SECDEF formally request the DCI :

- **Establish an I&W/TA center at NSA with CIA and DIA support**
- **Task and resource the intel community to develop the processes for Current Intelligence, I&W/TA for IW-D**
- **Encourage the intel community to develop information-age trade craft, staff with the right skills, and train for the information age.**
- **Conduct comprehensive case studies of U.S. offensive programs and a former foreign program to identify potential indicators - collection, funding, training, etc.**
- **Establish an organization to examine and analyze probable causes of all security breaches**
  - **Goal is to identify improved and cost effective security practices**
  - **Must have full access to all pertinent information and people, procedures, facilities (all sources)**
  - **Findings will not be used for administrative or legal action**
- **Develop and implement an integrated National Intelligence Exploitation Architecture to support the organization and processes**

Action: SECDEF

- **Direct development of IW Essential Elements of Information (EEI) (ASD(C3I) lead)**

Exhibit 6-2-1. Establish a Center for Intelligence Indications and Warning, Current Intelligence, and Threat Assessments

The recommendation to establish the center at NSA recognizes their role in electronic intelligence and is meant to build upon recent organizational efforts at NSA. However, NSA must be augmented by DIA and CIA personnel because of the extensive social engineering component of information warfare. The Task Force believes it is essential to keep separate the intelligence and operations functions. The reason for the separation is that these functions are different. The intelligence community focuses on strategic warning and the operations community focuses on continuity of service and the warning and response to immediate danger.

The Task Force believes the recommendations in Exhibit 6-2-1 are key to improving the intelligence support to defensive information warfare. While there has been some activity in these areas, the whole process needs a significant jump start. In addition, representatives from the intelligence community pointed to the lack of Essential Elements of Information (EEIs) from the operational community as a contributing factor to the intelligence challenge. This should not be an inhibitor to progress.

There may, in fact, be a need to form a National Center for Indications and Warning. This center would gather and analyze monitoring data continuously. The data would be derived from commercial infrastructure systems as well as government. The center could be charged with searching for and detecting early signs and precursors of a wide scale, coordinated attack and with providing warnings to U.S. government and private sector organizations. Toward that end, a phased approach would be appropriate, beginning with a DoD-specific organization which is scalable and extensible, and evolving towards a pan-government and private sector organization. Roles of the organization should include gathering and analyzing of voluntarily contributed data, disseminating of findings, and acting as a clearing house to coordinate feedback and responses from the community.

6.2.2 Establish a Center for IW-D Operations

The basic required defensive information warfare operations functional capabilities are shown in Exhibit 6-2-2. The terms tactical warning and attack assessment are familiar to the strategic nuclear forces. They fit in the information warfare context consistent with the definitions in Joint Pub 1-02, Dictionary of Military Terms. Providing these capabilities in the information-age context, however, is very different than the nuclear era. Emergency response and infrastructure restoration are self-explanatory.

- ***Functions***
  - **Tactical warning (monitor, detect, report)**
  - **Attack assessment (analyze, organize defenses)**
  - **Emergency response (control damage, reallocate infrastructure assets)**
  - **Infrastructure restoration**
- ***Support CJCS initiative to establish***
  - **Military IW operations center (J3 cell, Joint Information Warfare Center)**
    - **Support IW aspects of deliberate planning, exercises, and operations**
    - **Serve as time-sensitive IW point of contact for CINCs (911)**
    - **Serve as IW information source and clearinghouse for CINCs and operations forces**
    - **Provide operational liaison with counterpart federal, state and local agencies on matters of immediate relevance to current military operations or exercises**
  - **CINC IW cells**
    - **Support planning for and conduct of CINC IW activities**

Action (ASD(C3I) lead with CJCS support):

- **Establish a DoD IW-D operations center (*911*) at DISA with NCS, NSA, and DIA support.**
- **Develop/implement distributed tactical warning, attack assessment, emergency response, and infrastructure restoration procedures**
  - **Incorporate national guard, reserves, mobilization augmentees, contractor support**
  - **Mandate reporting of all suspected intrusions and computer incidents affecting DoD systems and networks**
- **Interface with Service and Agency capabilities and I&W/TA support**
- **Establish necessary liaison (e.g., military and government operations centers, service providers, intelligence agencies, computer emergency response centers)**

Exhibit 6-2-2. Establish a Center for IW-D Operations

The Chairman has already undertaken an effort to establish a military operations center and has instructed the CINCs to establish IW cells within their staffs. The military operations center will consist of two elements. First, a small cell will be established in the J3 and will be staffed during normal duty hours. During crises, the J3 cell will have specific authorities over the second element, the Joint Information Warfare Center. The Joint Information Warfare Center will be staffed 7 days a week, 24 hours a day, and will serve as the interface to organizations such as the CINC IW cells, the Joint Spectrum Center, the Joint Warfare Analysis Center, the Joint Command and Control Warfare Center, and the Service IW organizations.

The distinction to be made between the military IW center and the defensive information warfare operations center is that the military center will focus on military operations of a time-sensitive nature. The defensive information warfare center will be focused on the Defense Information Infrastructure and other critical infrastructures as appropriate.

While the Task Force recommends that the center be established at DISA, current technology certainly provides for establishing a virtual center. This virtual center would draw on support from geographically dispersed elements. Initial staffing should come from existing assets. As

suggested earlier, this operations capability must be distributed down and throughout the Department, linking, for the most part, existing operations centers, emergency response teams and so on. The Task Force envisions eventual links to other government centers including any that may result from the actions of the Infrastructure Protection Task Force recently created by Executive Order 13010.

Establishing the center is relatively easy. Developing and implementing the process and procedures to be used will be much more difficult; there has been almost no effort devoted to this area. One suggestion the Task Force makes is that eventual staffing and procedures take advantage of technical expertise available in the national guard, the reserves, mobilization augmentees, and contractors. Mandatory reporting sounds easy but may be difficult to implement because of a basic fear by those reporting that they will be held accountable for the intrusion or incident and that they will have to pay to fix the problem. Mandatory reporting may have to be accompanied with some form of inducements such as a "fix it free" offer. It will also be necessary to distribute these capabilities throughout the Department and establish an information channel with the indications and warning/threat assessment center for sharing of information essential to the performance of each center's mission.

If national-level centers for infrastructure protection are established as a result of the recommendations of the President's Commission on Critical Infrastructure Protection, then the Department should ensure appropriate interfaces are established between DoD functions and these centers.

The tentacles of this Operations Center should be virtually extended to every organization in DoD, ranging in scope from a single person serving as point of contact for the organization to having an emergency response cell located with the organization.

DISA should establish a threshold of information event that requires reporting to the Operations Center. Every information event reaching that threshold must be reported and penalties established to enforce that reporting. DISA should maintain a knowledge base of that reporting and ensure all response personnel are appropriately trained and informed.

6.2.3 Establish a Center for IW-D Planning and Coordination

The role of the planning and coordination center, shown in Exhibit 6-2-3, will be to support the ASD(C3I) in fulfilling his responsibilities as the focal point and to facilitate the sharing of sensitive information within the Department, among the Federal departments and agencies, and with the private sector.

- ***Functions***
  - **Develop IW planning framework**
  - **Assess**
    - **IW policy and plans**
    - **IW preparedness**
    - **Intelligence support**
    - **Allocation of resources to IW**
    - **IW incident reports**
  - **Develop procedures and metrics for assessing infrastructure and information dependencies**
  - **Facilitate sharing of sensitive information (e.g. threats, vulnerabilities, fixes, tools, techniques) within DoD and among government agencies, the private sector service providers and professional associations.**

***Action** (ASD(C3I) lead):*

- **Establish an IW-D planning and coordination center (*411+*) reporting to the ASD(C3I) with interfaces to the intelligence community, the Joint Staff, the law enforcement community, and the operations (911) center**

Exhibit 6-2-3. Establish a Center for IW-D Planning and Coordination

One of the first activities of the planning and coordination center should be to establish a planning framework which can provide for meaningful assessments of progress in information warfare preparedness. This center will not write plans for the CINCs, Services, and Defense Agencies, but will identify the need and means for integrating information warfare considerations into traditional planning activities.

The center will aid the focal point in assessing the treatment and implications of information warfare in policy and plans, operations, and the allocation of resources to information warfare. The center will also analyze and assess IW-related incident reports generated by the Services and Agencies and forwarded to the 911 operations center. The assessment will determine patterns of activity that might indicate the need to revise plans or resource allocations.

Since there is no established method for assessing the dependency of operations plans and DoD support activities on information and infrastructures, the center will need to develop the procedures and metrics for such assessments. The military operations community and the functional support community will perform the assessments. These infrastructure dependency assessments will be discussed in more detail later in this report.

Sharing of sensitive information is probably one of the most important first steps in building a defensive information warfare capability. There are significant legal, regulatory, competitive and emotional hurdles to overcome; these must be addressed as soon as possible.

6.2.4 Establish a Joint Office for System, Network and Infrastructure Design

It is not necessary to break the cryptographic protection to attack our classified computing environments. The protection paradigm used by DoD is based upon the classification of information. However, most classified computer systems contain, and often rely on, unclassified

information. This unclassified information often has little or no protection of the data integrity prior to entry into classified systems. The expected interaction between GCCS and GTN are examples of this. An increasing number of DoD systems contain decision aids and other event-driven modules. These should be buffered from unclassified data whose integrity cannot be verified.

Second-, third-, and "n" -order effects from an information warfare attack have not been observed and are not well understood. Further, good data are not available with which to conduct modeling and simulation of such effects. Data must be collected to support the modeling and simulation of the effects of specific information warfare attacks and defenses. Detailed data should be gathered through several means:

- Measure the specific local effects of a standard battery of attacks on common components such as operating systems, firewalls, routers, etc. Experiments should be conducted using various configurations and settings of the components and attack variations for as complete a picture as possible.

- Measure the effects and possible consequences for a standard battery of attacks against many common configurations of generic networked systems. The technologies and configurations selected for these experiments should be common to a large percentage of the DII and NII, including telecommunications, power, and control systems. Again the attacks should be carried out in multiple variations against multiple target system types and configurations, with various types of defenses, to obtain accurate data on the measurable effects of attacks in all these circumstances.

- Measure the effects and possibly consequences for a battery of attacks, that could include application-specific attacks, on stereotypical defense systems. Measure the effects on mission effectiveness.

To achieve the goal of protecting information systems from future IW attacks, a comprehensive, principled approach for architecture, design, and analysis of secure, survivable distributed information systems must be developed. These new principles and approaches should build upon, and be synthesized from, existing and emerging information system engineering principles based on work in fault-tolerant systems, trusted systems, and secure distributed systems. The principles must be promulgated as guidelines so that they will be widely applied.

There is a need to create a broader theoretical underpinning for understanding, design, and analysis of the security and survivability of information systems. Theoretical tools available today usually treat specialized aspects of information security. Early information-theoretic work in the 1950s and 1960, work in the 1980s on trapdoor functions, and recent work on Byzantine robust networks may form some basis for development of a broader theory. New theories should be developed for robust systems. These theories need to include models both for attacks on systems and for survivability defense strategies. Robust system theory should include formal methods that apply to large-scale, distributed, heterogeneous systems. Analysis techniques

should include methods for predicting and analyzing Red/Blue conflicts by, for example, extension/application of game theory and other relevant approaches.

Since the cost of highly secure network subsystems will be very high, the architect should assume that the defense network will traverse commercial infrastructures, and that the underlying substrate will be inherently insecure. The network architecture thus must ensure successful transmissions in the presence of failed, faulty, and spoofed network components. For example, spatial transmission diversity is an existing proof that reliability can improve with intelligent use of the network. Since the future global network will include subnets of varying robustness, it is suggested that a separable entity be established as an overall net security management system. The overall network security manager would be responsible for architectural add-ons (such as wrappers) for each subnet, to provide survivable, secure service over the entire net of nets.

For survivable systems, security is required at multiple levels, including applications, middleware, operating systems, and networks. New architectural approaches must enable the accommodation of legacy and COTS subsystems, perhaps via wrappers, into an overall adaptive system-of-systems architecture. This architecture must be designed to reallocate critical tasks dynamically to subsystems which have survived the attack. The security/survivability management of the system should be integrated into the overall system management framework, in terms of both the automated and the human components of the system management structure.

In order to test the effectiveness of the survivable system architecture, principles, and theory, it is essential to conduct experiments and demonstrations. It is recommended that such experiments and system demonstrations be conducted in existing and emerging system testbeds and networks, building on both experimental nets and the emerging DII and NII.

There are substantial differences between designing a typical information system and designing a resilient information infrastructure capable of enduring in the face of intentional disruptions. Information system design is typically based on efficiency; a resilient information infrastructure design must be based, instead, on effectiveness. Control must be decentralized and portions must operate independently of the infrastructure. For example, fault-tolerant computing introduces redundancy into otherwise efficient systems in order to make them more effective, particularly against random disruptions. Similarly, the design of a resilient infrastructure will ensure diversity of hardware and software so that a common failure mode will not result in an infrastructure failure. Investing in a proper design up front saves money in the long run and negates the very real possibility of introducing vulnerabilities by attempting to retro-fit security.

The goal is to design for utility, resiliency, repairability, and security, as shown in Exhibit 6-2-4. Presently, there is no significant body of knowledge on infrastructure design. It will have to be developed based on the existing design skills for fault-tolerant computing, resiliency, reliability, and so on. This body of knowledge will expand through on the results of the research currently under way and planned for large distributed networks and survivable systems. This growing body of knowledge will be used to develop and promulgate policies, architectures, and standards which enhance the utility, resiliency, repairability and security of the infrastructure. The collection of these policies, architectures, and standards will constitute the infrastructure design.

- ***Functions***
  - Develop and promulgate policies, architectures, standards
  - Design for utility, resiliency, repairability and security
    - No one event/attack should be able to do the system in
    - Perimeter defense not sufficient
    - Classified systems vulnerable to attack from unclassified data sources
    - Back-up repositories of data must be implemented and regularly updated
    - Diversity should be a key aspect of design
  - Develop and implement configuration management process
  - Conduct independent verification of design and procurement specifications

Action **(ASD(C3I) lead):**

- Establish a joint security architecture/design office within DISA to design the infrastructure in accordance with the above principles to shape the design of the DoD information infrastructure
- Establish a process to independently verify and enforce adherence to these design principles

Exhibit 6-2-4. Establish a Joint Office for System, Network and Infrastructure Design

The infrastructure design should be verified independently periodically to ensure that the design meets the goals of utility, resiliency, repairability, and security. The Task Force suggests using NSTAC, NCS, and similar resources to aid in this activity.

The infrastructure design should also be used to verify that goals of utility, resiliency, repairability, and security are reflected in the specifications for development of new systems and for purchase of services from the other government agencies and the private sector.

The Task Force recommends the establishment of a joint architecture/design office in DISA to develop and promulgate throughout the Department the needed design policies, architectures, standards, and configuration management process. This office should include the current architecture and design activities of DISA, but should also be focused on infrastructure design and the incorporation of security up front in the architecture and engineering process. The Task Force also recommends that a process be developed to verify compliance with the design independently.

6.2.5 Establish a Red Team for Independent Assessments

Red Teaming is an essential component of the IW-D strategy and technology development process. We recommend that the concept be extended to include vulnerability analyses as well as carefully planned attacks during experimental activities in controlled testbeds and during training/planning exercises. The Red Team exercises should be conducted under proper rules of engagement to avoid unnecessary damage or disruption to information systems.

Emphasis should be given to developing new attack methodologies in addition to reusing and applying of current attacker techniques. For example, attacks should be designed which exploit the system's survivability features. A sophisticated attacker would probably know about these features. In formulating these attack strategies, models should first be developed for system vulnerability and its likely defenses, and these models should be exploited in the attack strategies. Vulnerability analyses and Red Team attacks should be conducted at the application and system level, as well as at the subsystem level, with the goal of uncovering how operations can be perturbed (e.g., the planning and execution of an air tasking order or the deployment of sensors and communication assets), and how supporting communication links, or specific computers and network nodes, can be compromised.

The need for independent assessments is suggested in the notion that "you can only expect what you inspect." Many activities throughout the Department are in the process of forming Red Teams for the purpose of conducting vulnerability analyses, training, readiness assessments, and so on. The Task Force endorses these efforts, particularly in light of previous DSB Task Force recommendations. However, what the current Task Force is recommending is the "SECDEF/DEPSECDEF's Own"—a team whose central role is providing the SECDEF/DEPSECDEF with unbiased assessments on the Department's IW "state of health."

As shown at the bottom of Exhibit 6-2-5, the Task Force recommends that a Red Team be established to perform these independent assessments. Two previous Defense Science Board Studies have made a similar recommendation to establish such a Red Team. While the Task Force was unable to agree on whether the new organization should be a standalone organization or housed in an existing organization, there was unanimity on the fact that the Team will require significant management attention and, although reporting through the ASD(C3I), be accountable to the DEPSECDEF for its activities.

- ***Functions***
  - **Acquisition – assess vulnerabilities**
    - **Existing and planned DoD systems and networks**
    - **Include products and services provided to DoD by private sector**
  - **Operations – conduct "IW-like" attacks**
    - **Verify readiness posture and preparedness**
    - **Assess physical, cyber, and people aspects**
  - **Spectrum of attacks**
    - **Facilities, networks and systems, and people**
    - **Hardware, software, databases, systems, networks, communications**
    - **Deception, corruption, exploitation, denial**

Action (ASD(C3I) lead):

- **Establish a Red Team**
  - **Accountable to SECDEF/DEPSECDEF, independent of design, acquisition, operations**
  - **Red Team recommended by 1994 and 1995 DSB Summer Studies**
  - **Important management considerations**
    - **Tight leash and significant management attention**
    - **Integrated product team**
- **Develop procedures for employment of the Red Team**

Exhibit 6-2-5. Establish a Red Team for Independent Assessments

Developing and maintaining an independent assessment capability is very important because of the traditional resistance to self-assessment and potential embarrassment. However, it is essential that the Department evaluate its IW preparedness and not wait to learn of any major shortfalls because of the actions of an adversary. This Red Team should have a small permanent cadre for management and technical continuity and should be staffed by civilian personnel and military personnel on a rotating joint duty basis.

The organizational recommendations made by the Task Force are shown graphically in Exhibit 6-2-6. While it was obvious to the Task Force that similar information warfare (defense) capabilities and organizations must be established at the national level, the Task Force decided not to make specific recommendations about where these organizations should be established or to whom they should report. Instead, the Task Force recommends this be left to the President's Commission. However, it should be pointed out that there is a real need for extensive coordination and information sharing between government (Federal, state, and local) and the private sector.

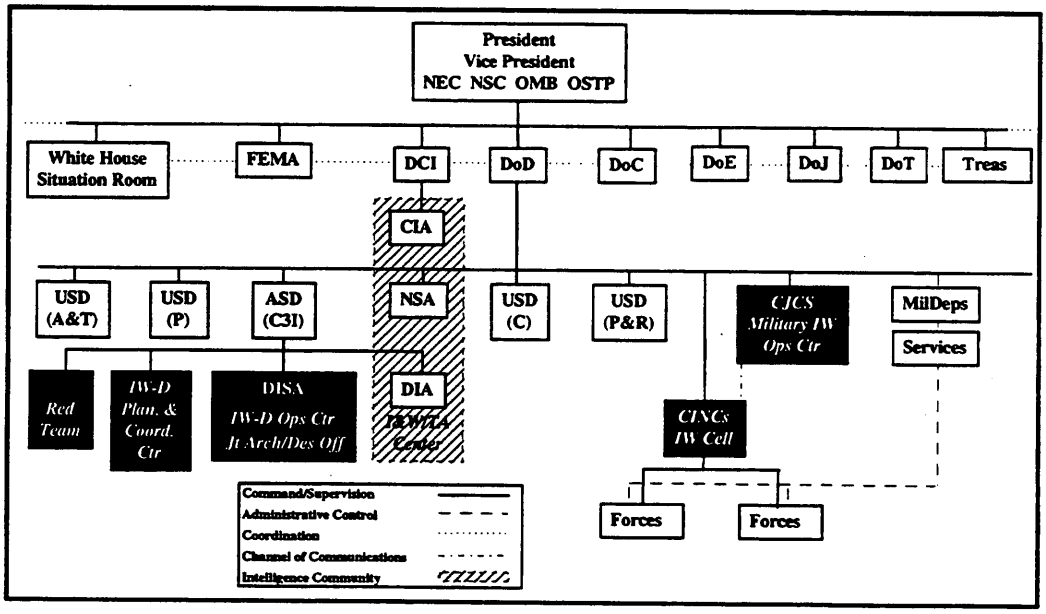


Exhibit 6-2-6. Organizational Recommendation - DoD Aspects

Exhibit 6-2-7 also shows the organizational recommendations made by the Task Force but emphasizes the functional aspects. The defensive information warfare process, procedures and mechanisms diagram discussed earlier in the report is shown in the middle of the Exhibit and the process has been divided by the gray line into preparedness functions and operations functions. The recommended organizations are arrayed in the Exhibit so as to relate their functions (shown near the ovals) to the entire defensive information warfare process.

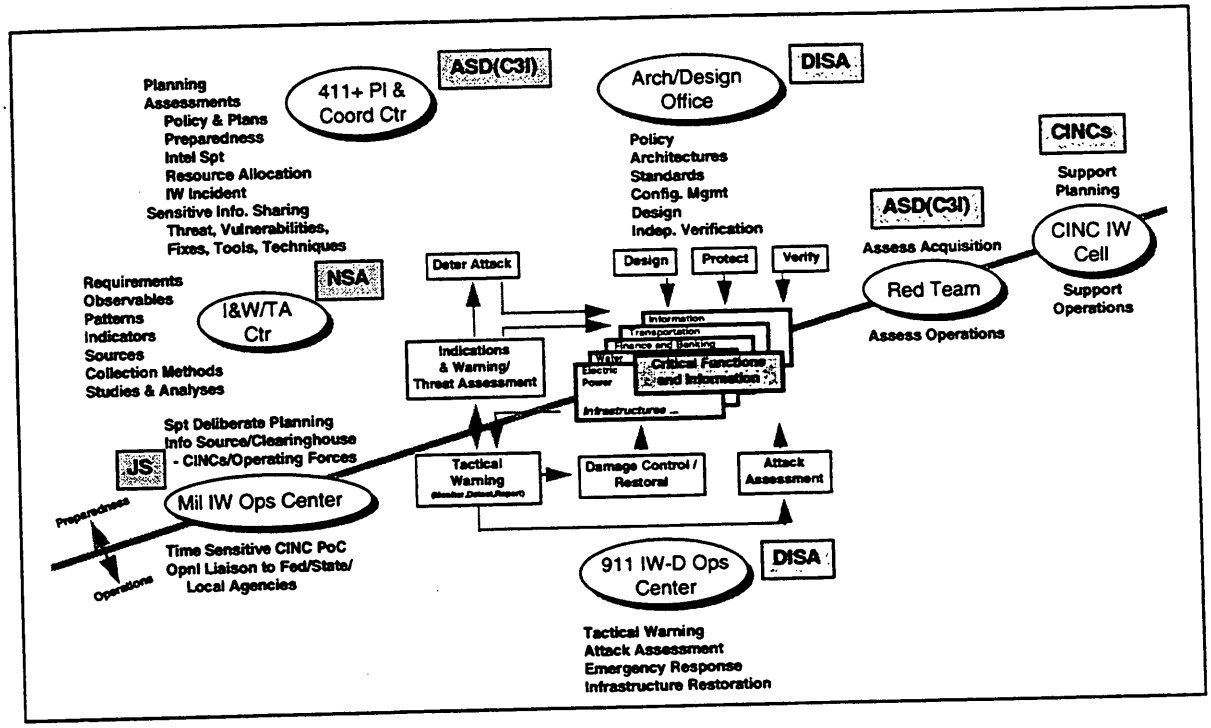


Exhibit 6-2-7. Organizational Recommendations - Functional Aspects

6.3 INCREASE AWARENESS

An important and cost effective first line of information warfare defense is a user and operations community that is aware of potential threats and is well trained in protection, detection, and reaction tactics, techniques and procedures. A well-trained and educated cadre of security and automated information system professionals can provide an effective second line of defense. The Services and Agencies (NSA in particular) have long provided INFOSEC training. Traditional DoD security awareness and training, however, has emphasized the security of classified national security information and information systems processing classified national security information. DoD components are currently implementing awareness, training, and education (ATE) programs to focus on new threats to both unclassified and classified networks. Working groups have been established to help coordinate efforts between components. There is a need, however, for a DoD-level forum with the authority to reduce duplication and implement consolidated training responsibilities. This forum must take advantage of core competencies to ensure a comprehensive, cost-effective program.

Current modeling and simulation efforts do not adequately address issues that can be expected to arise in an information warfare attack environment. For example, little or no consideration is given to the tactical impact of compromised or exploited computing and networking resources, beyond perhaps the classical effects of jamming or ESM techniques as applied to the battlefield communications infrastructure.

A fundamental shortcoming of traditional wargame-oriented simulations is the failure to predict changes in battlefield behavior resulting from the dynamic interplay of people with new weapons, sensors, tactics, etc. This is mainly due to deeply embedded, built-in assumptions of human tactical behavior. The introduction of a new dimension to the battlespace, namely that of IW, serves to aggravate the problem. A new generation of simulations and gaming environments is needed that not only generally minimizes built-in assumptions on human behavior, but also captures in particular the implications and impact of sophisticated information warfare types of attacks.

Because of our perceived lead in offensive information warfare capabilities, not everyone understands the need for defensive information warfare preparations. The Task Force review of several current Service and joint doctrine documents indicates that defensive information warfare matters are not adequately addressed. The Task Force strongly suggests the need to make senior-level government and industry leaders aware of the vulnerabilities and appreciate the implications. The recommended actions are shown in Exhibit 6-3.

The awareness campaign should be designed for several purposes. The internal campaign should make DoD personnel more aware of the threats, vulnerabilities, and fixes and should also make DoD a better informed customer in the acquisition of systems, COTS products, and services. The external program should make DoD suppliers better aware of DoD needs and should make the civil agencies and the general public understand DoD dependence on infrastructures and the role of DoD in the information-age "common defense."

- ***IC/IW (Offense) capability breeds complacency***
- ***Military doctrine does not adequately address IW vulnerabilities***
- ***Need senior-level government and industry appreciation of what's at stake***
  - **Pursue all avenues (briefings, conferences, articles, etc.)**

Action:

- **Establish an internal and external IW-D awareness campaign for the public, industry, CINCs, Services and Agencies (ASD(C3I) and Public Affairs)**
- **Expand the IW Net Assessment recommended by the 1994 Summer Study to include assessing the vulnerabilities of the DII and NII (USD(P) lead)**
- **Review joint doctrine for needed IW-D emphasis (CJCS lead)**
- **Explore possibility of large-scale IW-D demonstrations for the purpose of understanding cascading effects and collecting data for simulations (ASD(C3I) lead)**
- **Develop and implement simulations to demonstrate and play IW-D effects (USD(A&T) lead)**
- **Implement policy to include IW-D realism in exercises (CJCS lead)**
- **Conduct IW-D experiments (CJCS lead)**

Exhibit 6-3. Increase Awareness

The Task Force recommends that the ongoing IW net assessment recommended by the 1994 Summer Study be expanded to include an assessment of the vulnerabilities of the DII and the NII with particular emphasis on those portions of the NII upon which the Department is especially dependent. A brief review by the Task Force of selected joint doctrine revealed a heavy

dependence on information and information technology without corresponding attention to defensive information warfare. Existing doctrine should be reviewed for needed emphasis. The Department should also explore the possibility of large-scale demonstrations for the purpose of exploring cascading effects and for collecting data necessary for simulation of information warfare activities.

In addition and to the extent possible, information warfare (defense) must be realistically played in exercises. This will require some concerted management attention. The Task Force notes that since 1992, DoD policy has called for military exercises to include realistic information warfare play. To date, there has been very limited execution of this policy. In those cases where a realistic IW environment cannot be created, specific experiments should be developed to assess the effects of information warfare attacks. For example, policy directing the CINCs to conduct exercises with information warfare realism has been effect since 1992 and there has been no noticeable efforts to date to implement the policy. In those cases where such realism is not possible, specific experiments must be developed to assess the effects of information warfare attacks.

6.4 ASSESS INFRASTRUCTURE DEPENDENCIES AND VULNERABILITIES

Traditional thinking is that infrastructures, with few exceptions, are stable, reliable, and always available. The nation's interstate highway system is a prime example. Consequently, the Departments' operational and functional planners have not adequately addressed the possibility that key infrastructures such as telecommunications, electric power, and transportation might not be available in part to support military operations. The purpose of this recommendation, as shown in Exhibit 6-4, is to get the operational and functional planners to begin documenting the extent to which their plans are dependent on critical infrastructures and what effect infrastructure disruptions might have on execution of the plans.

- ***Dependencies and vulnerabilities not well understood***
  - **Affects efforts to mobilize, deploy, employ, control and sustain forces**
  - **Interconnected infrastructures have common single points of failure**
  - **Mitigation (protection) techniques and procedures must be developed**
- ***The Mission Needs Statement for Infrastructure Assurance Modeling developed by Joint Staff will help***

Action

- **Develop a process and metrics for assessing infrastructure dependency (ASD(C3I) lead)**
- **Assess/document operations plans infrastructure dependencies (CJCS lead)**
- **Assess/document functional infrastructure dependencies (PSAs lead)**
- **Assess infrastructure vulnerabilities (ASD(C3I) lead)**
- **Develop a list of essential infrastructure protection needs (CJCS lead)**
- **Develop and report to the SECDEF the resource estimates for essential infrastructure protection (ASD(C3I) lead with CJCS support)**
- **Review vulnerabilities of hardware and software embedded in weapons systems (USD(A&T) lead)**

Exhibit 6-4. Assess Infrastructure Dependencies and Vulnerabilities

The Joint Staff has begun to address the issue by developing a draft Mission Needs Statement for Infrastructure Assurance Modeling. The MNS approach is to use modeling and simulation. This is probably the best long-term approach to understanding infrastructure inter-dependencies, potential cascading effects, etc.

The Task Force recommends that a separate effort be initiated by the ASD(C3I) to develop an alternative approach using other analytical techniques that could be employed in the near term by the operational and functional planners to assess all critical infrastructure dependencies. Based on these assessments by the Chairman and the Principal Staff Assistants, the Chairman should develop the essential infrastructure protection needs and the ASD(C3I) should develop the resource estimates for the needed protection.

The Task Force recognizes that this will be an enormous task. However, the complexity and difficulty of the task should not be an impediment to starting the effort; "the journey of a thousand miles begins with a single step."

6.5 DEFINE THREAT CONDITIONS AND RESPONSES

Exhibit 6-5-1 shows that, as in the traditional operations community, the IW-D operations community requires an alerting mechanism to heighten awareness and preparedness as the threat increases. In addition, there should be some prescribed response by the IW-D operations community to increasing threat conditions such as minimizing the traffic on the networks, restricting personnel access to operational facilities, disconnecting certain systems from networks which are likely targets, and possibly implementing wartime modes of operation. While the effort is urgently needed, it will be complicated by the extensive interconnectivity of systems and networks and because some actions will be required by the private sector, in part, since much of the Defense Information Infrastructure is embedded in the public switched and data networks.

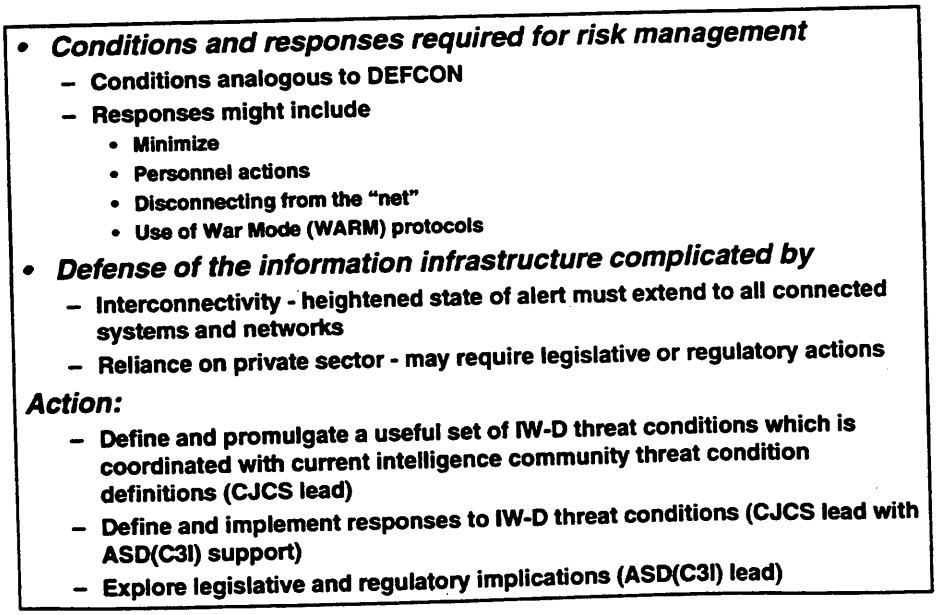


Exhibit 6-5-1. Define Threat Conditions and Responses

Exhibit 6-5-2 is an illustrative cut at what a structured threat condition and response table might look like. This is not a definitive threat chart. For example, "normal" is yet to be defined and very damaging attacks can be postulated that would not cause a noticeable increase in the number of incidents. Also, it should not be inferred that the Task Force believes an information warfare attack will necessarily escalate in a linear manner from level II to level V. An attack could be oriented on a specific critical target or could immediately threaten multiple centers of gravity within the United States. The term "special contexts" is an attempt to highlight the potential linkages between an information warfare attack and other circumstances that may be present. For example, disruption of the infrastructures supporting Fort Bragg, North Carolina, would have much greater impact during a deployment of U.S. forces to a crisis location than it would during normal peace-time training operations.

CONDITION	SITUATION	REQUIRED RESPONSE
I-Normal	- Normal threat-crime/incompetents - Normal activities in all sectors	- Normal actions and requirements
II-Perturbation	- 10% increase in incident reports, regional or functionally based - 15% increase in all incidents	- Increase incident monitoring - Look for patterns across wide range of variables - Alert all agencies to increase awareness activities - Begin selective monitoring of critical elements
III-Heightened Defense Posture	- 20% increase in all incident reports - Condition II with special contexts	- Disconnect all unnecessary connections - Turn on real-time audit for critical systems - Begin mandatory reporting to central control
IV- Serious	- Major regional of functional events that seriously undermine U.S. interests - Condition II/ III with special contexts	- Implement alternate routing - Limit connectivity to minimal states - Begin "aggressive" forensics investigations
V-Brink of War	- Widespread incidents that undermine U.S. ability to function - Condition III/ IV with special contexts	- Disconnect critical elements from public infrastructure - Implement WARM protocols - Declare state of emergency

Exhibit 6-5-2. Sample Threat Condition and Response

Deriving a solid set of threat conditions and appropriate responses will require some serious research. The various levels reflect combinatorial effects as well. For example, it is possible to move from Condition I to Condition V without passing through the intervening conditions. Condition II reflects the notion that an attack may be surgical rather than broad-based.

6.6 ASSESS IW-D READINESS

Information warfare defense should be viewed from a warfighting perspective. Operational forces should be able to detect, differentiate among, warn of, respond to, and recover from disruptions of supporting information services. Recovery from disruptions resulting from failures or attacks might involve repair, reconstitution, or the employment of reserve assets. In some cases, network managers may have to isolate portions of the network, including users of the network, to preclude the spread of disruption. Given the speed with which disruptions can propagate through networks, these capabilities may need to be available in automated form

within the network itself. Finally, there must be some means to manage and control these capabilities. At its heart, this is an operational readiness matter.

A standardized process to enable commanders to assess and report their operational readiness status as it relates to their specific dependency on information and information services is an essential element of operational readiness. A standard vocabulary will enable common description of risk scenarios and assessment methodologies. (A more complete explanation of the proposed process is at Appendix C.) The use of a structured assessment and reporting process will help move information assurance from a global and unsolvable problem to the identification of discrete information and information service dependencies that illuminate quantifiable risk to specific information dependent activities within a commander's sphere of responsibility. A similar assessment and reporting process can be applied by supporting elements and in the commercial sector.

Exhibit 6-6 shows that information warfare (defense) must be mainstreamed as a readiness issue. A means must be developed for including information warfare (defense) issues in readiness reporting and a process must be developed to assess the information warfare (defense) readiness posture independently. The assessment scenarios differ from the threat conditions discussed earlier in that the assessment scenarios are used to assess readiness against a wide range of possible threats to specific units, missions, and functions, while the threat conditions are used to describe the existing threat condition to the broad interconnected population. The assessment scenarios are applied locally, while the threat conditions are applied globally. Standardized assessment scenarios could be used for planning considerations, in warning orders, and so on. The assessment regime provides a means for addressing variability and should be used in concept and operations planning.

- ***Readiness assessment system***
  - **Need explicit process to tie IW-D readiness assessments to the ability to execute operational missions**
  - **Propose standardized, graduated assessment scenarios**
    - **Accident**
    - **Amateur hackers**
    - **Experienced hacker**
    - **Well-funded non-state purchase or hire of advanced IW capabilities**
    - **State-sponsored IW**
    - **State-sponsored IW with the active collusion of an insider**
  - **Propose standardized, graduated assessment regime**
    - **An unknown information assurance capability for a specified threat scenario.**
    - **Engineering estimate based on design parameters and recovery plans**
    - **Engineering estimate based on design, simulation exercises, and review of recovery plans, but no physical testing for a specified threat scenario,**
    - **Internal assessment organization and live contingency plan exercise**
    - **Independent security assessment organization and live contingency plan exercise**

Action:

- **Establish a standardized IW-D assessment system for use by CINCs, MilDeps, Services, and Combat Support Agencies (CJCS lead)**

Exhibit 6-6. Assess IW-D Readiness

- ***Readiness reporting system***
  - **Need a standard IW-D preparedness reporting system using assessment factors from previous exhibit**

Action:

- **Incorporate IW preparedness assessments in Joint Reporting System and Joint Doctrine, for example (CJCS lead):**
  - **SORTS (Status of Resources and Training System), Joint Pub 1-03.3**
    - **Add IW preparedness to overall unit readiness rating (C-Level)**
  - **CSPAR (CINCs Preparedness Assessment Report), Joint Pub 1-03.31**
    - **Add explicit review of IW to review of Ops/Con Plans**
  - **CSAAS (Combat Support Agency Assessment System), Joint Pub 1-03.32.1**
    - **Address IW preparedness in new annual CSAAS cycle**
  - **Joint Tactics, Techniques, and Procedures for Base Defense, Joint Pub 3-10.1**
    - **Include IW, apply to CONUS and OCONUS bases**
  - **Joint Doctrine for Operations Security, Joint Pub 3-54**
    - **Add IW posture to assessment factors**
  - **DISA Communications Spot & Status Reports, Joint Pub 1-03.10**
    - **Modify to include status reporting on major computing resources**
    - **Include CSAs, MilDeps and Service mobilization & sustainment assets**

Exhibit 6-6. Assess IW-D Readiness (Continued)

The Task Force recommends that the Chairman of the Joint Chiefs of Staff incorporate information warfare preparedness assessments in the Joint Reporting System and into Joint Doctrine. The systems, reports and publications cited are only examples that the Task Force reviewed to illustrate how these assessments might be incorporated. Additional details will be provided in the written report.

6.7 "RAISE THE BAR" WITH HIGH-PAYOFF, LOW-COST ITEMS

There are a number of things the Department can undertake, as shown in Exhibit 6-7, that are relatively low cost, but that will raise the bar significantly for potential system and network intruders. Training and awareness have already been emphasized. The two specific examples are cited to illustrate the fact that there is existing Executive Branch policy regarding this matter and that the use of banners to alert users is a good way to increase awareness. Certification by users of banner understanding is another technique to emphasize the importance. One of the Task Force members cited as an example the procedure used in his company. On a periodic basis, users of the network are presented with a security awareness quiz. If the questions are not answered correctly after three tries, the user must have the systems administrator provide access to the system or network.

- ***Training and awareness***
  - Enforce provisions of Appendix 3, OMB Policy A-130
  - Use banners
- ***Improve security of DoD's unclassified computers***
  - Access control (get rid of fixed passwords!)
  - Identification and authentication
  - Much more effective than encryption in "raising the bar"
- ***Promote use of government approved commercial security technologies***
  - Support JWCA Phase 5 plan of action

***Action** (ASD(C3I) lead:*

- Direct the immediate use of approved products for access control
  - As an interim until a MISSI solution is implemented
  - For those users not programmed to receive MISSI products
- Examine feasibility of using approved products for identification and authentication
- Require use of escrowed encryption for critical assets
  - Preclude rogue employee from locking up systems and networks
  - Data bases, program libraries, applications, transaction logs

Exhibit 6-7. "Raise the Bar" With High-Payoff, Low-Cost Items

One of the most important acts is to improve the security of DoD's unclassified computers by instituting dynamic access control and authentication of users. Until this is done, the Department has little assurance that it has any control over these systems, many of which are essential to critical support functions. The Department should also promote the use of existing commercial and government security technologies.

The Task Force recommends the immediate use of commercial access control technologies for this purpose. These technologies can be used as an interim solution for MISSI and as a solution for those users not programmed to receive MISSI. The Department should also explore the feasibility of using approved commercial products for identification and authentication and continue its plans for the use of escrowed encryption, particularly for the protection of critical assets.

6.8 ESTABLISH AND MAINTAIN A MINIMUM ESSENTIAL INFORMATION INFRASTRUCTURE

The current information infrastructure which supports telecommunications, power, transportation, etc., is susceptible to IW attacks, and in particular to wide-scale coordinated attacks aimed at disabling or disrupting government as well as commercial systems. A strategy and overall architecture concept must be developed for a minimum essential information infrastructure (MEII). This minimum infrastructure can serve as a means for restoring services and adapting to wide-scale outages. Milstar should be investigated as a means for determining available connectivity and providing modest but critical packet data service for exchange of routing, node status, and other essential network management information. In this role, Milstar would be supplemented with available commercial resources as possible and as needed.

The concept should consider the applications and deployment of secure gateways connected to Milstar ground station equipment and reallocated Milstar assets as a hardcore network for use in restoring critical connectivity. The authentication of commercial wireline and wireless network access through the gateway to the hardcore network is a critical issue, and must be addressed.

In addition to an overall MEII architectural concept, minimum essential services, an operational concept, and a management structure must be developed. A strategy must be developed for transitioning from peacetime or normal operational activities to the minimum essential information infrastructure. It will be important to execute the transition strategy in the context of exercises.

The minimum essential information infrastructure capability shown in Exhibit 6-8 could serve the Department for critical missions and functions and could serve the nation for other national security-related functions. The 1995 DSB Summer Study titled *Investments for Century Military Superiority* recommended a minimum essential C3 capability. Included are the specific recommendations leading to that capability.

- ***Current NII/DII is vulnerable***
  - **Not designed for resiliency or repair**
  - **Cannot fully depend on public switched network**
- ***Need***
  - **Failsoft infrastructure to support critical functions while under attack**
  - **Failsafe minimum infrastructure**
  - **Failsafe capability to manage restoration independent of the public switched network**
- ***Core capabilities exist***
  - **Milstar**
  - **Government Emergency Telecommunications Service (GETS)**
  - **Telecommunications Service Priority System (TSP)**
  - **National Telecommunications Management Structure (NTMS)**
  - **Etc.**
- ***Critical interaction of fuel, power, and telecommunications***
- ***Base on infrastructure dependency assessments***
- ***Build on 1995 DSB Summer Study recommendation***

Action:

- **Define options with associated costs and schedules (ASD(C3I) lead)**
- **Identify minimum essential conventional force structure and supporting information infrastructure needs (CJCS lead)**
- **Prioritize critical functions and infrastructure dependencies (CJCS lead)**
- **Design a Defense MEII and a failsafe restoration capability (ASD(C3I) lead)**
- **Issue direction to the Defense Components to fence funds for a Defense MEII and failsafe restoration capability (USD(C) lead)**

Exhibit 6-8. Establish and Maintain a Minimum Essential Information Infrastructure

6.9 FOCUS THE R&D

New information security products—from biometric personnel identification devices to advanced firewalls—are being introduced every day into the commercial marketplace. Many of the products are either focused on protecting against network-based intrusions or are attempting to enable some form of electronic commerce. However, these products often do not scale well in large distributed environments, are too expensive, and are too difficult to configure.

The Department of Defense should monitor the progress in commercial information technology and take care not to duplicate or reinvent the progress being driven by market forces. However, the commercial market will not provide the Department the necessary tools and techniques to rapidly and securely assemble and protect a robust, resilient, deployable information system to support a Joint Task Force or coalition operations. The Bosnia C2 Augmentation initiative is an example of the challenge.

As cost-affordable technologies are developed, they should be given early tests in the Joint C4ISR Battle Center Environment.

The Task Force is aware of several of the ongoing information system security initiatives under way in DARPA and has read the descriptions of other IW-D R&D efforts in the Joint Warfighting Science and Technology Plan and in the Defense Technology Objectives of the Joint Warfighting Science and Technology and Defense Technology Area Plan (both of May 1996). However, the Task Force suggests a tighter, more integrated focus on support to U.S. defense activities in the areas outlined in Exhibit 6-9. In addition, Task Force did initially consider a much broader and more comprehensive list of R&D initiatives required for information warfare defense. Because of the potential contribution of commercial security activities to some of the Department's requirements, the Task Force recommends the Department should focus its R&D on those aspects of information protection and assurance not likely to be addressed by the private sector. Several Task Force members stressed that the R&D program must emphasize cost and operational realism. For example, it would be helpful if the primary design criteria included per-seat costs for installation, training, and support.

- ***Current security products are not designed to protect large distributed environments***
- ***Must devote attention to verifying security configuration of a rapidly assembled system for Joint Task Force or coalition environments***
- ***DoD must carefully evaluate emerging commercial technologies and products***
  - ***To include testing in Joint C4ISR environments***
- ***Focused research effort required which involves academia, industry and government; however,***
  - **Few universities currently have related courses or research programs**
  - **There are no established avenues for sharing experience and knowledge in resilient system design**

Action (USD(A&T) lead):

- **Focus the DoD R&D program on the following areas**
  - **Robust survivable system architectures**
    - **No one event/attach should lead to failure of a critical function**
    - **Design should provide for graceful degradation and rapid restoration of critical functions**
  - **Techniques and tools for modeling, monitoring and management of large-scale distributed /networked systems**
  - **Tools and techniques for automated detection and analysis of localized or coordinated large-scale attacks**
  - **Tools for synthesizing and projecting the anticipated performance of survivable distributed systems**
  - **Tools and environments for IW-D oriented operational training**
  - **Testbeds and simulation-based mechanisms for evaluating emerging IW-D technology and tactics**
- **Work with the National Science Foundation to develop**
  - **Research in U.S. computer science and computer engineering programs**
  - **Educational programs for curriculum development at the undergraduate and graduate levels in resilient system design practices**

Exhibit 6-9. Focus the R&D

The development of robust survivable systems resistant to information warfare attack, as well as other types of failure, must involve major advances in technology and will require the efforts of a vigorous research community embracing academia, industry, and government. Prior R&D efforts have focused on areas such as computer and network security, encryption technology, and single node failures. Little attention has been paid to surviving willful malicious attack, or detecting and eliminating corrupt software.

The area of robust survivable systems offers an opportunity for a unifying theme to develop a broad-based research effort covering the full range of 6.1, 6.2, and 6.3 research to overcome the current lack of significant new ideas and problem solutions. Particular emphasis should be given to the following areas:

- Designing a system such that no one event/attack will lead to process failure
- Design methods for work processes and software that enable the monitoring of functional activities, provide for the graceful degradation of functional activities, and ease the rapid restoration of functions.

As indicated in the previous exhibit, specific attention should be paid to verifying the configuration of a rapidly assembled system for use in Joint Task Force or coalition environments. This should include positive identification of system components with passive identification of users, in both the static and mobile environments.

Regarding test beds and simulation-based mechanisms, it will be important to:

- Verify whatever security claims are made for a product
- Understand and model cascading events from an information warfare event
- Understand the impact (and psychology) of multiple carefully timed attacks.

In addition to the above, the R&D community should also consider establishing a focused effort on the theory, science and analysis of high assurance, massively distributed systems to include:

- Developing rigorous mathematical approaches and principles for complex system analysis and synthesis. The DARPA BAA 96-40, Survivability of Large Scale Information Systems, 28 August 1996, provides a good start.
- Developing advanced modeling and analysis techniques extending existing formal method approaches.
- Developing advanced formalized techniques for predicting, testing, and verifying complex system performance.

Finally, the Department should work with (and even possibly provide seed money to) the National Science Foundation to establish research and education programs for resilient system design in the universities and colleges.

6.10 STAFF FOR SUCCESS

IW vulnerability is often due to human error, insufficient training, or lack of knowledge of or failure to follow procedures or adhere to policy. This vulnerability represents a gap which cannot be closed with technology alone. Currently, capabilities of system and network administrators and system managers vary widely. This is partially due to a lack of appropriate training, and partially due to the difficulty in use of existing security products and in obtaining information on how to configure a system securely.

A cadre of high-quality, trained professionals with recognized career paths is an essential ingredient for defending present and future information systems. It is recommended that research be conducted towards the development of techniques, curricula, tools, and technology specifically for security-focused training for system and network administrators. Developing partnerships with universities, colleges, existing DoD professional development programs, and vocational schools for the purpose of curriculum development will be an essential ingredient of this process. It will also be important to capitalize on emerging distributed interactive simulation technology to provide a realistic, dynamic, operations center-like training environment indicative of a real-world IW combat setting.

The Task Force acknowledges that there are a number of studies and initiatives under way in the area of information warfare (defense) training. Included in these is a recent NSTISSC review of training which recommended the development of a database of all available INFOSEC training courses. NSTISSC has also developed training standards for Systems Administrators, Information System Security officers, and Designated Accreditation Authorities. However, efforts throughout the Department do not appear to be well coordinated and there does not appear to be a concerted effort to train systems and network coordinators properly.

As shown in Exhibit 6-10, the Task Force recommends establishment of a skill specialty for military personnel to enable the formation of a cadre of knowledgeable and experienced defensive information warfare specialists. The skill specialty is recommended instead of a career path to ensure that operational experience is reflected in the performance of the information warfare (defense) duties and to preclude the possible formation of a closed community of experts.

- ***Systems/network administrators are the first line of defense***
  - **Need a professional cadre - not "other duties as assigned"**
  - **Keep the defenses in good order**
  - **Serve as the "picket line" to sound the warning**
- ***Need IW-D skills and awareness in all functional areas***

Action:

- **Establish a career path and mandate training and certification of systems and network administrators (USD(P&R) lead)**
- **Establish a skill specialty for IW-D (USD(P&R) lead)**
- **Develop specific IW awareness courses with strong focus on operational preparedness in DoD's professional schools (CJCS lead)**

Exhibit 6-10. Staff for Success

6.11 RESOLVE THE LEGAL ISSUES

Legal issues can be a distraction from moving on with what can be done. As shown in Exhibit 6-11, the Task Force found some confusion among the Department's representatives regarding the scope of their authority to monitor systems and networks for the purpose of assessing the security of the systems and networks. As discussed earlier, the advent of distributed computing has and will continue to blur the boundaries of the systems and networks that DoD uses. Confusion also stems from uncertainty over when or whether a wiretap approval is needed. All DoD system and network administrators should assume that any intrusion is a hostile intrusion and take action to minimize the effects of the intrusion and report the intrusion for purposes of tactical warning and to obtain necessary protective support, including law enforcement.

- ***Issues:***
  - Defending DoD systems
    - DoD has needed authority, but rules must be clarified
  - Defending other government and civil systems
    - Need government-wide guidance (perhaps legislation)
    - Areas to examine include:
      - DoD assistance to the private sector (e.g. Computer Security Act)
      - Attacker of unknown nationality (intelligence versus U.S. persons)
      - Tracking attackers through multiple systems
      - Obtaining/requiring reports from the private sector owners and operators of critical infrastructures

Action (General Counsel lead):

- For DoD systems, promulgate:
  - Guidance and unequivocal authority for DoD users to monitor, record data, and repel intruders in computer systems for self protection
  - Banners that make it clear the DoD's presumption that intruders have hostile intent and warn that DoD will take the appropriate response
  - IW-D rules of engagement for self-protection (including active response) and civil infrastructure support
- Provide to the Presidential Commission on Critical Infrastructure Protection proposed legislation, regulation, or executive orders for defending other systems.

Exhibit 6-11. Resolve the Legal Issues

To lessen the confusion, the SECDEF/DEPSECDEF should direct the General Counsel to explore this matter and issue rules of engagement regarding appropriate defensive actions that may be taken upon detection of intrusions into and attacks against DoD systems and networks. This should include promulgating clear guidance regarding monitoring of systems under DoD control and the use of warning banners on these systems.

The SECDEF/DEPSECDEF should also task the General Counsel to propose legislation, regulation, or executive orders as may be needed to make clear the DoD role in defending non-DoD systems. This should specifically address the need for changes to the Computer Security Act, the capture of information on unidentified intruders (issue of intelligence collection on U.S. persons), the authority to conduct "hot pursuit" of intruders, and the ability to obtain reports from the operators of critical elements of the civil infrastructure.

The findings and recommendations developed by the General Counsel should be provided to the President's Commission to aid in their deliberation of the legislative and policy initiatives required for the protection of the critical infrastructures.

6.12 PARTICIPATE FULLY IN CRITICAL INFRASTRUCTURE PROTECTION

Exhibits 6-12-1 through 6-12-4 indicate the Task Force recommendations regarding what DoD should offer to, advocate to, request from, and suggest to the President's Commission. Exhibit 6-12-1 suggests what capabilities DoD might offer to the Commission and the nation in support of critical infrastructure protection. The Department should think through and propose to the Commission appropriate national defense response and retaliation capabilities in the event of an information warfare attack on the critical civil infrastructures, understanding that Defense is not the sole element in responding to threats to the national security.

Action: Offer DoD capabilities to the President's Commission (USD(P) and ASD(C3I)):

- Improve private-sector defenses
  - Transfer R&D, share standards and purchasing power
  - Loan technical and operational expertise to civil agencies and private sector
- Provide IW&TA to private sector
  - Supplement and back up law enforcement and private sector capabilities
  - Use IW&TA center as test bed for applicable private-sector techniques
- Restore service to critical infrastructures
  - Use Federal Response Plan as a model
  - Explore use of Defense MEII and stand-by contracts
  - Use DoD 911 Ops Center to back up private sector capabilities
  - Plan for effective reaction and restoration
- Response/Retaliation/Deterrence
  - Propose DoD responsibilities

Exhibit 6-12-1. Participate Fully in Critical Infrastructure Protection

Exhibit 6-12-2 suggests what DoD interests should be advocated before the Commission. The information-age war powers for the President are suggested in light of the outdated nature of Section 706 of the Communications Act of 1934. This Act is the basis for Federal intervention in assuring the operation of the telecommunications infrastructure. Critical infrastructure assurance goals can be articulated in a general fashion, but should be eventually based on the infrastructure dependency assessments discussed earlier in the report.

Action: Advocate DoD interests to the President's Commission (USD(P) and ASD(C3I)):

- Continued clarity of responsibilities of the Commander-in-Chief and SECDEF in any policy proposed by the President's Commission
- Information-age war powers for the President (draft necessary legislation)
- Critical infrastructure assurance goals

Exhibit 6-12-2. Participate Fully in Critical Infrastructure Protection (Continued)

In addition, there are many international aspects of information warfare that must be addressed as the U.S. formulates a defensive information warfare strategy that will guide DoD operations. For example:

- What international regimes currently address defensive information warfare, and, if none, what regimes should be created to address defensive information warfare?
- What agreements must be in place to effectively deal with the threat if protect/detect/react capabilities require such activities as countermeasures, tunneling through other nation's infrastructures, active monitoring, etc.?
- What information warfare actions constitute an act of war?

- How should IW-D concerns be addressed by country teams, defense attaches, and other diplomats. What effect does status of forces agreements have on IW-D strategies?
- Will the U.S. share IW-D technology (similar to President Reagan's proposal of shared SDI)?
- Will there be vilification of certain types of IW attacks (i.e., against health systems)?
- What are the critical interdependencies with other nations infrastructures (i.e., European financial systems)?
- Is it possible to coordinate crisis management for information systems of global importance?

Exhibit 6-12-3 shows what DoD needs from the President's Commission.

Action: Request the President's Commission provide DoD (USD(P) and ASD(C3I)):

- **Essential critical infrastructure protection**
- **A national-level IW-D structure to include organization and procedures for:**
  - **IW&TA center, "911" Operations Center, "411" Planning and Coordination Center**
- **Coordinated infrastructure design theory, research, principles, and guidelines**
- **Incentives and indemnity for private sector participation in IW-D**
- **Mechanism to adjudicate the conflicting IW-D equities**
- **Consolidation of continuity of government, emergency, and information warfare - defense planning**
- **Authority for DoD, law enforcement, and intelligence agencies to conduct efficient coordinated monitoring of attacks on the critical civilian information infrastructure (without knowing the nationality or location of attackers) (previously discussed under "Resolve the legal issues")**
- **Procedures for DoD to provide assistance to elements of the critical civilian information infrastructure when these elements are attacked (previously discussed under "Resolve the legal issues")**

Exhibit 6-12-3. Participate Fully in Critical Infrastructure Protection (Continued)

Recognizing the difficulty of defining an appropriate role for the government and the private sector in critical infrastructure protection, the Task Force offers these suggested roles which DoD could provide to the Commission. These suggestions are based on input to and deliberations by the Task Force and individual panels of the Task Force. Exhibit 6-12-4 suggests such roles.

Action: Suggest IW-D roles for government and the private sector to the President's Commission (USD(P) and ASD(C3I)):

- Government
  - Legislate as necessary
  - Regulate through
    - Establishing infrastructure assurance goals
    - Promulgating best practices
    - Certifying the certifiers
      - Preparedness assessments ("due diligence')
  - Motivate with
    - Regulatory relief
    - Tax incentives
    - Indemnification for assurance
- Government (Continued)
  - Facilitate
    - Awareness (Informed self-protection, not government sponsored solutions)
    - Dialogue among stakeholders
    - Sharing of sensitive information
      - Threats, vulnerabilities, fixes, tools, techniques, intrusions
    - The "common defense"
      - Research, advice, training, back-up support, registry of knowledgeable personnel
    - Disaster assistance
  - Make use of government and private sector capabilities
    - DoD and other government emergency response teams
    - Commercial emergency response/disaster recovery/business continuity capability in each affinity group
    - Information protection practices ("fire brigades")
- Private Sector
  - Operate and maintain infrastructures
  - Invest in infrastructures and infrastructure protection
  - Share sensitive information within private sector and with government

Exhibit 6-12-4. Participate Fully in Critical Infrastructure Protection (Continued)

The NSTAC Model for Government-Industry Cooperation

- *Establish necessary programs (e.g., GETS, NTMS, TSPS, CPAS)*
- *Share sensitive information (e.g., NSIEs)*
- *Exchange general information (e.g., R&D exchange)*
- *Review/generate requirements for security stds (e.g., NSSOG, SLG)*
- *Conduct risk assessments (e.g., PSN, Electric Power, Finance, Transportation)*
- *Participate in games and exercises ("The day after..., natural disaster exercises, Global games)*
- *Enhance awareness of vulnerabilities/threats (Outreach activities)*
- *Develop principles/standards for products/services (NIITF ISSB)*
- *Coordinate crises operations (NCC)*

Exhibit 6-12-5. Participate Fully in Critical Infrastructure Protection (Continued)

The NSTAC model shown in Exhibit 6-12-6 could serve as a model for refining the roles of government and industry as suggested here. Sensitive information includes threats, vulnerabilities, intrusions and other incidents, fixes to vulnerabilities, etc.

Exhibit 6-12-6 suggests a model as a starting point for refining the government and private sector roles.

	Personal	Business	Public Infrastructure	Government	National Security
Incompetent	O	O	O	G	G
Hacker	O	O	O	G	G
Disgruntled Employee	O	O	O	G	G
Crook	O	O	O	G	G
Organized Crime	O/G	O/G	O/G	G	G
Political Dissident	O	O	O	G	G
Terrorist Group	O/G	O/G	O/G	G	G
Foreign Espionage	O/G	O/G	O/G	G	G
Tactical Countermeasures	---	O/G	O/G	G	G
Orchestrated Tactical IW	---	O/G	O/G	G	G
Major Strategic Disruption of US	---	---	---	G	G

O = Owner Responsibility
O/G = Owner Responsibility to secure, Government surveillance
G = Government responsibility to surveil and secure

Exhibit 6-12-6. Possible IW Target Protection Responsibilities

This exhibit provides another view of how the government and private-sector roles might be defined. It also provides the Task Force view of how target protection responsibilities might be assigned. The exhibit is not intended to be authoritative, but to provide a construct for discussion of the roles of the government and the private sector.

Some areas are exclusively the responsibility of the owner, while others are exclusively the responsibility of government. It is in the areas of shared responsibility between the owner and the government where much work must be done to define levels of responsibility.

6.13 PROVIDE THE RESOURCES

Resources must be provided if a viable defensive information warfare capability is to be achieved. The need has been recognized in part since an INFOSEC special budget issue has been submitted each of the past 3 years. The Task Force has developed a rough estimate of the resources required to get started. The Department must make a detailed estimate. The resource estimates are for resources in addition to those reflected in the proposed FY 97 budget, so some reprogramming actions will be required for FY 97.

The Task Force recommends that the ASD(C3I) develop a detailed plan of action to implement the recommendations and a detailed estimate of the resource required.

- ***INFOSEC "special budget issue" written past 3 years***
- ***Rough "get started" estimates provided - detailed estimates required***
- ***Requires***
  - **Reprogramming FY97**
  - **Programming FY98 and beyond**

ACTION:

- **Develop a plan and associated budget beginning in FY 97 to obtain needed IW-D capability (ASD(C3I) lead) (duplicated from 1. Designate an accountable IW focal point)**

Exhibit 6-13-1. Provide the Resources

Exhibit 6-13-2 shows the estimated resources to implement the key recommendations. These are the very rough estimated resources to implement the key recommendations. The Task Force reviewed all of the individual recommendations categorized under the key recommendations and estimated to $5 million granularity what the implementation costs might be. The figures are the totals of the individual recommendations for each key recommendation. These resources are in addition to the current Information Systems Security Program and other distributed information security costs which in the aggregate total about $1.6 billion annually. The Department should perform a more detailed cost estimate.

Major Recommendations	FY 97	FY 98	FY 99	FY 00	FY 01	Totals
1. Designate IW focal point/staff	5	5	5	5	5	25
2. Organize for IW-D	150	225	215	185	180	965
a. I&W/TA Center	45	60	60	35	30	230
b. IW-D Operations Center	35	60	60	60	60	275
c. Planning & Coordination Ctr	5	10	10	10	10	45
d. Joint Arch/Design Office	25	45	55	50	50	225
e. Red Team & Ind. Assessments	40	50	50	50	50	240
3. Increase awareness	35	65	85	135	135	455
4. Assess infra. depend's & vuln's	45	45				90
5. Define threat cond's/responses						Existing
6. Assess IW-D readiness	10	5				15
7. "Raise the bar," ... access control	70	90	10	10	10	190
8. Establish and maintain MEII	25	50	100	100	100	375
9. Focus the R&D	60	75	125	160	160	580
10. Staff for success	35	65	55	50	50	255
11. Resolve the legal issues						Existing
12. Participate fully in CIP						Existing
13. Provide the resources						Existing
Totals	435	625	615	665	660	3010

* Dollars in Millions

Exhibit 6-13-2. Get Started Resources

SECTION 7

SUMMARY

In summary, the Department must tie several factors together, as shown in Exhibit 7-1.

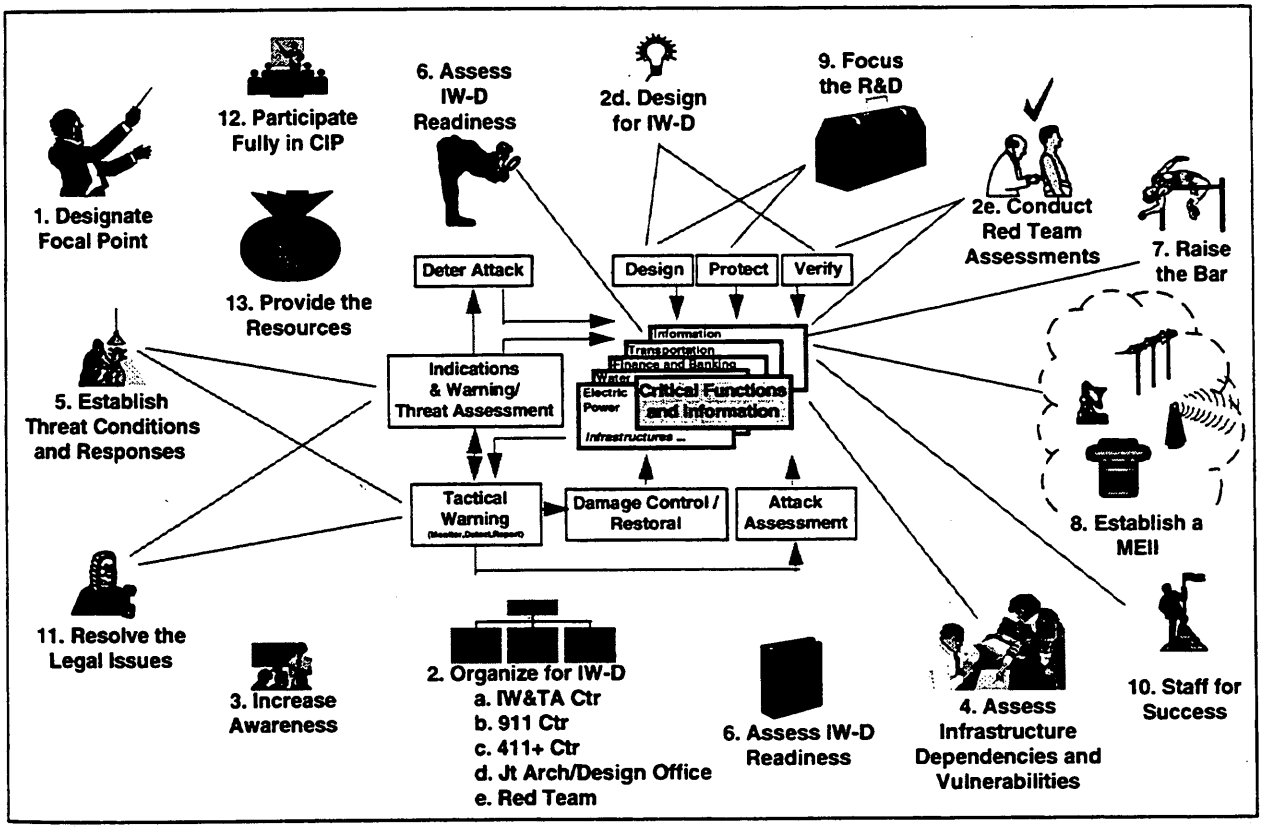


Exhibit 7-1. Tie It Together

And the Department must start immediately, as shown in Exhibit 7-2. Although all the recommendations are important, the check marks indicate where the Task Force believes immediate action will jump-start the process of getting a handle on this challenge. Again, as pointed out earlier, the DSB has called for action on these matters in each of the past 3 years.

- ✓ *1. Designate an accountable IW focal point*
- *2. Organize for IW-D*
- *3. Increase awareness*
- *4. Assess infrastructure dependencies and vulnerabilities*
- *5. Define threat conditions and responses*
- ✓ *6. Assess IW-D readiness*
- ✓ *7. "Raise the bar" (with high-payoff, low-cost items)*
- ✓ *8. Establish a minimum essential information infrastructure*
- *9. Focus the R&D*
- *10. Staff for success*
- *11. Resolve the legal issues*
- *12. Participate fully in critical infrastructure protection*
- ✓ *13. Provide the resources*

Do it now!

(DSB has been saying this for 3 years!)

Exhibit 7-2. And Start Immediately!

APPENDICES

Appendices are provided as background and resource information. ***They <u>do not</u> represent a consensus view of the Task Force and recommendations contained in the Appendices <u>are not</u> Task Force recommendations to the Department.*** Some of the appendices were used in part as input to the main body of this report. Other appendices are provided because they contain useful information for further discussion of matters addressed in the main body of the report.

APPENDIX A

THREAT ASSESSMENT

A.1 THE REALITY OF THE PROBLEM

Advances in the information infrastructure and the growing dependence of the economy and government itself on that infrastructure raise questions about its security. These questions are not new. In 1990 National Academy of Sciences, Computer Science and Telecommunications Board's (CSTB) report, *Computers at Risk: Safe Computing in the Information Age*, began by observing: "We are at risk. Increasingly, America depends on computers. They control power delivery, communications, aviation, and financial services. They are used to store vital information, from medical records to business plans to criminal records. Although we trust them, they are vulnerable—to the effects of poor design and insufficient quality control, to accident, and perhaps most alarmingly, to deliberate attack. The modern thief can steal more with a computer than with a gun. Tomorrow's terrorist may be able to do more damage with a keyboard than with a bomb."

In 1989, another CSTB report, *Growing Vulnerability of the Public Switched Network*, sponsored by the National Communications System, cautioned that: "Virtually every segment of the nation depends on reliable communications.... The committee, after careful study, has concluded that a serious threat to communications infrastructure is developing. Public communications networks are becoming increasingly vulnerable to widespread damage from natural, accidental, capricious, or hostile agents."

Since those reports were written, use of networks and network-related systems has grown in the economy at large and in the government in particular. Within the government, Department of Defense (DoD) dependence on information systems and infrastructure has grown. This growing dependence is giving rise to heightened concern about the vulnerability to electronic threats of the Defense Information Infrastructure (DII) as well as the national and global information infrastructures (NII & GII) to which it is inextricably linked (notwithstanding intentionally separate components). Additional government computer and communications network vulnerability may come from the growing use of commercial off-the-shelf (COTS) systems. For example, COTS constitutes over 90 percent of the information systems procured by DoD. Additionally, government procures over 95 percent of its domestic telecommunications network services from U.S. commercial carriers. These numbers are at levels that underscore the inherent linkage between defense, commercial, and civilian security concerns. Consider the following examples as additional input:

US Dependence on Information Systems

- **Industry increasingly reliant on communications infrastructures**

  -- Internet presence as of May 1994 (Internet info as quoted in the Computer Security Journal, Fall 1995)

  As a sample: Exxon had 261 registered networks; GTE had 228 registered networks; Boeing had 139 registered networks; Motorola had 137 registered networks; Martin Marietta had 62 registered networks; Lockheed had 62 registered networks

  -- "The number of users who have access to the Internet within companies is growing at a rate of 10% every six months." EDP Weekly, by Computer Age, 6 Nov 95, p. 4

- **Governmental Structure of the US dependent on a tenuously secured communications infrastructure**

  -- One switch handles all federal funds transfers and transactions

- **DoD information infrastructure is enmeshed**

  -- with other Governmental structures and industry and private citizens through shared resources of the electrical grid, telecommunications, and the Internet

Trends

- **On line services are a $9.6B industry growing at 100% CGR**
  - Address by Michael A. Braun, President and CEO of Kaleida Labs, Multimedia 94, 30 July 1994
- **US Financial Institutions**
  - transfer more than $1 trillion every day via computer
  - Federal Reserve System handles more than 24,000 wire transfers per day
    - Pitsburg City Paper, Vol 4, No. 34, August 24-30, 1994, pp 8-9
- **Intel Chairman Andy Grove predicts that by the end of this decade, PC sales will surpass 100 million units worldwide - more than sales of cars or TVs.**
  - Egil Juliussen, "Small Computers," IEEE Spectrum, January 1995, p. 44
- **By 1993, 32.7% of US households had a personal computer**
  - Marvin Sirbu, CMU
- **12 million copies of Microsoft Office have been distributed worldwide as of December 1995**
  - Microsoft Corporation Annual Report, 1995

A.2 ASSESSMENT OF THE THREAT

In today's information intensive environment, the information warfare threat can come in many forms. The challenge in evaluating that threat, and the appropriate level of protection or response, has been in sorting out the actual from the perceived, and determining the potential for future developments. In order to adequately assess this threat, the Task Force divided the subject into three categories:

- What is known—the validated threat.
- What is suspected—trends, indications, and the assessment process.

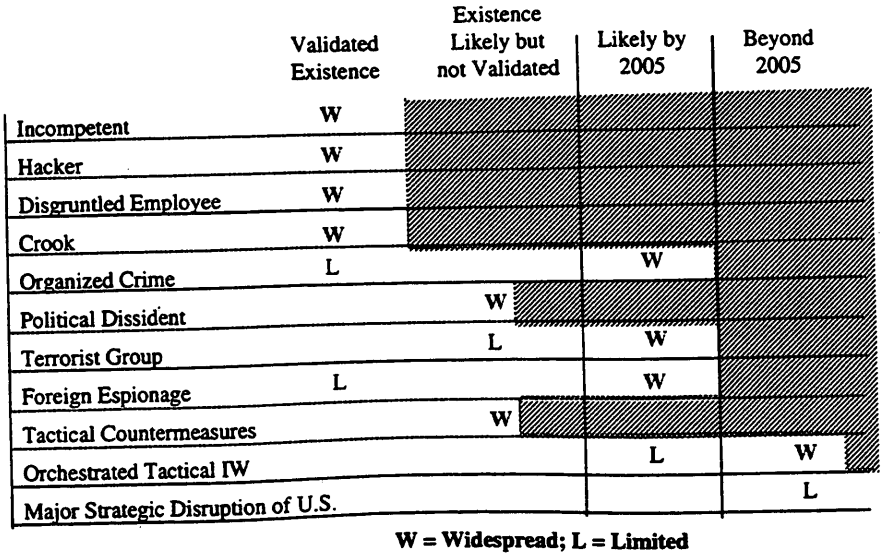
- What is unknown—potential events based on existing capabilities.

These threats to the National and Defense Information Infrastructures vary greatly in terms of intent, sophistication, technical means, and potential impact. The threats can be categorized into the following groups:

- Incompetent, inquisitive or unintentional blunderer; mischief makers and pranksters.
- Hackers driven by technical challenge.
- Disgruntled employee, unhappy customer intent on seeking revenge for some perceived wrong.
- A crook interested in personal financial gain or stealing services.
- Major organized crime operation interested in financial gain or in covering their crimes.
- Individual political dissident attempting to draw attention to a cause.
- Organized terrorist group or nation state trying to influence U.S. policy by isolated attacks.
- Foreign espionage agents seeking to exploit information for economic, political, or military intelligence purposes.
- Tactical countermeasure intended to disrupt specific U.S. military weapon or command system.
- Multi-faceted tactical IW capability applied in a broad orchestrated manner to disrupt a major U.S. military mission.
- Large organized group or major nation-state intent on overthrowing the U.S. by crippling the National Information Infrastructure.

Based on validated incidents, some of these threats clearly exist today. Others are less certain, but can be estimated based on available technology and analysis of continuing trends in development. An estimate of the likelihood for each of these threat categories is shown below.

IW Threat Estimate

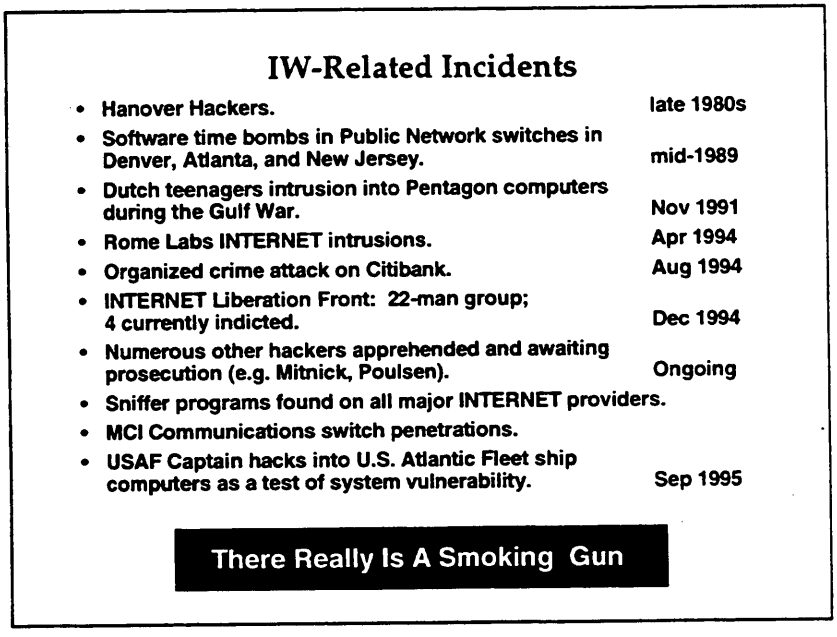


W = Widespread; L = Limited

The information throughout this Appendix was compiled from unclassified sources and briefings received by the DSB from subject matter experts within the Department of Defense, and throughout the civilian sector.

A.3 THE VALIDATED THREAT

IW-related incidents date back to the mid 1980s with the growth of personal computers on a worldwide scale.



The well known case involving the Hanover Hackers is one of the first recorded incidents and is considered to be an example of hacker activity performed for the challenge of gaining entry into someone else's system--without malicious intent.

Although most Public Network (PN) attacks are aimed at accessing other systems, or avoiding toll charges, the software time bomb attacks indicate that denial of service was the objective.[1] (Note: References are at Attachment 1 to this Appendix). In the case involving Dutch teenagers, sensitive information related to U.S. war operations during Desert Storm was modified or copied. Access techniques used in this case included INTERNET and other networks.[2] The Rome Labs incident is another highly publicized case which eventually revealed that over 150 INTERNET intrusions had occurred between 23 March and 16 April 1994. The intrusions were accomplished by a 16-year old British hacker and an unknown accomplice. Several research programs and systems were compromised through the use of Trojan Horses and Network Sniffers. The individual was eventually apprehended by Scotland Yard, and is awaiting prosecution.[3]

In the 1994 attack on Citibank, an international crime group used the electronic transfer system and the international phone network to gain access and transfer approximately $12M to their own accounts. Prosecution of individuals apprehended in Russia and several European countries is

pending at this time.[4] In December 1994, a group known as the INTERNET Liberation Front was charged with stealing phone net data, performing INTERNET attacks for money, and development of highly sophisticated attack tools. Numerous phone, information service, and INTERNET providers were attacked, including some government systems. There was also a substantial international component to their activity based on membership involving at least eight countries.[5] The MCI incident involved an engineer who electronically collected 60,000 calling card numbers and sold them to an international crime ring. To accomplish this task, the individual penetrated several barriers which could have shut down the switch for a prolonged period.[6]

A final example is a case involving a programmed test of electronic systems vulnerabilities. An Air Force hacker remotely entered the command and control system of a ship at sea, through use of a standard computer, INTERNET connection, and the E-mail system onboard the ship. Access included ship navigational control systems which could have effected ship performance or response to guidance commands.[7]

The cases listed here are certainly not an all-inclusive list. They do support an alarming trend toward widespread vulnerability on a case by case basis. The major concern involves what the potential outcome would be if these types of attacks were coordinated to occur simultaneously, or if the tools and techniques used were applied with a more subversive intent.

A.4 THE SUSPECTED THREAT -- AND THE ASSESSMENT PROCESS

In order to more clearly identify the suspected threat, the Task Force considered a variety of sources for analytical support, and paid particular attention to some of the more detailed threat and vulnerability assessments accomplished within the last year.

The Defense Information Systems Agency (DISA) conducted an extensive vulnerability assessment of government network systems in 1994 and 1995. A summary of the DISA focus, and findings is shown below[8]:

IW Assessments - DISA Report

(Developing the Information Warfare Defense: A DISA Perspective, Dec 1995)

Focus:

- **DISA ability to support defensive information warfare (DIW) initiatives.**
- **Assessment of vulnerabilities.**

Findings:

- **DISA is organized to effectively support DIW initiatives, but lacks personnel and funding in many key areas.**
- **It is estimated that DoD is attacked about 250,000 times per year, but only 1 in 500 attacks are detected and reported.**
  - **DISA assessment verified that less than 5% of all attacks are ever detected, and of those, less than 3% are reported.**
  - **Most damaging attacks come from insiders, but hacker tools commonly available on the Internet are capable of intruding on a majority of DoD systems.**

The result of this report was an increased awareness of a growing problem, but the initial actions were primarily focused on security awareness training, and increased training for Local Area Network (LAN) managers. Indications from DISA are that numbers of reported attacks remain at single digit percentage levels, and the problem continues to grow.

At the request of Congress, the General Accounting Office (GAO) conducted an assessment, with the report published in June, 1996. A summary of the GAO focus, findings, and recommendations is shown below[9]:

IW Assessments - GAO Report

(Information Security: Computer Attacks at Department of Defense Pose Increasing Risks, 22 June '96)

Focus:

- Potential for further damage to DoD computer systems.
- Challenges DoD faces in securing sensitive information on its computer systems.

Findings:

- DoD relies on a complex information infrastructure to design weapons, identify and track enemy targets, pay soldiers, mobilize reservists, and manage supplies.
- Use of the Internet to enhance communication and information sharing has increased DoD exposure to attack.
- DoD information is unclassified, but it is sensitive, and should be protected.
- DISA estimates that DoD is attacked about 250,000 times per year, but only 1 in 500 attacks are detected and reported.
- Attackers have stolen, modified, and destroyed data and software, disabled protection systems, and shut down entire systems and networks.
- Security breaches cost DoD hundreds of millions of dollars annually, and pose a risk to national security, yet CERT teams are inadequately staffed, limiting response capability.
- Policy and training regarding computer security and network management are greatly outdated. There is no uniform policy for assessing risks, protecting systems, responding to incidents, or assessing damage.

(Continued on next slide)

Recommendations:

- Develop departmentwide policies for preventing, detecting, and responding to attacks, mandating the following:
  - Report all security incidents within the Department.
  - Perform risk assessments routinely.
  - Correct vulnerabilities and deficiencies expeditiously.
  - Expeditiously assess damage from intrusions to insure integrity of data and systems compromised.
- Require military services and Defense agencies to use training and other mechanisms to increase awareness and accountability.
- Require trained information system security officers at all installations.
- Continue developing and cost-effectively using departmentwide network monitoring and protection technologies.
- Evaluate the incident response capabilities within DISA, the military services, and the Defense agencies to ensure that they are sufficient to handle the projected threat.
- The Secretary should assign clear responsibility and accountability within OSD, the military services, and Defense agencies for ensuring the successful implementation of this computer security program.

Results of this report have been forwarded to the Senate Armed Services Committee and House Committee on National Security; the Senate Committee on Appropriations, Subcommittee on Defense, and the House Committee on Appropriations, Subcommittee on National Security; the Senate Select Committee on Intelligence and the Permanent Select Committee on Intelligence;

the Secretary of Defense; the secretaries of the military services; and the Director, Defense Information Systems Agency.

The report concludes that there are significant risks based on these findings:

- Defense cannot locate or deliver supplies promptly without properly functioning inventory and logistics systems.
- Defense relies heavily on computer technology— especially a network of simulators that emulate complex battle situations—to train staff.
- It is impossible to pay, assign, move, or track people without globally networked information systems.
- Defense cannot control costs, pay vendors, let or track contracts, allocate or release funds, or report on activities without automation.
- Defense systems handle billions of dollars in financial transactions for pay, contract reimbursement, and economic commerce.

According to the FBI and Defense Investigative Service (DIS), high technology and defense-related industries remain the primary targets of foreign economic intelligence collection operations. This finding continues a trend reported in the *1995 Annual Report*. The most likely industry targets of economic espionage and other collection activities during the past year include the following areas, most of which are included on the 1996 Military Critical Technology List (MCTL):[10]

- Advanced materials and coatings
- Advanced transportation and engine technology
- Aeronautics systems
- Aerospace
- Armaments and energetic materials
- Biotechnology
- Chemical and biological systems
- Computer software and hardware
- Defense and armaments technology
- Directed and kinetic energy systems
- Electronics
- Energy research
- Guidance, navigation, and vehicle control
- Information systems
- Information warfare
- Manufacturing processes
- Marine systems
- Materials
- Nuclear systems
- Semiconductors
- Sensors and lasers

- Signature control
- Space systems
- Telecommunications
- Weapons effects and countermeasures.

According to a DIS summary of suspicious contacts reported in FY95, entities associated with 26 foreign countries displayed an interest in 16 of 18 technology categories listed in the new MCTL. The U.S. considers all of the above industries to be strategically important because they produce classified products for the government, produce dual-use technology used in both the public and private sectors, or are responsible for the leading-edge technologies required to maintain U.S. economic security.[10]

FBI Director Freeh provided the following five examples of foreign targeting activities in his 28 February 1996 statement before the Senate Judiciary and Intelligence Committees:

- One foreign government controlled corporation targeted U.S. proprietary business documents and information from U.S. telecommunications competitors.
- Another foreign competitor acquired the technical specifications from a U.S. automotive manufacturer.
- In violation of U.S. export laws, a foreign company attempted to acquire a U.S. company's restricted radar technology.
- Several U.S. companies reported the targeting and acquisition of proprietary biotechnology information.
- One U.S. company reported the foreign theft of its manufacturing technology regarding its microprocessors.

Types of U.S. government economic information—pre-publication or unpublished "insider" data—of special interest to governments and intelligence services include:[10]

- Bid proposals
- Economic, trade, and financial agreements
- Energy policies
- Marketing plans
- Price structuring
- Proposed legislation affecting the profitability of foreign firms operating in the U.S.
- Tax and other monetary policies
- Technology transfer and munitions control regulations
- Trade developments.

Three additional case studies were reviewed by the Task Force involving a southeast U.S. port city, a rail traffic control center, and a 1996 Federal Aviation Administration (FAA) vulnerability assessment. A summary of the findings:

- **Port City Assessment:**
  - **Identified single point of failure for instrastructures supporting military mobilization and deployment**
- **Rail Traffic Control Center Assessment:**
  - **Central control switching facility for east coast rail traffic.**
  - **Potential contributor to problems resulting in fatal Maryland rail collision of AMTRAC and MARC trains in fall of 1995.**
- **FAA Assessment:**
  - **Not vulnerable today due to antiquated systems, limited networking, and proprietary software.**
  - **Upgrades will lead to vulnerabilities due to widespread use of COTS technologies and increased networking.**

Details of the assessment which could impact deployment of units and follow-on forces which rely on transport out of the port terminal region are provided in Reference 13. Investigation of the AMTRAK - MARC collision indicated human error, but vulnerabilities were detected in the control center, making it a potential single point of failure for exploitation. The FAA assessment, provided in briefing form to the Task Force in June, 1996, concluded that even though vulnerabilities were likely to grow, financial realities restricted the ability to plan protective measures into proposed upgrades—until mandated, or in worst case, following a major incident.[11]

A.5 ARE WE AWAITING AN ELECTRONIC PEARL HARBOR?

The trends seen in development of intrusive tools on the INTERNET, growth in hacker activity, and related incidents cause further concern. A summary of recent trends is given below:

IW Trends

- **Open availability of intrusion tools.**
  - **SATAN made available to the public, April 1995.**
  - **Rootkit: Recently available, used to mask intrusions.**
- **Continued growth of hacker activity:**
  - **Masters of Deception: Programmed attacks on phone companies.**
  - **Legion of Doom: Phone switching/billing, and credit card abuses.**
  - **Poulsen/Mitnick/Shadowhawk: Phone, system access, computer code abuses.**
  - **5 hacker group break-in of computers at University of Washington, Bank of America, ITT, and Martin Marietta, (1993).**
  - **Operation Moon Angel: Federal agents arrest 74 hackers nationwide for unauthorized entry into business and government computers (April 1995).**
- **Continued growth in reported computer crimes:**
  - **Academy of Criminal Justice Sciences Study indicates that 98.5% of participating businesses had been victims of computer theft or attempted theft.**
- **Cell phone cloning**
- **Terrorist acts: World Trade Center Bombing.**

Tools: The NSTAC Assessment of Risk to Security of Public Networks reported in February, 1996 that SATAN, the Security Administrator Tool for Analyzing Networks, scans and reports system vulnerabilities, which if improperly used, could enable system attacks. It was made

openly available on the INTERNET in April, 1995. The report also identifies Rootkit as a tool which falsifies data, making detection of intrusion difficult even with state-of-the-art technology. Rootkit is also openly available on the Internet

Hacker growth: Additional case study information is provided at Attachment 1 for first three listings. In the case of the 5-hacker group, one raid wiped out data on the Learning Link, a NYC public television station computer serving hundreds of schools.[2] The Moon Angel offenses included breaking into NASA computers controlling the Hubble telescope, and rerouting calls from the White House.[2]

In October, 1995 New York officials made arrests in what was declared the largest cell phone cloning operation in the country. Estimates are that over 27,000 phones were cloned within a seven month period at an estimated loss of $1.5M per day in cell phone revenue nationwide.[2]

Finally, consider the World Trade Center bombing as a case which might be a good example of physical versus virtual attack: Twin tower, 110 story building; 50,000 workers and 80,000 visitors daily vs. Global marketplace nerve center, many City/State/Federal offices, several international office, $3M phone switch station, telecom for Wall Street to the World.[12]

These trends are cause for a growing concern—the unknown threat, and the potential for an attack having strategic significance.

A.6 THE UNKNOWN THREAT - POTENTIAL EVENTS BASED ON EXISTING CAPABILITIES (THE DEVELOPMENT OF A STRATEGIC THREAT)

Existing, easily acquired capabilities make the potential for an attack having strategic significance a reality. The most common capabilities for IW-related attacks are, by themselves, often seen as more of a localized nuisance, rather than a strategic threat. When applied in a coordinated attach however, the results are far more widespread. Consider the Nth order effects in the following example from Col Charles Dunlap's essay, "How We Lost the High-Tech War of 2007", published in *The Weekly Standard*, January 29, 1996:

The Setting: (The year 2007):

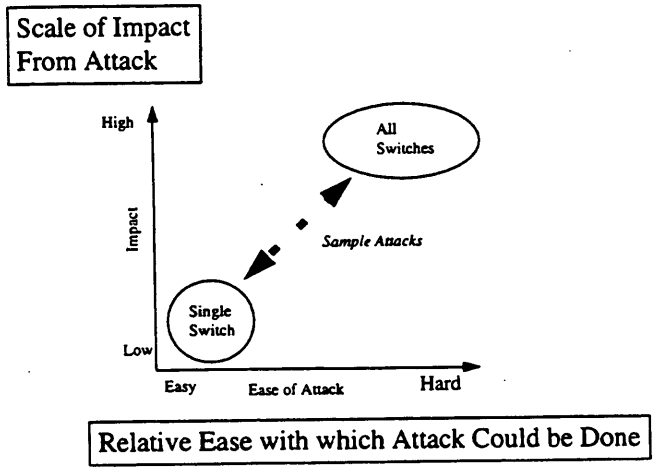
- Downsizing and cuts in military infrastructure are "off-set" by information technology.
- COTS technology used widely by U.S. and her adversaries.
- Open architecture provides information equality - not information dominance. U.S. insistence on open architecture leaves sources of information readily available to opponents - News media is a particularly valuable source.
- Warfare has become even more savage - not cleaner, more high-tech. Televised atrocities and deaths of U.S. troops become a tool of adversaries to sway public opinion.

The Indirect Attack - U.S. C2-Protect efforts are successful in countering direct attack - leading adversary to indirect attack with many Nth order effects:

- Mexican economy attacked - computers corrupted on a massive scale
- Counterfeit electronic pesos flood Mexican bank accounts
- Hyperinflation; economy collapses
- Refugees flood into U.S.
- Call for troops to be brought home to face domestic situation.

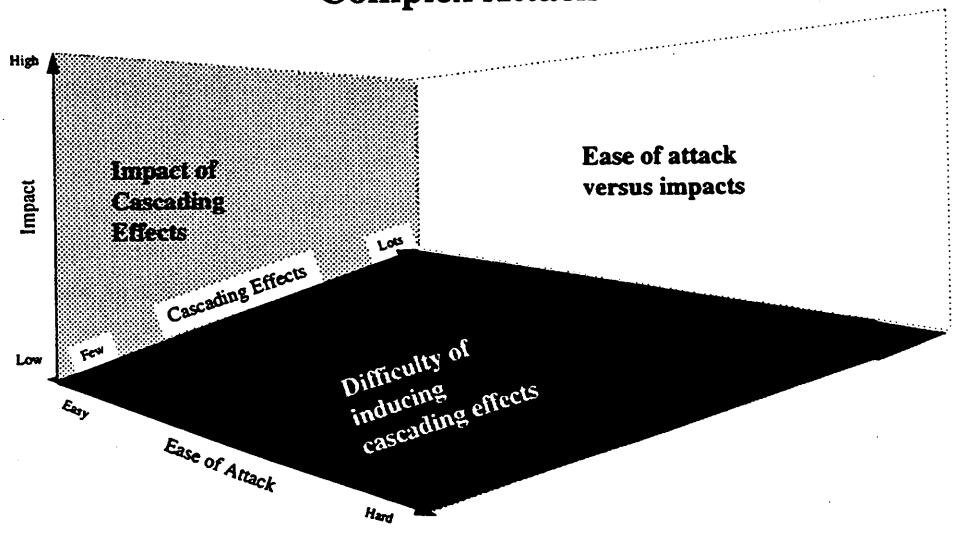
The technologies required to perform this these types of attack are available today. The issue of whether or nor they comprise a strategic threat is more a matter coordinated timing. Some may come in the form of a simple attack on a target identified as a single point of failure:

Simple Attack



A more complex, coordinated attack takes on a multi-dimensional nature:

Complex Attack



In either of these cases, the timing of the attack is what in fact may have made it strategic in nature. Consider the port city example:[13]

- A power outage, communications failure, or road/rail disruption would be an inconvenience to citizens on an average day.
- However, these same incidents coordinated to occur at the peak of Desert Storm deployment could easily have constituted a strategic threat which would have altered arrival of troops and equipment which played a critical part in the outcome of the war.
- Combine these with the previous examples of attacks on Pentagon computers, Rome Lab, Citibank, and the MCI switch, and the result is widespread loss of confidence in the government's ability to respond to problems both at home and abroad.

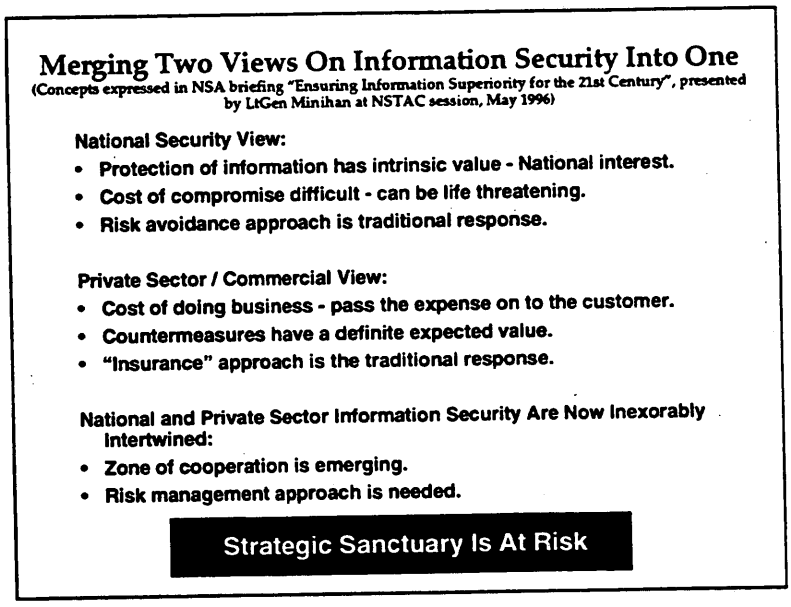
To demonstrate the relative ease of achieving an IW capability, the Threat Panel prepared the following table:

Country \ Enabling Technologies	C2W															
	OPSEC	PSYOPS	EW	Deception	Destruction Lethal	Destruction Non-Lethal	Encryption	S/W Eng	Network Eng	Computer Security	Info Security	Comms Technologies	HPMW	Physical Security	Intelligence	
Russia	↗ D	= D	↘ D	↗ D	↘ D	= D	= D	↘ A	↘ A	↘ D	= D	↘ D	↘ D	↗ D	↗ D	Legends
China	↗ D	= D	= A	= D	↘ D	↘ D	= D	↘ A	↘ A	↘ A	= D	↘ D	= D	↗ D	= D	↗ significant, equal to our best effort
North Korea	↘ D	↘ D	↘ A	= D	↘ D	↘ A	↘ D	↘ A	↘ A	↘ A	= D	↘ A	↘ A	↗ D	= A	= average or good capabilities
Iraq	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↗ D	= A	↘ minor or nascent capabilities
Iran	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	= D	= A	D Developer - making and/or exporting
India	= D	↘ A	↘ A	↘ A	↘ D	↘ A	↘ D	↗ D	↗ D	↘ D	↘ A	= D	↘ A	= D	= A	A Acquiring from external sources
Egypt	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	= D	= A	
Cuba	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	= D	= D	
Libya	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	= D	= A	
Syria	↘ D	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	↘ A	= D	= A	

As an example of a country heavily involved with developing their own capability, consider Russia. Of the 15 categories listed, Russia has a significant capability in seven categories, and a good capability in four (total: 11 of 15). These developments continue, even in the face of widespread economic difficulties. More importantly, almost any nation is capable of developing significant Information Warfare capabilities. Unlike nuclear capabilities, however, IW is relatively inexpensive, and quick to obtain, given the volume of available markets. Thus, a country such as Iran could acquire a strategic capability to threaten the United States without requiring a significant investment, or a long-term development cycle.

A.7 THREAT CONCLUSION

In order to best understand the significance of a potential IW threat, we must consider the often opposing views of information security between the private/commercial sector, and the national security view:



The private sector has viewed IW as a cost of doing business that was often passed on to the customer. The national focus still struggles with the concept of what constitutes a strategic threat. The response has been to avoid risk rather than manage and anticipate it. A zone of cooperation is now emerging which must be better defined:

- Where do protection, detection, and response responsibilities lie?
- Risk management rather than risk avoidance is a critical step.

These issues are at the heart of the defensive information warfare issues.

ATTACHMENT 1

REFERENCES

1. NSTAC *Assessment of Risk to Security of Public Networks,* Feb 1996.
2. *Trends and Experiences in Computer-Related Crime,* Academy of Criminal Justice Sciences, 1996.
3. Rome Lab Attacks Final Report, 20 Jan 1995.
4. Senate hearing on Security in Cyberspace, 5 June 1996.
5. *Trends and Experiences in Computer-Related Crime,* Academy of Criminal Justice Sciences, 1996.
6. 1995 DSB Report.
7. *Hacker Exposes U.S. Vulnerability,* Defense News, Oct 9-15, 1995.
8. DIS Briefing, "Developing the Information Warfare Defense: A DISA Perspective," given by Mr. Bob Ayers, March 1996.
9. GAO Report, *Information Security: Computer Attacks at Department of Defense Pose Increasing Risks,* 22 June 1996.
10. *1996 CSI/FBI Computer Crime and Security Survey,* as reported in Computer Security Issues and Trends, Volume II, Number 2, Spring 1996.
11. FAA Briefing, "Security of the Air Traffic Control System," given by FAA representatives, Mr. Dennis Hupp and Ms. Trish Hammer, June 1996.
12. NSA Briefing, "Ensuring Information Superiority for the 21st Century," given by LtGen Minihan, May 1996.
13. Joint Program Office (JPO) Briefing, "Infrastructure Assurance Supporting Military Operations," given by the Joint Program Office for Special Technology Countermeasures, Ms. Susan Hudson and Mr. Bob Podlesney, July 1996.

APPENDIX B

NATIONAL INTELLIGENCE EXPLOITATION ARCHITECTURE

The Task Force was briefed by a wide variety of officials and members of the Defense and Intelligence Communities. Several consistent themes became apparent. The "Changed World" in which we live, the changes in threats to the United States, the impact of the "Peace Dividend," and our concomitant expanded "global vision" all drive us to realize that information, per se, has become a precious commodity to the U.S. Further, our existing intelligence structure, collection, analytic and information integration capabilities are optimized for yesteryear. Even though we clearly need specific intelligence collection in a number of areas, such as from networked systems such as the INTERNET and other open sources, it became readily apparent that we do not effectively exploit all of the data that we already collect! The decrements, often horizontal, in analytic resources increase the need for effective integration of the analysis processes across the Intelligence Community (IC). Neither our current structure nor our information processing systems are optimized for the new world set of problems.

Issues relating to Intelligence Community resources, IC support to the military acquisition processes, strengthened IC Issue Managers, review of intelligence collection investment strategies, and developing areas of IC business excellence, all point to a critical need for improved intelligence information integration. We simply will not return to the larger number of analytic resources of the cold war; thus a new paradigm is urgently needed. A "New Vision" is proposed.

The Director of Central Intelligence, in concert with the Secretary of Defense, should create "A New Vision" for intelligence exploitation in the U.S. This "New Vision" would lead to the mission of an integrated National Intelligence Exploitation Architecture which, over time, would develop the meta core system (integrated system of systems) for the National Intelligence Community.

Why do we need this New Vision? Because our existing exploitation and analytic systems were created and built during a period in which virtually all such systems were custom designed and implemented; and thus "stove piped" for specific tasks without particular regard for interfaces and compatibility with other systems. These existing systems were built for what became relatively well understood problem sets with characteristics such as:

- known geography and political boundaries
- known jargon and syntax
- known major nations, entities, forces, units, etc.
- known doctrine and tactics
- known, or at least slowly evolving, military capabilities
- known goals and objectives
- known cultures and ethics

- parametric and other signature characteristics known to and largely exploitable by our collection systems
- well-defined and established data bases, data dictionaries and processing techniques to exploit and analyze observables.

In relative terms, this was a fairly static target set for many years.

Our world has changed to the extent that we now do not know who all of our potential adversaries are, or might be. Who would have predicted two years ago that Rwanda, Somalia and Haiti would demand so much from our intelligence communities. Our requirements now are for globally based intelligence, dynamic in nature and rich in detail, which include increased exploitation of open sources and networks in a totally new information age. The INTERNET provides potential for access to rich repositories of open source information. However, IC access to the INTERNET raises difficult questions and serious concerns about conflicts between law enforcement, intelligence activities and constitutional guarantees. These issues will have to be addressed as part of the NIEA.

Given this shift, we should not be surprised that our existing exploitation and analyses systems do not provide the level of capability required in the new world in which we live.

It is estimated that the National Intelligence Community invests between one and two billion dollars a year in new information management technology (not signal processing, although substantial sums are invested there as well). Additionally, DARPA has over $300 million in its budget for advanced computational technologies alone.

If we focused one-quarter of these moneys towards a coherent, integrated and distributed exploitation and analysis system(s), the U.S. could invest the necessary resources to realize this architecture over the next decade. Why would we wish to do so?

First, our dramatically changed world has been exacerbated by our "Peace Dividend" in the sense that we have taken substantial billet reductions in analytic resources. Thus, we can no longer afford the redundancies of the past and at the same time, we must be able to adapt our exploitation and analysis by sharing (or in many cases shifting) the analytic processes in real-time.

Second, hardware and software technology permit us now to design and implement relatively open systems that have a high degree of interoperability and can use a great deal of COTS. We no longer require the vast majority of our systems to be custom and monolithic! We can have systems that can be modified quickly to address changing requirements and to take maximum advantage of rapidly developing technologies.

Third, the NFIP is going to spend (has budgeted) a larger amount on information technology per year, but in a largely diffused manner. Today, there is neither a coherent architecture, nor focused activity to distribute our development activities in such a way to bring together the best IT resources of the entire Intelligence Community into a highly distributed and interoperable

meta system. Surely there are some excellent IT development activities occurring in the IC. These should continue, but in the broader framework of where we need to be in the 21st century. If the past ten years are an example and absent a coordinated development activity as proposed here, we will spend billions of dollars on information technology in the NFIP alone without achieving the kind of integrated capabilities we must have for the 21st century.

How would this work? The "New Vision" would drive the creation of an architecture, supported by enforced building codes (standards, interfaces, security protocols, etc.) in which development activities would be parsed to specific agencies of the IC and supported by the experience of, for example, DoD's experience in promoting interoperability in the JROC process and the development of the GCCS. Over time, each agency would become a center of excellence for a particular area of technology. All of this would fit within the framework of the architecture to permit modules of capability to be developed by one agency for the benefit of any or all other agencies. Let's take but a few examples:

- Text processing is crucial to us all. CIA and NSA arguably have the preponderant IC capability and interest. Each of them should be charged with developing several tiers of text processing capabilities which would build first the foundation and thence the 21st century capabilities we need to exploit open source and covertly collected information. CIA, for instance, might be asked to concentrate on data vaults (archiving large amounts of unformatted data), context based retrieval and query by example. NSA might be asked to concentrate on automated exploitation of facsimile, automated translation and understanding of foreign languages and natural language interfaces.

- Image processing in all of its forms will explode in importance to the IC. While we have no processes today to automatically index, search, retrieve or exploit video, such capabilities will be crucial to our ability to deal with intelligence requirements of the 21st century. Thus the new National Imagery and Mapping Agency would be charged with developing the technology, tools and techniques to exploit video; and to handle the huge volume of SAR & EO/IR imagery from both airborne and spaceborne sensors. This is needed even though we do not have today robust collectors of video. But we will, and we must lay the groundwork today for that future.

- DARPA might logically be asked to develop the tools needed for 21st century automated integration of systems and a number of other technologies which potentially span and integrate with other IT developments. Examples of these include decision aids, correlation and fusion aids and visualization tools that work across disparate sources of intelligence and support a collaborative community of effort.

In each of these cases, there would be strong emphasis on exploiting and integrating technology from the private sector as well. For example, Time-Warner and Salomon Brothers are but two firms investing hundreds of millions of dollars in advanced information technology. We need to assess where the private sector will be providing the research and development so as to leverage those developments and conserve our scarce resources for R&D specific to IC/DoD needs and for integration of commercial technologies.

Over time, the IC could develop a series of interoperable systems which would be less expensive and more powerful by several orders of magnitude for the 21st century, than if we proceed during the next decade in the same mode as the last decade.

The Intelligence Community will have to change in response to the NIEA. Carrying out the initiative may require a more highly centralized focus on information systems that are both within individual organizations and across the IC as a whole. Long-debated plans for Central Information Services Offices may have to be implemented to create the budgetary resources and organizational authority needed to guide an internal information revolution. A Central Information Council may be needed at the SECDEF/DCI level (perhaps to include other government agencies) to establish policy and to guide the IC to focus on common interests. Whatever organizational reforms are taken to ensure the success of the initiative, change will be needed to break down resistance to change, shift established patterns of investment, and enforce a high degree of cooperation and interoperability.

- Investments in information systems must be shifted from operations and maintenance of existing, slowly-evolving systems to the development of more powerful and adaptable systems that are the focus of the initiative.

- Higher levels of cooperation and coordination between the collection, exploitation and analytical communities are needed to support the dynamic, uninhibited research environment envisioned in the initiative.

- An unconstrained research environment will break down the isolation of analysts from each other and the policymakers and encourage the integration of military, economic, ethnic, political and technological factors in analysis. Analysis standards must be established and enforced throughout the IC to avoid "tabloid" intelligence reporting and to ensure the presentation of sound, but divergent views.

The most difficult part is to make the decision. To commit to a road map of information technology which will become the exploitation and analysis meta system (or system of systems) of the 21st century. The target environment is an integrated, yet highly distributed, heterogeneous IT infrastructure which—over time—will permit an individual in the Intelligence or Defense Communities to query this information environment (much as can be done today on INTERNET). The responses would be relevance ranked and presented in a contextual framework pertinent to that particular user. Thus, military commanders/CINCs, acquisition managers, intelligence analysts and a myriad of other users could gain access to the most comprehensive and broadly based information and intelligence available. Sure security is both an issue and a potential problem. Keep in mind that we are talking about the system for the 21st century and many of the security issues of today will be resolved either procedurally (a la the Joint Security Commission Report) or technically through protective hardware and software. Figure 1 illustrates the concept whereby an individual seeking information "goes fishing in the sea of data." The system would understand some of the context from which the query was made, and as the user asked additional and clarifying questions, the system builds more and more

relationships pertinent to the user's needs. Additionally, the system is capable of making queries by example. Thus, the user could ask, "tell me if you know of any more of those." Alerting tools would be embedded in this as well. Both AT&T and American Express have profiles of millions of users which, when violated or exceeded, alert the service provider of anomalies in spending, geography or activity norms. Some of these norms are dynamically adjusted automatically as people use their phone or credit cards.

What the User Needs

An easy capability to extract information related to his problem from the mass of data (national and otherwise) available on distributed problem solving networks

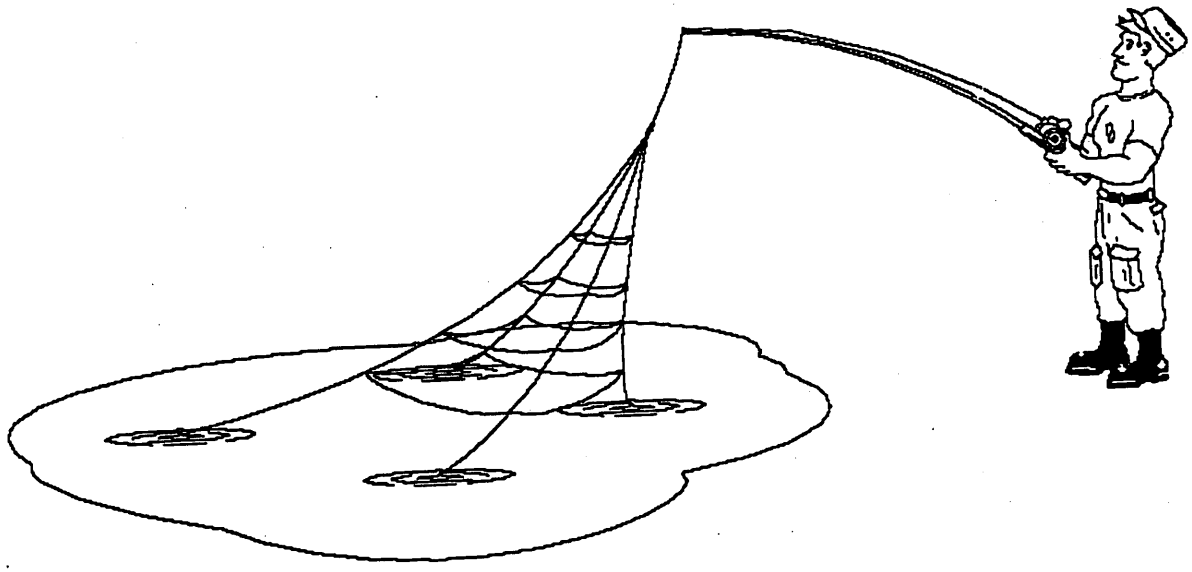


Figure 1.

Figure 2 illustrates the distributed nature of the component systems. They could be spread across Washington, the country, or the world. The key is that, like the INTERNET, the user does not have to know where information is stored in order to retrieve it! His query will seek data through the network of servers/routers/switches that dynamically interface the systems. Although today's INTELINK is a significant improvement over a couple of years ago in accessing intelligence from remote, distributed agencies and commands, it relies on pre-identified and indexed intelligence. What we need for the future is a system that aids the user in finding "unknown" information.

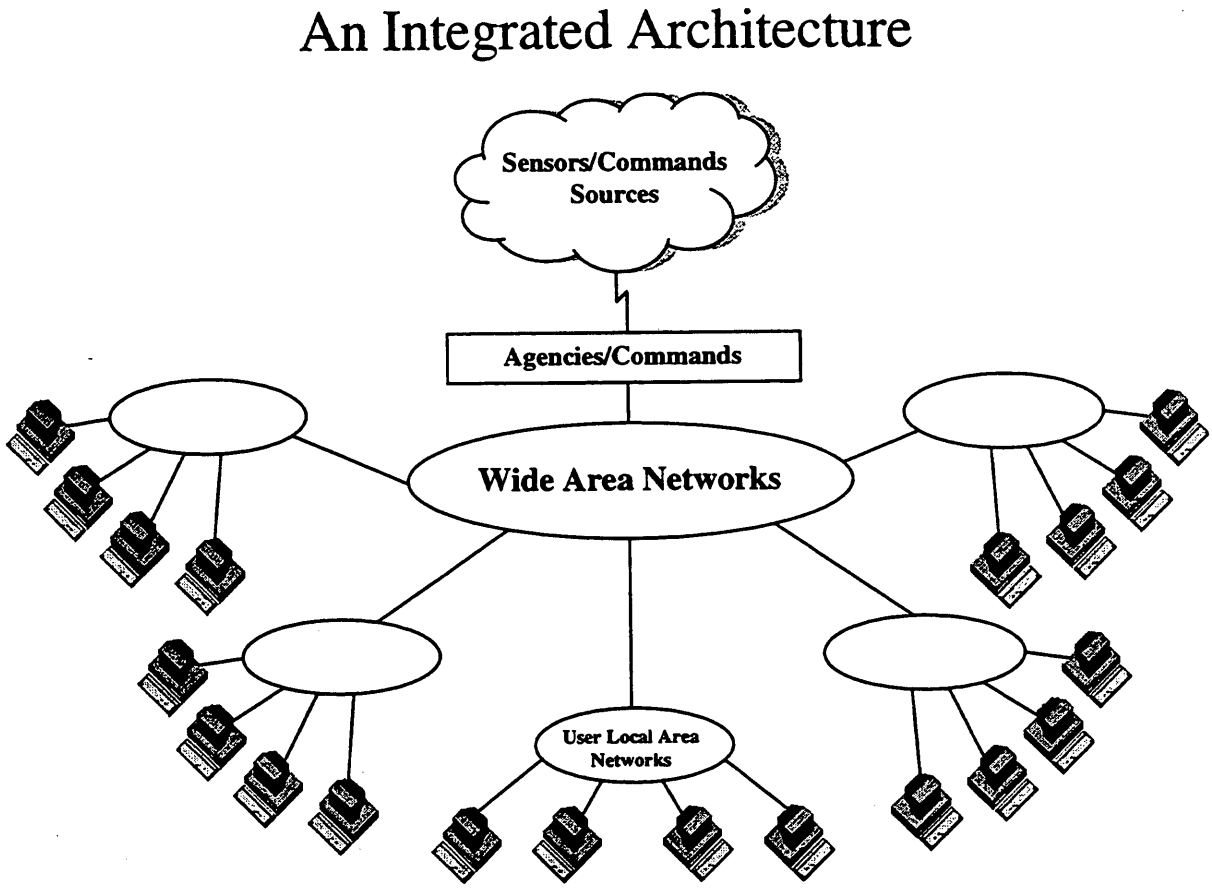


Figure 2.

Figure 3 shows how an integrated interactive multi-media workstation would have (or access) decision aids, correlation and fusion aids and visualization tools to provide the user the most pertinent and timely information. There is no intent to create and keep current monolithic data bases from which searches would be made. Data bases, as we currently know them, are necessary but hardly sufficient for our 21st century purposes. More about that shortly.

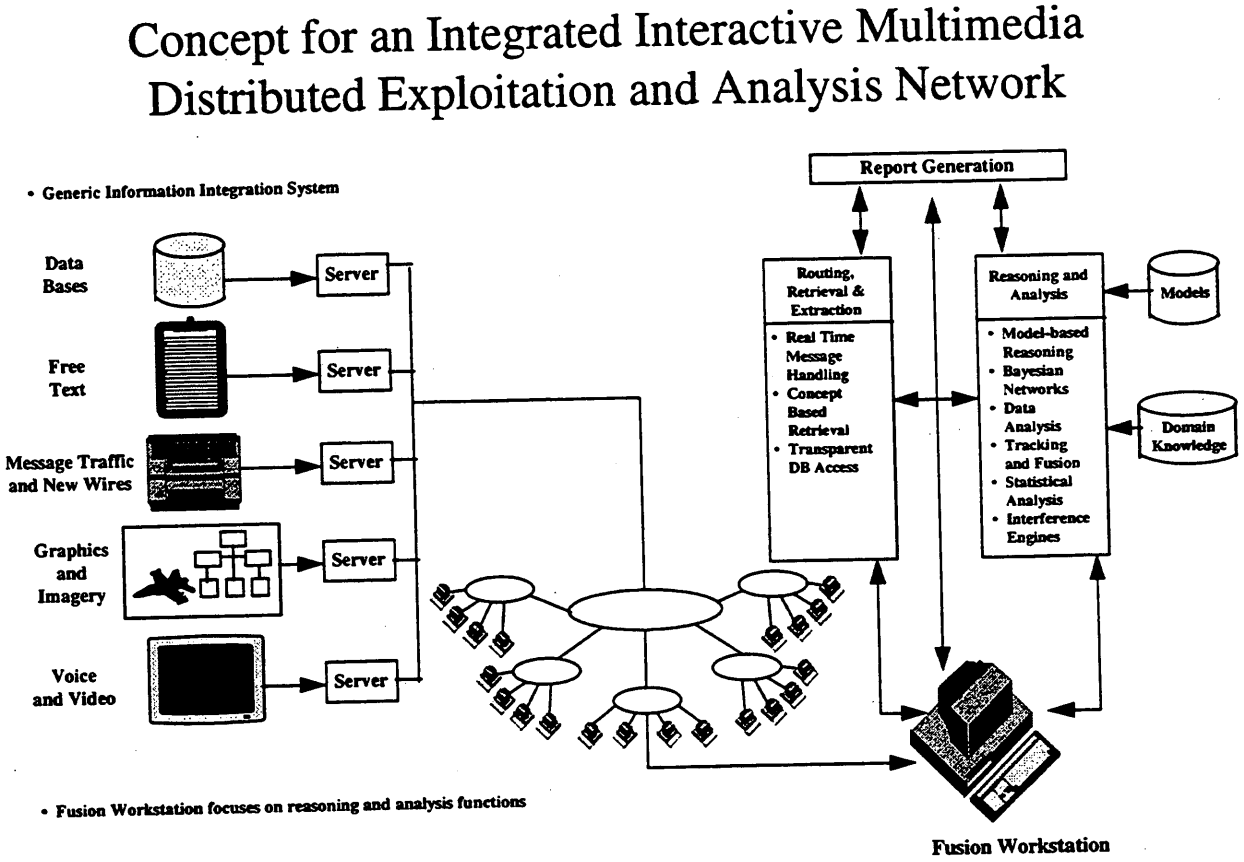


Figure 3.

A powerful aspect of this proposed National Intelligence Exploitation Architecture is that this identical infrastructure could support all of DoD, or all of the government. The tools, techniques, technology and integration required to build and implement this system, need only to provide access to the data sources others might need to serve all of DoD or all of Government. Surely there would be requirements for domain specific tools, decision aids and presentation unique or nearly unique to particular user communities. But the underlying infrastructure would be as widely applicable and robust for all, as is the INTERNET today and tomorrow. There is within the DoD a Common Operating Environment (COE), used principally as the core of the GCCS and some other C2 systems. This may offer a starting point—a building block—from which design the NIEA.

Surely many of the issues associated with the successful implementation of this architecture seem intractable today. A great deal of technology R&D and technical development must be accomplished and integrated over time to achieve these goals. This is a journey we believe is absolutely essential. Our existing "stovepipe" systems were built with old technologies under different paradigms. We have a new world, and a new paradigm for sharing information—most of which will now be unformatted, in contrast to most information in existing intelligence data bases.

Most of the existing analytical support systems in use today deal with three major types of information in various storage sizes (e.g., megabytes to terabytes). The information types are:

- Fixed-format database - file, record, field with predefined field sizes and attribute names. Collected data which cannot be fitted within the existing data definition must be discarded, since there is no way to store and retrieve it.

- Free-form text databases - unformatted messages, open source materials, etc.

- Pictorial or graphic databases - graphics, imagery, etc. (Note: these are largely still images, with limited animation or video.)

Enormous effort has gone into developing automated systems to support filing collected information into one of these types such that it can be queried, retrieved, and disseminated using existing (circa 1980) indexing and database technology. The "New World Order" and the emergence of new database types such as analog and digital video, voice, and new National collection capabilities are generating a need for tools and techniques for dealing with extremely large data vaults.

The term data vault describes a repository of data of information in a multiplicity of formats - Boolean, single character, character string, or numeric fields; free-form text; and "blobs" (Block of Bytes). Blobs can contain images, digitized audio, video, etc. Dealing with data vaults of the magnitude which we can now collect will require substantial innovation in relational and/object oriented database storage, indexing, and retrieval that are needed are:

- High speed, high volume storage and retrieval, including full automated stuffing of formatted databases from text messages and packed parameterized data streams.

- Automated means of storing, indexing and accessing blobs of non-textual materials (graphics, imagery, video, etc.) by content.

- High speed data transmission of the contents of entire data vaults or subsets thereof.

- Super high performance object database systems. Automatic format recognition and transformation. (Simple example: PICT to TARGA and the reverse. More complex

examples: Rembrandt or PictureTel to Fractal or DVI and reverse, Model 204 to SQL and Back.)

- "Profiling" of non-textual materials better than the way we now do text and messages.
- Fully automated formation of hyperlinks.
- Case Frame of Concept-based retrieval.
- Intelligent User Assistance Agents ("knowbots").
- Self Organizing databases (especially text, imagery, video, etc.).
- Superior query techniques for sporadic users who are not (and do not have time to become) data retrieval specialists (see next section).
- All of this within a secure environment (classified and unclassified).

There are a number of systems under development which may attack some of these issues. For example, EOSDIS will collect, store and make accessible on the order of terabytes a day.

Refer back to Figure 1 which illustrates the capability needed for the user in response to the explosion of dissimilar information to which we have and need access and understanding. The technologies cited above can be referred to as those necessary to provide Distributed Problem Solving (DPS) capabilities to intelligence analysts and others.

While we attempt to attack the multi-source correlation and fusion problem with the automation, we often overlook the finest and fastest correlation system available - the human eye, ear, and brain. Further, almost since the beginning of application of ADP technology to intelligence problems, analysts have asked for a "smart map."

The third fundamental piece of the puzzle is finding ways of displaying complex and voluminous disparate data streams such that our premier correlation tool can visualize them. A true smart map is one presentation approach, to which almost any analyst can relate. Some of the features included in smart maps would be: pan and zoom, movable viewpoints, active regions, alerts and alarms, validity representation and so on.

In addition to these smart map capabilities, we need better ways to visualize dynamic phenomena such as occurrences of scenario events with respect to time, and to integrate temporal and spatial relationships in displays, operations clocks, etc. These need to be integrated with the smart map display, with corresponding active regions on the timeline displays such that the analyst can access the same information from either place. Display techniques are needed to allow visualization of problems with dimensionalities higher than four (three-space + time).

Additionally, efforts in voice recognition technology could minimize keyboard entry of database and knowledge base input and queries.

The technologies cited above (and a number of others such as imagery processing, compression techniques, interactive multi-media, etc.) represent a panoply of capabilities, some of which are far more attainable or cost effective than others. Some are more likely at the end of a decade, others reasonably soon. Much of the needed technology is being developed, or will be developed in the private sector. Systems for voice recognition and understanding are already replacing commercial telephone operators; office work stations are already taking dictation; personal computers are translating scientific journals from Japanese into English. Image understanding systems are being used to read x-ray mammograms and inspecting cell cultures. Advanced computer systems are being used by commercial airlines for resource allocation and logistics planning beyond human capabilities. Other applicable commercial developments include worldwide, point-to-point voice, compressed data, and even encrypted communications for cellular phones and the INTERNET. The entertainment industry is investing huge sums to develop new wideband data distribution systems (i.e., high definition television) and direct, digital broadcast satellites.) These are all technologies which are directly applicable and will be developed far faster by commercial industry than by the government.

These technologies need not be developed twice. The trick, or course, is to pick the right ones; fit them into a critical path, and integrate them into the National Intelligence Exploitation Architecture. This drives us to realize that integration, per se, is becoming and must become a technology in its own right. Advanced integration tools, techniques and testing require significant development. DARPA, in concert with the private sector, is the obvious candidate to tackle these issues.

The challenge then for the Intelligence Community (the DCI and SECDEF) is to:

- Develop the "New Vision." This should be accomplished working with the customer base to derive a set of design objectives for the National Intelligence Exploitation Architecture. Next,

- Develop the basic system architecture road map; evaluating various technologies and approaches, and then

- Create a detailed program plan to implement the infrastructure, and

- Make needed organizational adjustments to ensure the program is carried out.

It is believed that adequate funds are present in existing NFIP (with partial DARPA support) budgets to support this architecture. Success would take commitment to a coherent road map and parsing varied development activities to agencies which would essentially become centers of excellence for varied components of this architecture. This program provides the framework for our 21st century intelligence exploitation and analysis support to government.

APPENDIX C

A TAXONOMY FOR INFORMATION WARFARE?

Taxonomy:

1. The classification of organisms an ordered system that indicates natural relationships.
2. The science, laws, or principles of classification; systematics.
3. Division into ordered groups or categories: "Scholars have been laboring to develop a taxonomy of young killers" (Aric Press).

[French taxonomie: Greek taxis, arrangement; see TAXIS + -nomie, method (from Greek -nomia; see -NOMY).] American Heritage Dictionary

Summary: A taxonomy of information warfare that describes information warfare was derived by the Defense Science Board Task Force on Information Warfare Defense. Unfortunately, as in most cases where both objects and processes are present, this taxonomy would not scale in a linear manner beyond three levels. This is the result of the number of permutations and combinations by which the attacks could be mounted against a particular process, over variable time periods. The derivation of the taxonomy is discussed latter in this Appendix.

However, by adopting concepts from Joint Pub sources and inputs of the Threat and Policy Panels of the Task Force on Information Warfare (Defense), a standard vocabulary for use in threat alerting and for the assessment and reporting of defensive preparedness, tied to specific information dependent processes, was developed for information warfare defense.

Such a tailored warning, assessment and reporting system can and should be developed for use in each civil agencies and in various domains of commercial sector such as electrical power and financial services. A caution: Whatever schema is used to evaluate the operational readiness of information dependent processes and activities, it must be timely and reflect the current state of the security policy being implemented, the supporting infrastructures (computers, communications, electricity and other supporting utilities) and the training status of the personnel, both systems administrators and users of information and information systems.

A range of standardized scenarios should be promulgated for use by the components of the Department of Defense in conducting preparedness surveys and for use in military planning. A proposed partitioning of increasingly robust assessment scenarios for use in planning and assessments follows:

1) accident. (The inclusion of accidental failure is important because in many cases the cause of failure may never be determined but it is still important to know the range of potential effect on the information dependent process.),
2) amateur hackers,
3) experienced hackers,

4) well-funded non-state group or actor able to purchase or hire advanced information warfare capabilities,

5) state-sponsored information warfare, and

6) state-sponsored information warfare with the active collusion of an authorized insider (worst case).

A standardized set of methods for assessing information dependent processes should be used so that reporting is consistent across a wide range of information dependent activities. A proposed partitioning of assessment methods follows:

a) an unknown information assurance capability for a specified assessment scenario,

b) an engineering estimate of information assurance, based on a review of design and recovery plans, but no physical testing for a specified assessment scenario,

c) an engineering estimate of information assurance, based on design parameters, simulation exercises, and the review of detection capabilities and recovery plans, but no physical testing for a specified assessment scenario,

d) an internal information assurance audit by an internal but independent organization, based examination of the written record of security and accidental incidents and responses from a live contingency plan exercises designed to simulate a specified assessment level defined above,

e) an internal information assurance audit by an internal but independent organization, based on testing and examination of security and accidental incidents and responses from a live contingency plan exercise designed to simulate a specified assessment scenario defined above, and

f) an information assurance audit by a totally independent security assessment organization, based on testing and examination of security and accidental incidents and responses from a live contingency plan exercise designed to simulate a specified assessment scenario defined above (most stringent test case).

Note that all organizations would not be expected to meet the most stringent assessment scenario. The application of an evaluation level would be determined by the criticality of the information dependent process to the overall activity.

In such an information assurance, planning, testing and evaluation construct, the most robust and resilient organization would have demonstrated a 6-f capability of information assurance.

Although not a taxonomy of information warfare, this approach provides a standard vocabulary for assessing and reporting operational readiness of organizations to carry out information dependent processes in an information warfare environment. This construct also provides a basis for developing an information warfare readiness reporting process.

Within the Department of Defense, suitable information assurance reporting criteria along the above lines should be added to the Status of Resources and Training System (SORTS) (or a SORTS-like report); Communications Spot Report (COMSPOT) and daily Communications Status Report (COMSTAT); annual CINCs Preparedness Assessment Report (CSPAR); Combat

Support Agency Assessment System (CSAAS); and the Base Defense and Operations Security evaluation schemes.

In addition to preparedness assessments, which address specific information dependent processes, a generalized threat warning system is needed to communicate a heightened level of alert to numerous interconnected information dependent activities.

Design of a warning system is complicated by the interconnectivity of the national (and global) information infrastructure. A heightened state of alert must extend to all connected systems but at higher threat levels appropriate actions could include disconnecting from the infrastructure so a warning method is needed that does not fully depend upon the interconnected infrastructure. Conceivably, preparation could include "war modes" that extend across lower levels of network protocols (physical level through transport layer protocols). In addition, a workable information warfare alert and response process will require a comprehensive legal, regulatory and operational infrastructure.

Detection of information warfare attacks will likely not come directly from intelligence or the managers of individual systems. "Warlike" attacks may have many diverse targets but probably will not follow the pattern of normal thefts or disruptions caused by amateur intruders, except as cover, concealment or deception.

Reporting of incidents, particularly of attacks on civil information users of national interest, will neither be automatic nor directed to a common point unless a distributed structure is created now, like the Center for Disease Control. Creation of a distributed reporting structure that filters upward with a focus on finding broader and broader patterns through indirect measurement and iterative analysis is essential as most "problem" detection will take place locally in a very decentralized fashion without the necessary visibility to detect the linkages between apparently unconnected events.

The Tactical Warning/Attack Assessment functions will require the synthesis of diverse and apparently unrelated information. Specialists in offensive information warfare should be included in the make-up of Department of Defense and national TW/AA centers to ensure suitable tradecraft is applied to the TW/AA process.

On receipt of an information warfare alert message or threat condition, the individual managers of information dependent processes could initiate appropriate defensive actions to include disconnecting from the shared infrastructure. Although Alert Conditions could be issued as a result of strategic warning, most would be triggered by an aggregation of tactical warning reports of individual incidents which will show a pattern of an attack rather than isolated incidents.

A set of proposed information warfare (IW) Alert Conditions and Responses for use by the Federal government, in both civil and national security activities, follow:

IW Alert Condition I

Situation – Normal

Normal level of threat from accident, crime and amateurs

Normal level of unexplained activities in all sectors of the nation

Response Required:

Normal protective actions to include:

- Due diligence in protecting information systems and assets
- Reasonable level of maintenance activities
- Compliance with IRS transaction auditing requirements
- Compliance with all applicable rules, regulations and laws

Normal level of unexplained activities in all sectors of the nation

IW Alert Condition II

Situation – Perturbation

a) 10% increase in incidence reports, either regional or within a functional information dependent activity of national interest

- Regional would include a large communally served geographic area
- Functional would include sectors of the infrastructure, including but not limited to
  - Sector systems, such as medical systems or financial systems
  - Telecommunications service providers
  - Public utilities

b) 15% increase in all incidents

- Not limited to obvious infrastructure connections

Response:

Increase incident monitoring and cooperative analysis

Look for patterns across a wide range of variables

- Including source, users, time, connection, and type of equipment

Alert all agencies to increase awareness of activities

- Including Federal agencies, regulatory bodies, trade groups, professional organization, and corporate entities

Begin selective monitoring of critical information services

- Initiate expanded audit and tracking capabilities with increased reporting to central manager

IW Alert Condition III

Situation – Heightened Defense Posture

a) 20% increase in incidence reports across the board, even with no apparent connection

b) Condition II with special contexts

- Contextual sensitivity subject to integration with all other operations and activities of the U.S.

Response:

Disconnect all unnecessary connections

- Advisory notices broadcast over diverse media to all elements of infrastructure: an IW emergency broadcast warning
- Limiting connections should force a channeling of hostile activity and reduce the number of backdoors that can be exploited

Turn on real time audit for critical information systems

- Augment audit analysis teams to handle the increased loads

Begin mandatory reporting to central manager

- Support forensic investigations and help determine the identity of the aggressors

IW Alert Condition IV

Situation – Serious Situation

a) Major regional or functional events that seriously undermine U.S. interests

b) Conditions II or III with special contexts

- Contextual sensitivity subject to integration with all other operations and activities of the U.S.

Response:

Implement alternate routing

- Example: replace a beleaguered switch with an ACTS satellite until the system can be rebuilt

Limiting interconnectivity to minimal states

- Begin triage to protect the main body

Begin "aggressive" forensics investigations

- Require legal back-up to allow active tracing of activities independent of identity or citizenship constraints
- Includes proactive defensive measures
- Includes intent to prosecute or exact retribution

IW Alert Condition V

Situation – Brink of War

a) Widespread incidents that undermine U.S. ability to function

b) Conditions III or IV with special contexts

- Contextual sensitivity subject to integration with all other operations and activities of the U.S.

Response:

Disconnect critical elements from the public infrastructure

- Deploy the Minimum Essential Information Infrastructure and temporary systems as required

Implement WARM protocols

- For critical systems, implement alternate protocols for network to transport layers of systems

Declare state of emergency

Prepare for warfare, including retribution against aggressors using the full force of the U.S.

Consideration of A Taxonomy for Information Warfare

Many of the definitions, concepts and words that follow are drawn from the Joint Publication System, and in particularly from the Joint Doctrine for Command and Control Warfare and the Joint Reporting Structure.

The central concept of information warfare is straightforward: The ultimate target of information warfare is an information dependent process, whether human or automated. The use of the word "warfare" should not be construed as limiting information warfare to a military conflict, declared or otherwise.

The root concept of information warfare is offensive in nature. In turn, the concept of information warfare defense flows from the offense. This is not surprising as most defensive actions (counter-air, anti-submarine warfare, counter-mine, anti-crime, anti-drug) only have meaning within the context of action-reaction. Offensive information warfare targets information or information systems in order to affect the information dependent process, whether human or automated. Defensive information warfare protects the information dependent process, whether human or automated

The question of interest is whether a useful taxonomy information warfare can be derived.

In Joint Pub 3-13.1, Joint Doctrine for Command and Control Warfare, an "information system" is defined as the organized collection, processing, transmission, and dissemination of information, in accordance with defined procedures, whether automated or manual. This includes the entire infrastructure, organization, and components that collect, process, store, transmit, display, and disseminate information. It includes everything and everyone that performs these functions—from a laptop computer to local and wide-area voice and data networks, broadcast facilities, buried cable and, most importantly, the people involved in transmitting, receiving, processing, and using the information. People, decisionmakers at all levels, are the most important part of the information system.

However, information systems themselves are part of larger information infrastructures. These infrastructures link individual information systems in a myriad of direct and indirect paths. The growing information infrastructures of today transcend industry, media, and the military and includes both government and non-government entities. The collection, processing, and dissemination of information by individuals and organizations comprise an important human dynamic, which is an integral part of the information infrastructure. A news broadcast on CNN, a diplomatic communiqué, and a military message ordering the execution of an operation all depend on the global information infrastructure. The information infrastructure has been assigned three categories global information infrastructure (GII), national information infrastructure (NII), and defense information infrastructure (DII).

- The GII is the worldwide interconnection of communications networks, computers, data bases, and consumer electronics that make vast amounts of information available to users. It encompasses a wide range of equipment, including cameras, scanners, keyboards, fax machines, computers, switches, compact disks, video and audio tape, cable, wire, satellites, fiber-optic transmission lines, microwave, nets, switches, televisions, monitors, printers and much more. The GII, however, includes more than just the physical facilities used to store, process, and display voice data. The personnel who operate and consume the transmitted data constitute a critical component of the GII.
- The NII is the subset of the GII within the U.S. used for social, economic and national security activities.
- The DII is the shared or interconnected system of computers, communications, data applications, security, people, training, and other support structures serving DoD's local, national and worldwide information needs. The DII connects DoD mission support, command and control (C2), and intelligence computers through voice, telecommunications, imagery, video and multimedia services. It provides information processing and services to subscribers over the Defense Information Systems Network. It includes C2, tactical, intelligence and commercial communications systems used to transmit DoD data

In actuality the GII, NII and DII labels are misleading as there are few distinct boundaries in the information environment. The DII, NII, and GII are inextricably intertwined, a trend that will only intensify with the continuous application of rapidly advancing technology. Again, no ordered structure is readily apparent on which to base a taxonomy.

If information warfare targeting and information warfare defense are shaped by particular information dependent processes then perhaps ordering information dependent processes will lead to a structure. However, only a little reflection leads to the conclusion that there are an infinite variety and scope of information dependent processes. Clearly, there is no "ordered system" that will tie these potential processes together, other than the shared characteristic of depending on information. Enumerating information dependent processes will not yield a taxonomy.

What of the methods of information warfare? Consider that attacks and defenses may involve:

- Physical attacks the components of the information infrastructure, e.g., computers, communications devices, software, cables, control devices, etc.

- Physical attacks on the components containing or supporting the information infrastructure such as buildings, power systems, environmental services.
- Physical attacks on or the subversion of the people (witting or unwitting) who operate elements of the information infrastructure.
- Physical destruction of information (erasure or over-write) without harming the infrastructure components.
- Logic (malicious code) attacks on the components of the information infrastructure, e.g., computers, communications devices, software, control devices, etc.
- Logic attacks on computer-controlled components supporting the information infrastructure. These may include air conditioners, air handlers, power distribution, and cooling water.
- Attacks on information provided via the information infrastructure that is used by a specific function(s) (e.g., deception operations, and insertion of false information).
- Corruption of information using logic or digital attacks without harming the components of information infrastructure. (The greatest harm may result from an attack which corrupts or injects false information in a manner that cannot be detected by the users of that information who subsequently take actions based on the corrupted or false information.)
- Combined attacks where both physical and logical attacks on the information infrastructure or supporting elements are undertaken in combination to either mask one or the other types of attack or to obtain the benefits of a combined attack.

From the above it follows that at the highest level information dependency can be partitioned into two elements: one, the availability of information needed by the process; and two, the integrity of information used in the process. Some would add a third element, the confidentiality of information, as it is an important factor in many civil and military information dependent processes. In the following derivation all three are addressed. Note that this trial taxonomy is irrespective of the offensive or defensive actions that may be undertaken to achieve or defend against these conditions it is just a structure for information warfare.

A top-level taxonomy for information warfare

Availability of information or information services

Loss of information

Detected on occurrence

Detected after *n** units of time

Undetected

Delay in receipt of information

Detected on occurrence

Detected after n units of time

Undetected

Loss of an information service

Detected on occurrence

Detected after *n* units of time

Undetected

Delay in an information service

Detected on occurrence

Detected after *n* units of time

Undetected

Integrity of information

Unauthorized change in data

Detected on occurrence

Detected after *n* units of time

Undetected

Insertion of false data

From a correct source

Detected on occurrence

Detected after *n* units of time

Undetected

From an incorrect source

Detected on occurrence

Detected after *n* units of time

Undetected

Confidentiality of information

Compromise detected on occurrence

Compromise detected after *n* units of time

Compromise undetected

*The unit of time can vary from microseconds to years. The criticality of *n* is determined by the information dependent process in each particular case

Although only at three levels of complexity this sample taxonomy rapidly becomes unwieldy. Complexity grows at the next level as each of these conditions can be the result of accident or caused by deliberate intent. In many cases it may be impossible to determine which led to the

condition. At the next level deliberate intent can be carried out by an exterior actor, an insider with authorized access to the information or information services use in an information dependent process, or by both internal and external actors may be working in concert. Then there is the factor of time. If the failure was detected only after n units of time had elapsed, the affects that matter cannot be generalized but rather are unique to a specific information dependent process. The introduction of process-dependent timing takes us back to the earlier infinite variety of processes which has already been rejected as a basis for a taxonomy.

But to press on with this sample taxonomy, we recognize that all of these events can be arrayed in multiple sequences and combinations. There are an infinite combination and permutation of such attack methods and countering defenses available for application within the intertwined DII/NII/GII environment. Thus, an attempt to add successive layers to the taxonomy sketched out above would explode into incomprehensible complexity. Each element of data; each bit and byte of software; each device, whether in a computer at an end-node or along a communication path; each waveform; and each person with access to any of the components would have to be mapped onto the structure.

It is just this complexity that is large part of the challenge facing the defender: he cannot know or protect against all the possible means of attack to succeed, the attacker needs only to know one weakness that the defender has left unprotected or have a weapon that can breech one point in defense. This is the imperative for risk management, resilient systems, and robust recovery capabilities. Again, although a top-level information warfare taxonomy can be sketched, it does not scale to a useful construct. (See the last page of this Appendix for a footnote on complexity.)

Now the principle reason an information warfare taxonomy is a desired objective is that it adds precision to communication. Although the simple taxonomy sketched above does not meet that goal, a workable alternative is proposed that can be inserted into existing reporting structures. The development of this alternative to a taxonomy has the benefit that it builds on existing models from the Joint Publications System.

Joint Publication 1-03, "**Joint Reporting Structure (JRS),**" establishes a standard reporting vocabulary for the Department of Defense. Joint Publication 1-03.3 establishes the "**Status of Resources and Training System (SORTS)**", and provides the general provisions and detailed instructions for collecting and preparing data on units of the U.S. Armed Forces and selected foreign and international organizations. In practice, the utility of SORTS is not optimum because of the timeliness and quality of data submitted. Whether incorporated in SORTS or a stand-alone method, an information warfare SORTS-like reporting scheme is needed.

SORTS functions as the following:

a. Central Registry of All Operational Units in the U.S. Armed Forces. SORTS is the single, automated reporting system within the Department of Defense that provides the National Command Authorities (NCA) and the Chairman of the Joint Chiefs of Staff with authoritative identification, location, assignment, personnel, and equipment data for the registered units and organizations of the U.S. Armed Forces, Defense agencies, and certain foreign and international organizations involved in operations with U.S. Armed Forces. The composite registry of all units is maintained by the Joint Staff. After initial registration, SORTS is designed to receive reports by exception when changes occur.

b. Repository of Resource Status of Selected Units. For selected registered units, SORTS also provides the condition and level of resources and training. This includes the unit commander's assessment of how resources and training levels will affect the unit's ability to undertake its wartime mission. Units report by exception within 24 hours of a change or as directed by the Chairman of the Joint Chiefs of Staff. If no change in unit status occurs within 30 days of report submission, units submit a validation report.

SORTS contains provisions for reporting various readiness items:

(a) Overall C-Level (OVERALL) Set. Data in this set include the overall C-Level for the unit and the codes for primary, secondary, and tertiary degradation reasons. The overall readiness showing how well the unit meets prescribed levels of personnel, equipment, and training for the wartime mission for which the unit has been organized or designed is ranked in descending order from C-1 to C-5:

C-1. The unit possesses the required resources and is trained to undertake the full wartime mission(s) for which it is organized or designed. The resource and training area status will neither limit flexibility in methods for mission accomplishment nor increase vulnerability of unit personnel and equipment. The unit does not require any compensation for deficiencies.

C-2. The unit possesses the required resources and is trained to undertake most of the wartime mission(s) for which it is organized or designed. The resource and training area status may cause isolated decreases in flexibility in methods for mission accomplishment but will not increase vulnerability of the unit under most envisioned operational scenarios. The unit would require little, if any, compensation for deficiencies.

C-3. The unit possesses the required resources and is trained to undertake many, but not all portions of the wartime mission(s) for which it is organized or designed. The resource and training area status will result in significant decreases in flexibility for mission accomplishment and will increase vulnerability of the unit under many, but not all, envisioned operational scenarios. The unit would require significant compensation for deficiencies.

C-4. The unit requires additional resources or training to undertake its wartime mission(s), but it may be directed to undertake portions of its wartime mission(s)) with resources on hand.

C-5. The unit is undergoing a Service-directed resource action and is not prepared, at this time, to undertake the wartime mission(s)) for which it is organized or designed.

(b) Personnel Level (PERSONEL) Set. Data in this set include the personnel level (P-level) and a code for the primary reason for degradation in the personnel area.

(c) Equipment and Supplies On Hand Level (EQSUPPLY) Set. Data in this set include the equipment and supplies on hand level (S-level) and a code for the primary reason for degradation in the equipment and supplies on hand area.

(d) Equipment Condition Level (EQCONDN) Set. Data in this set include the equipment condition level (R-level) and a code for the primary reason for degradation in the equipment condition area.

(e) Training Level (TRAINING) Set. Data in this set include the training level (T-level) and a code for the primary reason for degradation in the training area

(f) Forecasted Category Level (FORECAST) Set. Data in this set include the forecasted C-level for the unit and the date the unit expects to attain that C-level.

(g) Category Level Limitation (CATLIMIT) Set. Data in this set include the imposed maximum C-level for the unit, if any, and the primary resource area causing the limitation.

An additional category should be added to SORTS specifying at what level of assessment scenario the unit is prepared to operate and how this preparedness was assessed using the terminology described earlier.

Joint Pub 1-03.10, "**JRS Communications Status,**" provides for the Defense Information Systems Agency to provide near-real-time status information on a serious degradation of the Defense Communication System (DCS) via a Communications Spot Report and to provide a summary of significant status information on the DCS via a daily Communications Status Report.

These reports should be expanded to include information systems and information services. Further, these reports should be used by the military departments, services, combat support agencies and the CINCs to report the status of information systems and services.

Joint Pub 1-03.31, "**Preparedness Evaluation System,**" establishes the CINCs Preparedness Assessment Report (CSPAR). These report provide a biennial appraisal of the preparedness of the unified and specified commands to accomplish Joint Strategic Capability Plan tasks (both supporting and supported) within the constraints of the total apportioned force (Active and Reserve). In the CSPAR, each CINC identifies overall strengths and significant deficiencies affecting the command's ability to carry out assigned missions and execute the plans produced during the most recent planning cycle. In submitting the CSPAR, CINCs are reporting on their ability to accomplish a specific task using available capabilities.

The CINCs should be required to include an assessment of their ability to carry out assigned missions at the appropriate assessment scenario level and indicate the process used to determine preparedness.

Joint Pub 1-03 32 1. "**Combat Agency Assessment System,**" sets forth the guidelines and procedures for operating the Combat Support Agency Assessment System (CSAAS), a uniform system for reporting to the Secretary of Defense, the commanders of the unified and specified commands (CINCs), and the Secretaries of the Military Departments concerning readiness of each combat support agency to perform with respect to a war or threat to national security.

Chairman, Joint Chief of Staff (CJCS)-sponsored exercises provide the principal means of on-site evaluation of agency responsiveness in reacting to National Command Authority decisions and CINC warfighting requirements. In the event no such exercises are scheduled during the first two quarters of even-numbered fiscal years, Joint Staff observers conduct independent site visits to each of the combat support agencies. Although the CSPAR is the principal means for the

combatant commands to assess agency support, Joint Staff observers may also visit combatant command headquarters to discuss overall support, agency supporting plans, and ongoing efforts to improve shortfalls.

These reports should be modified to include an annual assessment of the preparedness of the combat support agencies, at a specified assessment level to carry out their mission. The current two year schedule currently followed in assessing the readiness of combat support agencies is not realistic in an age of information warfare. The information dependent processes of these agencies are directly tied to the ability to mobilize, deploy and sustain the forces. Currently, this is an unknown in the age of information warfare.

Joint Pub 3-10.1, "**Joint Tactics, Techniques, and Procedures for Base Defense**," categorizes threats to bases in the rear area by the levels of defense required to counter them. Emphasis on specific base defense and security measures may depend on the anticipated threat level. (These threat levels are discussed in detail in Joint Pub 3-10.)

a. Level I threats can be defeated by base or base duster self-defense measures.

b. Level II threats are beyond base or base cluster self-defense capabilities but can be defeated by response forces, normally military police (MP) units assigned to area commands with supporting fires.

c. Level III threats necessitate the command decision to commit a Theater Contingency Force. Level III threats, in addition to major ground attacks, include major attacks by aircraft and theater missiles armed with conventional weapons or nuclear, biological and chemical (NBC) weapons.

The threat to bases in the rear area should be modified to include information warfare attacks.

Joint Pub 3-10.1 also spells out Threat Conditions and Responses and states that in combating terrorism, bases should use common terrorist threat conditions (THREATCONs), each with its specific security measures and required responses.

Threat assessments are used to determine threat levels, to implement security decisions, and to establish awareness and resident training requirements. Threat levels are determined by an assessment of the situation using the following six terrorist threat factors:

(1) Existence. A terrorist group is present, assessed to be present, or able to gain access to a given country or locale.

(2) Capability. The acquired, assessed, or demonstrated level of capability to conduct terrorist attacks.

(3) Intentions. Recent demonstrated anti-U.S. terrorist activity, or stated or assessed intent to conduct such activity.

(4) History. Demonstrated terrorist activity over time.

(5) Targeting. Current credible information on activity indicative of preparations for specific terrorist operations.

(6) Security Environment. The internal political and security considerations that impact on the capability of terrorist elements to implement their intentions.

The severity of the terrorist threat is indicated by the designated threat level, assigned through. analysis of the above threat assessment factors. Threat levels, and associated factors, are:

(1) Critical. Factors of existence, capability, and targeting must be present. History and intentions may or may not be present.

(2) High. Factors of existence, capability, history and intentions must be present

(3) Medium. Factors of existence, capability, and history must be present. Intentions may or may not be present.

(4) Low. Existence and capability must be present. History may or may not be present.

(5) Negligible. Existence and/or capability may or may not be present.

The terrorist threat level is one of several factors used in the determination of terrorist THREAT CON. Factors that enter into the decision to assign a particular THREATCON and its associated measures include threat, target vulnerability, criticality of assets, security resource availability, impact on operations and morale, damage control, recovery procedures, international regulations, and planned U.S. Government actions that could trigger a terrorist response.

The terrorist THREATCON system provides a common framework to facilitate inter-Service coordination, support U.S. military anti-terrorist activities, and enhance overall DoD implementation of U.S. Government anti-terrorist policy. THREATCONs are described below:

(1) THREATCON NORMAL. Applies when a general threat possible terrorist activity exists, but the threat warrants a routine security posture.

(2) THREATCON ALPHA. Applies when there is a general threat of terrorist activity against personnel and installations, the exact nature and extent of which are unpredictable and circumstances do not justify full implementation of THREATCON BRAVO measures. However, base defense forces may have to implement selected measures from higher THREATCONs based on intelligence received. Base defense forces must be able to maintain the measures in this THREATCON indefinitely.

(3) THREATCON BRAVO. Applies when an increased and more predictable threat of terrorist activity exists. Base defense forces must be able to maintain the measures of this THREATCON for weeks without causing undue hardship, without affecting operational capability, and without aggravating relations with local authorities.

(4) THREATCON CHARLIE. Applies when an incident occurs or when intelligence indicates an imminent terrorist action against U.S. bases and personnel. Implementation of measures in the THREATCON for more than a short period probably will create hardship and affect peacetime activities of the unit and its personnel. Sustaining this posture for an extended period probably will require augmentation.

(5) THREATCON DELTA. Applied in the immediate area where a terrorist attack has occurred or when intelligence has been received that terrorist action against a specific location is likely. Normally, this THREATCON is declared as a localized warning.

The description of threat levels, threat assessments, severity of threat, and threat condition found in Joint Pub 3-10.1 is a good model for information warfare defense preparation, assessment, and warning.

Finally, Joint Pub 3-54, "**Joint Doctrine for Operations Security,**" Change 1, Appendix E, outlines procedures for Operations Security (OPSEC). These surveys in general:

a. Thoroughly examine an operation or activity to determine if adequate protection from adversary intelligence exploitation exists.

b. Check on how effective the OPSEC measures the operation or activity being surveyed in protecting protect its critical information.

c. Cannot be conducted until after an operation or activity has at least identified its critical information for without a basis of identified critical information, there can be no specific determination that actual OPSEC vulnerabilities exist. (This is also true in information warfare.)

Each OPSEC survey is unique. Surveys differ in the nature of the information requiring protection, the adversary collection capability, and the environment of the activity to be surveyed

a. In combat, a survey's emphasis must be on identifying operational indicators that signal friendly intentions, capabilities, and/or limitations and that will permit the adversary to counter friendly operations or reduce their effectiveness.

b. In peacetime, surveys generally seek to correct weaknesses that disclose information useful to potential adversaries in the event of future conflict. Many activities, such as operational unit tests, practice alerts, and major exercises, are of great interest to a potential adversary because they provide insight into friendly readiness, plans, crisis procedures, and C2 capabilities that enhance that adversary's long-range planning.

OPSEC Surveys are not Security Inspections:

a. OPSEC surveys are different from security evaluations or inspections. A survey attempts to produce an adversary's view of the operation or activity being surveyed. A security inspection seeks to determine if an organization is in compliance with the appropriate security directives and regulations.

b. Surveys are always planned and conducted by the organization responsible for the operation or activity that is to be surveyed. Inspections may be conducted without warning by outside organizations.

c. OPSEC surveys are not a check on the effectiveness of an organization's security programs or its adherence to security directives. In fact, survey teams will be seeking to determine if any security measures are creating OPSEC indicators.

d. Surveys are not punitive inspections, and no grades or evaluations are awarded as a result of them. Surveys are not designed to inspect individuals but are employed to evaluate operations and systems used to accomplish missions.

e. To obtain accurate information, a survey team must depend on positive cooperation and assistance from the organizations participating in the operation or activity being surveyed. If team members must question individuals, observe activities, and otherwise gather data during the course of the survey, they will inevitably appear as inspectors, unless this nonpunitive objective is made clear.

f. Although reports are not provided to the surveyed unit's higher headquarters, OPSEC survey teams may forward to senior officials the lessons learned on a nonattribution basis. The

senior officials responsible for the operation or activity then decide to further disseminate the survey's lessons learned.

There are two basic kinds of OPSEC surveys: command and formal.

a. A command survey is performed using only command personnel and . on events within the particular command

b. A formal survey requires a survey team composed of members from inside and outside the command and will normally cross command lines (after prior coordination) to survey supporting and related operations and activities.

c. Both types of surveys follow the same basic sequence and procedures.

Although Joint Pub 3-54 is scheduled to be rewritten, it is quoted extensively as another possible model for conducting information warfare assessments. The assessment methodology cited at the beginning of the annex should yield more rigorous conclusions.

By adopting concepts from each of the Joint Pub sources cited above a standard vocabulary of status reporting, tied to specific information dependent processes, can be developed for information warfare. Such an assessment and reporting system should be developed that stands on its own for use in civil agencies and the commercial sector. Within the Department of Defense this may be more easily achieved by making suitable modification of the several portions of the Joint Reporting System.

In the case of information warfare, as in the terrorism example above, a range of standardized threat scenarios should be promulgated for use in conducting preparedness surveys, as standardized assessment conditions for planning purposes, and a set of standardized threat warnings or THREATCONS, if warning is available.

Whatever schema is used to evaluate the operational readiness of information dependent processes and activities, it must be timely and reflect the current state of the security policy being implemented, the supporting infrastructures (computers, communications, electricity and other supporting utilities) and the training status of the personnel, both systems administrators and users of information and information systems.

Complexity Footnote:

A military example of how the complexity builds is found in command and control warfare (C2W). The U.S. military defines C2W as an application of information warfare in military operations.

The execution of C2W involves the integrated use of some or all of the tools of psychological operations (PSYOP), military deception, operations security (OPSEC), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary C2 capabilities while protecting friendly C2 capabilities against such actions. Again, these are just means to carry out information warfare in a particular military environment.

Defensive tools called out in Joint Pub 6.0, Doctrine for C4 Systems Support to Joint Operations, include:

(1) Physical security of facilities,

(2) Personnel security of individuals authorized access to systems,

(3) Operations security (OPSEC) procedures and techniques protecting operational employment of C4 system components,

(4) Deception, deceiving the adversary about specific system configuration, operational employment, and degree of component importance to mission accomplishment,

(5) Low probability of intercept (LPI) and low probability of detection (LPD) capabilities and techniques designed to defeat adversary attempts to detect and exploit transmission media

(6) Emissions control procedures designed to support OPSEC and LPI/LPD objective,

(7) Transmission security capabilities designed to support OPSEC and LPI/ LPD objectives,

(8) Communications security (COMSEC) capabilities to protect information transiting terminal devices and transmission media from adversary exploitation,

(9) Computer security capabilities to protect information at rest, being processed, and transitioning terminal devices, switches, networks, and control systems from intrusion, damage, and exploitation,

(10) System design and configuration control (e.g., protected distribution systems, protection from compromising emanation (TEMPEST)) to mitigate the impact of information technology vulnerabilities, and

(11) Identifying technological and procedural vulnerability analysis and assessment programs.

To this list can be added nonrepudiation, identification and authorization, end-user use of encryption services, transmission encryption, replication, and a host of other techniques to protect various elements of the information infrastructure. As in the case of C2W, these are tools and in themselves, they are not information warfare.

APPENDIX D

ORGANIZATIONAL MODELS

The Task Force reviewed three organizational models for possible application at the Department of Defense or national levels. These included the Centers for Disease Control and Prevention, the Federal Emergency Management Agency, and the National Drug Intelligence Center. The following reviews are provided for reference only.

D.1 CENTERS FOR DISEASE CONTROL AND PREVENTION

Surveillance, Research, Prevention Efforts In The Area Of Infectious Diseases:

Applicability Of CDC Experience To A
National Center For Information Systems Security

D.1.1 Introduction

In the United States, the threat of infectious disease is changing rapidly in conjunction with dramatic changes in global society and environment. Worldwide, there is explosive population growth with expanding poverty and urban migration which, with rapid environmental changes, is resulting in the emergence of new and the reemergence of previously controlled infectious diseases; international travel is increasing so that infectious microbes can easily travel across borders with their human or animal hosts. Diseases that arise in other parts of the world are repeatedly introduced into the United States, where they may threaten our national health and security.

The threats to the U.S. Information Technology (IT) infrastructure bear similarities to the emerging infectious disease threat to public health. In particular, the context of Information Warfare Defense is parallel to that in public health. IT infrastructure growth, changing technology and increasing network interconnectivity correspond to global population growth, environmental change and increased travel. The U.S. Government approach to the increasing public health threat, led by the Centers for Disease Control and Prevention (CDC), can provide lessons in responding to national IT security threats.

D.1.2 Background and Legislative History

The Centers for Disease Control and Prevention (CDC) is an agency of the Public Health Service, in the Department of Health and Human Services. Its mission is to promote health and quality of life by preventing and controlling disease, injury, and disability. As the nation's prevention agency, the CDC accomplishes its mission by working with partners throughout the nation and the world.

The CDC formally came into being in a department reorganization in 1980. In 1993, the organization officially became known as the Centers for Disease Control and Prevention, but the commonly known abbreviation CDC remained.

The CDC traces its beginnings to 1946 when the Communicable Disease Center was established as a Field Station of the Bureau of State Services in the Public Health Service. It took over the offices and some responsibilities of the DoD's Office of Malaria Control which was being disestablished. The primary mission was to work with the States in tracking and controlling the spread of communicable diseases in the United States.

The Center grew out of the general authority granted to predecessor organizations of the Department of Health and Human Services (HHS) That is, no specific legislation was required for its establishment. However, it is noteworthy that in 1893 Congress mandated that state and municipal authorities report information weekly about the incidence of certain diseases to the Public Health Service. Currently, CDC general authority flows through the general authority given to the Secretary for Health and Human Services. Funding for studies on specific programs such as lead poisoning prevention, HIV, and breast cancer prevention are contained in various legislative acts.

CDC supports surveillance, research, prevention efforts, and training in the area of infectious diseases through its National Center for Infectious Diseases (NCID). Created in 1981, NCID is committed to the prevention and control of traditional, new, and reemerging infectious diseases in the United States and around the world.

NCID accomplishes its mission of preventing illness and death from infectious diseases by focusing its resources in five areas:

- Epidemic Assistance
- Surveillance Of Infectious Diseases, In Collaboration With State And Local Health Departments
- Epidemiological And Laboratory Research
- Formulating, Disseminating, And Evaluating Prevention And Control Strategies
- Training And Consultation Programs In Cooperation With Other CDC Units And Outside Agencies And Organizations

D.1.3 Concept of Operations: The CDC Approach to the Global Threat of Infectious Disease

NCID Surveillance Activities

NCID collects, analyzes, and interprets reports of nationally notifiable infectious diseases and outbreaks submitted by state and local public health agencies and disseminates the findings. In addition to this traditional form of surveillance, the center uses supplemental, non-traditional systems to monitor trends in infectious diseases of public health importance. These systems include laboratory-based surveillance; population-based active surveillance; sentinel physician networks; hospital-based networks for surveillance of infections; analyses of national databases; and serosurveys and studies of special populations and settings. The Center also collaborates with international organizations and agencies in the global surveillance of selected pathogens.

Partnerships

NCID provides epidemiological, microbiologic, and consultative services to federal agencies, state and local health departments, medical and biomedical science institutions, schools of public health, health care providers, and the World Health Organization (WHO) and other international agencies.

D.1.4 Appropriate Analogies/Examples in the National Responses to the Threat of Infectious Disease

The similarities that the threats to the U.S. Information Technology (IT) infrastructure bear to the emerging infectious disease threat to public health suggest that the CDC experience can provide lessons in responding to national IT security threats. Below are elements of the CDC approach to the threat to U.S. public health which appear to apply to any formulation of a response to IT threats.

Formulating a National Strategic Response Plan

CDC's NCID strategic plan of 1994 has identified need to:

- improve public health infrastructure at local, state and national level
- recognize the global nature of the problem
- institute global surveillance.

The Plan's goals are:

Goal I - *Surveillance*: Detect, promptly investigate, and monitor emerging pathogens, the diseases they cause, and the factors influencing their emergence.

Goal II - *Applied Research*: Integrate laboratory science and epidemiology to optimize public health practice.

Goal III - *Prevention and Control*: Enhance communication of public health information about emerging diseases and ensure prompt implementation of prevention strategies.

Goal IV - *Infrastructure*: Strengthen local, state, and federal public health infrastructures to support surveillance and implement prevention and control programs.

Similarly, the Federal Government must have a strategic plan to respond to the increasing IT threat, a plan to:

- improve IT infrastructure security at the national level,
- recognize the ubiquitous nature of the problem and
- institute national (and even global) surveillance.

The goals of such a plan could be expected to closely parallel those of CDC's NCID strategic plan:

Goal I - *Surveillance*: Detect, promptly investigate, and monitor Information Technology Infrastructure threats, and the factors influencing their occurrence.a national consortium of IT providers and users to promote rapid interchange of event occurrence information a near real time monitoring and assessment function

Goal II - *Applied Research*: Integrate private industry, standards body and government research and development to optimize public and private security practice. Support R&D in IT security. Establish effectiveness studies and disseminate results

Goal III - *Prevention and Control*: Enhance communication of industry and government information about emerging security threats and ensure prompt implementation of prevention and control strategies. Disseminate information. Support security implementation guidelines/ standards.

Goal IV - *Infrastructure*: Strengthen national and international infrastructures to support surveillance and implement prevention and control programs. Promote establishment of procedures and policies with supporting legislation and industry, government and intergovernmental agreements. Promote establishment of IT security centers (analogous to Carnegie Mellon's role in S/W process improvement) for research, standards development and training

Establishing an Information Exchange Infrastructure

The Information Network for Public Health Officials (INPHO) was initiated by the Centers for Disease Control and Prevention (CDC) in 1992 as part of its strategy to strengthen the infrastructure of public health in the United States. The ultimate goal of INPHO is to improve the health of Americans through more effective public health practice. CDC's role in the INPHO initiative is to provide policy and technical assistance states can use to develop INPHO projects for their own public health needs.

The INPHO initiative addresses the serious national problem that public health professionals have lacked ready access to much of the authoritative, technical information they need to identify health dangers, implement prevention and health promotion strategies, and evaluate health program effectiveness. INPHO utilizes state-of-the-art telecommunications and computer networks to give state and community public health practitioners new command over information resources.

As the U.S. health care system shifts towards a managed care model, the role of public health agencies increasingly will center on the provision and use of information. Public health will be responsible for key functions that health care providers themselves cannot perform: 1) systematic surveillance and assessment of health trends, 2) assurance that those in need receive health services, that health care is not excessively costly, and that community health goals are met, and 3) clarifying policy options and implications for public and private decision makers. INPHO helps states build strategic information partnerships between people and organizations that are critical to achieving these goals.

There are three essential components of the INPHO vision: linkage, information access, and data exchange. INPHO computer networks and software link local clinics, state and federal health agencies, hospitals, managed care organizations and other providers, eliminating geographic and

bureaucratic barriers to communication and information exchange. Public health practitioners have unprecedented electronic access to health publications, reports, databases, directories, and other information. High speed communications capacity enables them to communicate and exchange data locally and across the nation on the full universe of public health issues. (The INPHO is described further in Attachment 1.)

Similarly, the Federal Government might promote or sponsor systematic information and data exchange among national, state and local IT users and providers to respond to the increasing IT threat.

Convening an Inter-Agency Working Group to Recommend U.S. Government Actions

A U.S. Government interagency working group was convened on December 14, 1994, to consider the global threat of emerging and re-emerging infectious diseases. The working group was established under the aegis of the Committee on International Science, Engineering, and Technology Policy (CISET) of President Clinton's National Science and Technology Council. Dr. David Satcher, the Director of the Centers for Disease Control and Prevention (CDC), chaired the CISET working group, which included five sub-groups with co-chairs from CDC, the Food and Drug Administration (FDA), the National Institutes of Health (NIH), the U.S. Agency for International Development (USAID), the Department of Defense (DoD), and the State Department. The working group's membership, which included representatives from more than 17 different Government agencies and departments, reviewed the U.S. role in detection, reporting, and response to outbreaks of new and re-emerging infectious diseases and made a number of recommendations which are described in *Global Microbial Threats in the 1990s*, published in late 1995 by the President's National Science and Technology Council.

As with the National Science and Technology Council's Government interagency working group on the global microbial threat, a multi-agency government advisory panel to recommend U.S. Government responses to the IT threat might be appropriate.

Forming Partnerships for Interaction, Cooperation, and Coordination

Effective public health policy results from interaction, cooperation, and coordination among a wide range of public and private organizations and individuals. Particularly critical to this process are CDC's partnerships with state and territorial health departments; other federal agencies; professional organizations; academic institutions; private health care providers; health maintenance organizations and health alliances; local community organizations; private industry; and international partners, including the World Health Organization (WHO) and international service organizations and foundations. Each of these partners play an integral role in the cooperative efforts required to safeguard the public's health from emerging infectious disease threats.

CDC partnerships at the federal level have been helpful in confronting infectious diseases of public health importance in the United States. For example, CDC and NIH developed improved diagnostic tests for Lyme disease and various fungal infections. CDC has also worked closely

with FDA and USDA in controlling emerging foodborne illnesses. Recent CDC collaborations with EPA have been instrumental in recognizing and controlling waterborne outbreaks of giardiasis and cryptosporidiosis in several states.

In addition, CDC has often joined forces with USDA and DoD to control or prevent vector-borne infectious disease threats. Such cooperative efforts were used successfully to address potential mosquito-borne illness following Hurricane Andrew in Florida and Louisiana in 1992.

Clear, well-established lines of communication and responsibility between appropriate personnel in federal agencies, such as CDC, NIH, EPA, FDA, USDA, DoD, and others, are essential to the development of efficient, cost-effective prevention and control strategies. Such links help eliminate costly duplication of effort and focus limited federal resources on the early recognition and timely control of new infectious disease problems.

Similarly any U.S. Government effort to meet the IT threat would require active, long-term partnerships among Federal agencies and with elements of the IT industry.

Assume International Leadership

The CDC is actively promoting U.S. leadership in the development of an international partnership to address emerging infectious diseases. This leadership role is a natural one for the United States since American business leaders and scientists are in the forefront of the computer communications and biomedical research communities that must provide the technical and scientific underpinning for disease surveillance. The United States maintains more medical facilities and personnel abroad than any other country, in terms of both civilian and military, and public and private sector institutions. Furthermore, American scientists and public health professionals have been among the most important contributors to the international efforts to eradicate smallpox and polio.

Similar arguments would support U.S. leadership in the formulation of a global response to what will surely become a global IT threat.

D.1.5 References

Addressing Emerging Infectious Disease Threats: A Prevention Strategy For The United States, 1994.

Global Microbial Threats in the 1990s, 1995.

ATTACHMENT 1

CDC's Information Network for Public Health Officials (INPHO):
A Framework for Integrated Public Health Information and Practice.

Baker EL, Friede A, Moulton AD, Ross DA.

J Public Health Management Practice, 1995; 1(1):43-7.

CDC's Information Network for Public Health Officials (INPHO):

A Framework for Integrated Public Health Information and Practice

Contents

* Summary
* Vision and Goals
* Why We Need Better Communication
* (Box) INPHO: The Vision, the Need, the Basic Concepts
* Three Key Concepts
* CDC Strategies
* The INPHO Project and the Systems Approach
* References
* Footnotes
* About the Authors

Summary

To strengthen the public health infrastructure, the Centers for Disease Control and Prevention (CDC) initiated the Information Network for Public Health Officials (INPHO). CDC INPHO has three goals: (1) to make communication among public health practitioners throughout the United States easy, (2) to make information accessible, and (3) to make secure data exchange as swift and smooth as contemporary technology will allow. Based on a systems approach to supporting the core functions of public health, CDC INPHO achieves its goals by creating a flexible and user-responsive infrastructure of open communications and information exchange.

"Where is the wisdom we have lost in knowledge? Where is the knowledge we have lost in information?" *T.S. Eliot, The Rock*

Vision and Goals

The Centers for Disease Control and Prevention (CDC) initiated the Information Network for Public Health Officials (INPHO) in 1992 as part of its strategy to strengthen the infrastructure of public health in the United States. [1] The vision driving CDC INPHO is that of a new, integrated public health information system based on a state-of-the-art telecommunications network linking the public health community and providing seamless exchange of information (see the box titled, " INPHO: The Vision, the Need, the Basic Concepts "). When fully deployed, CDC INPHO will become the common pathway for public health practitioners throughout the United States--at the community, state, and national levels alike--to exchange information with each other, with CDC, and with colleagues globally. As a result, every public health worker in

the United States should be linked to every other public health worker through telecommunications technology.

CDC INPHO has three goals: (1) to make communication easy, (2) to make information accessible, and (3) to make secure data exchange as swift and smooth as contemporary technology will allow. Achieving those goals will involve a variety of activities in the states, depending on the status of their public health information strategy, telecommunications networks, end-user priorities, and other factors. Similarly, the CDC role will vary from state to state to serve the needs of their public health agencies. All INPHO activities, however, will focus on building a common public health information network linking all public health practitioners across the nation.

Why We Need Better Communication

A particularly insightful way to conceptualize the value of improved public health information comes from Harlan Cleveland, author of The Knowledge Executive: Leadership in an Information Society.[2] Cleveland makes the distinction between data, information, and knowledge. Data are undigested observations and unvarnished facts--basically the raw material of public health. Information is organized data. In public health, however, information typically is assembled not by the practitioners who are the end users but by others who are often in remote, centralized agencies. Knowledge, in turn, is the product of information the end user organizes, internalizes, and integrates with everything else she or he knows from experience, study, or intuition. Knowledge, ultimately, is the best guide to our practice of public health. What public health professionals are interested in is creating access to information that will expand our knowledge base and guide our work.

In thinking about developing an information network for public health officials, CDC focused on four critical needs (see the box):

* Connecting a fragmented system. Everyone familiar with the Institute of Medicine report on the future of public health recognizes its diagnosis that the public health system is in disarray.[3] This clearly indicates the need to take action that will [re] connect the elements of the fragmented system. One way of doing this is through telecommunications technology.
* Linking public health professionals. Many public health professionals operate in significant isolation. One way to break down isolation is by connecting public health professionals through telecommunications technology. Two examples are CDC's WONDER/PC electronic mail and forums and the national telecommunications network CDC has created as part of the Public Health Leadership Institute.
* Leading and responding to health reform. Clearly, the public health community is in the information business and specifically in the business of providing information to the communities that public health serves.

* Activating public health for the health reform environment. As health reform advances--whether legislated in Washington and the states or propelled by market forces--public health needs to ensure that its core functions continue to be performed.

INPHO: The Vision, the Need, the Basic Concepts
The Vision * An integrated telecommunications network linking the public health community and providing exchange of data and information The Need * Connecting a fragmented system * Linking public health professionals * Empowering communities with information * Leading and responding to health reform The Basic Concepts * Linkage * Information access * Data exchange

Three Key Concepts

CDC INPHO embodies three concepts key to generating the data, information, and knowledge to address the needs outlined above (see the box). Linkage is the first key concept. Here CDC is active on several fronts. CDC is working with state and local. health agencies to build local and wide-area networks--actual physical construction of networks, supported in some cases through outside resources. Second, CDC is expanding "virtual networks" through the use of CDC WONDER PC, a software system that allows public health professionals to communicate across the globe through electronic mail and that also provides unprecedented access to data and information maintained in CDC's large public health databases.[4,5] Third, CDC is emphasizing the strategy of connecting to the Internet. CDC encourages each state to identify ways to connect with the Internet and have access to the information superhighway.

In partnership with the Georgia Division of Public Health, CDC is implementing an INPHO project to electronically link all parts of the public health system--the state health agency, district health departments, and county health departments. CDC is providing those offices access to the CDC information bases and other sources of information that the state public health agency and its project partners deem valuable. CDC will work with additional states in a similar manner beginning in late 1994, emphasizing development of network capabilities and applications defined by the states themselves. CDC also is linking its information system initiatives with its

Distance Learning Program. A clear linkage exists between the INPHO concept of an information network and the notion of a public health training and distance learning network for public health professionals.

The second key concept is information access. CDC generates a large body of information that is published in various forms, but not always in the form most accessible to end users. In this respect, the CDC INPHO is focused on improving practitioners' access to existing and future CDC information bases. The principal approach is to expand the number of information bases accessible through the CDC WONDER PC system. Areas that warrant particular mention are (1.) The prevention guidelines database, (2.) The training resource directory that will enable public health professionals to identify upcoming training offered by CDC and other organizations, and (3.) On-line access to the Morbidity and Mortality Weekly Report, complete with tables and graphs.

CDC is not attempting to expand access to information exclusively through the CDC WONDER PC system. Public health professionals currently access information in many other ways and from many other sources that have great value. It is CDC's hope that its own efforts will help public health professionals maximize their use of multiple access routes so they can achieve access to the information they want as rapidly as possible.

Exchange of data and information is the third key INPHO concept. Many different types of data are involved, among them health status data, health risk information, and particularly data on health care services. As the era of health care reform advances, it will be vital for public health to have rapid, electronic access to health care services information from personal care providers. One important issue is that of automating data entry. Many health departments do not have access to automated data entry systems. Protecting personal privacy and ensuring confidentiality may be one of the most important issues of all. The structure of the data exchange system also is important. Currently, public health has many disparate data systems in place and needs to look to a more integrated approach.

As the era of health care reform advances, it will be vital for public health to have rapid, electronic access to health care services information from personal care providers.

Finally, as health care reform becomes reality, related information systems are being created. It is essential that the public health community understand the implications of those systems and ensure that they generate information to support and enhance the ongoing core functions of population-based health assessment and assurance.

David Satcher, CDC Director, has identified the obstacles public health faces in fulfilling the concept of data and information exchange:

First, public health agencies at the local, state, and federal levels have a fragmented set of public information systems that threaten to overwhelm the capacity of state and local health departments to respond to the information needs they face.

Second, there is variable access to technology. Some health departments do not have or cannot make ready use of the telecommunications technologies that the INPHO project envisions.

Third, the issue of confidentiality is significant not only as a complex policy issue but also for its symbolic, perceptual importance. The American public is legitimately concerned about issues of confidentiality. The public health community must address this concern squarely and responsively.

Fourth, public health does not have a wealth of existing integrated systems on which to model its own integrated information initiative. The lack of precedents clearly presents an obstacle but, at the same time, a professional challenge to "reinvent" public health using a "bootstraps" approach that draws on the creativity and energy characteristic of the public health profession. [6]

CDC Strategies

How is CDC confronting these obstacles? To address the problem of fragmented information systems, Martha Katz, CDC's Associate Director for Policy, Planning, and Evaluation, formed a collaborative committee in 1993 that drafted the Report on Public Health Information and Surveillance Systems. [7] The report contains a set of recommendations for action toward integrated health surveillance and information systems that was issued for review and reaction by state and local public health agencies in the spring of 1994. Initial responses were gathered during the March 1994 first annual CDC INPHO conference held in Atlanta, Georgia, and attended by public health representatives from across the nation.

CDC is also working with states to support network development and address the obstacle of variable access to contemporary technology. The Georgia INPHO project is an invaluable prototype for the nation. CDC is mobilizing funding and other resources to help other states initiate similar projects that speak to their specific needs. CDC will support "knowledge transfer" from Georgia and the succeeding INPHO states.

In 1994, CDC organized a confidentiality work group and charged it to assess the legal and technological dimensions of the issue and to develop recommendations and guidelines for protection of confidentiality in the context of integrated information and health surveillance systems.

CDC's approach to dealing with the lack of precedents has two parts. The first is to proceed with the state INPHO projects and to learn from their experience. Second, and of equal importance, is to learn from the complementary projects that a number of state and local public health agencies have underway. These projects focus directly on integrated information systems, data exchange across categorical program lines, data exchange with hospitals and managed care providers, and other issues integral to the INPHO vision. A key role that CDC can play is to disseminate to the

national public health community the innovations, successes, and lessons learned by innovative local and state projects.

The INPHO Project and the Systems Approach

A central tenet of systems thinking, as represented, for example, in the work of Peter Senge, is that today's solutions create the issues of tomorrow. [8]

This insight is germane to the CDC INPHO initiative. It cautions that the goal of INPHO should not be to increase the sheer volume of data and information available to public health professionals. Instead, it is to increase their ability to generate and access the information and knowledge they need to guard the health of the public.

Information overload, already a reality in the lives of many public health professionals, threatens to become the leading occupational disease in the 21st century. Unfocused electronic information systems are a threat, not a boon, to public health. The rainfall of electronic mail that seemingly descends on users' computers overnight is a telling symptom. Surgeon General Joycelyn Elders recently remarked that a symptom of information overload is that the quantity of information in her professional life sometimes prevents her from enjoying the work that she knows in her heart she truly values.

Confronted with the challenges of the 1990s and the 21st century, the public health community ultimately needs wisdom on which to base its decisions and choices of action. Harlan Cleveland defines wisdom as "Integrated knowledge, information made super useful by theory which relates bits and fields of knowledge to each other, which in turn enables us to use the knowledge to do something." [2 (p.23)] Only the human mind can synthesize wisdom from data and information. The vision of CDC INPHO necessarily is more modest.

The key to building successful, integrated public health information systems is to focus on a vision consistent with the core mission and core functions of the profession. CDC INPHO is based on a systems approach to supporting the core functions of public health. It does that by creating a rich, flexible, and user-responsive infrastructure of open communications and information exchange. The CDC INPHO team is developing specific, valuable software and computer/telecommunications networks. The heart of the initiative, however, is the conceptual framework it provides for truly integrated health assessment and assurance both within the public health community and in conjunction with the evolving health care sector.

REFERENCES

1. Roper, W.L. Strengthening the Public Health Infrastructure. Speech to Association of State and Territorial Health Officials. Atlanta, Ga.: Centers for Disease Control, May 1990.

2. Cleveland, H. The Knowledge Executive: Leadership in an Information Society. New York, NY: Truman Talley Books, E.P. Dutton, 1985.

3. Institute of Medicine. The Future of Public Health. Washington, D.C.: National Academy Press, 1988.

4. Friede, A., Reid, J.A., Ory, H.W. CDC WONDER: A Comprehensive Online Public Health System of the Centers for Disease Control and Prevention. American Journal of Public Health, 1993; 83:1,289-94.

5. Friede, A., Rosen D.R., Reid, J.A. CDC WONDER/PC: Cooperative Processing for Public Health Informatics. Journal of the American Medical Informatics Association, 1994; 1 :303312.

6. Address to the "First INPHO Workshop: Creating the Public Health Information Highway," Atlanta, Georgia, March 29, 1994.

7. Centers for Disease Control and Prevention. A Report on Public Health Information and Surveillance Systems. Atlanta, Ga.: CDC, 1994.

8. Senge, P.M. The Fifth Discipline: The Art and Practice of the Learning Organization. New York, N.Y.: Doubleday Currency, 1990.

Footnotes

This article is adapted from an address given by Edward L. Baker, M.D., M.P.H., Director, Public Health Practice Program Office, Centers for Disease Control and Prevention, at the "First INPHO Workshop: Creating the Public Health Information Highway," in Atlanta, Georgia, March 29, 1994.

The authors wish to acknowledge the contributions made by a number of parties at the Centers for Disease Control and Prevention (CDC), universities, and public health agencies. The concepts, mission, and vision underlying the CDC Information Network for Public Health Officials (INPHO) have been shaped by members of the CDC INPHO lead team. They are Mr. James Seligman, Drs. Patrick O'Carroll, and Howard Ory, Information Resources Management Office; Ms. Barbara R. Holloway, Drs. Edwin Kilbourne. Donna Stroup. and Demetri Vacalis, Epidemiology Program Office; and Mr. Thomas Lacher and Mr. Wallace Wilhoite, Public Health Practice Program Office. The following members of the Georgia INPHO Project Steering Committee have also contributed in shaping our approach: Dr. Karen Chapman, Georgia Division of Public Health; Dr. Kathy Minor, Ms. Melissa Alprin, and Ms. Gail Horlick, Emory University School of Public Health; Drs. Dan Ward and Hartmut Gross, Medical College of Georgia; and Mr. Richard K. Snelling and Mr. Keith Bernhardt, Georgia Center for Advanced Telecommunications Technology. The Robert W. Woodruff Foundation has given generous support to advance the Georgia INPHO project and the national CDC INPHO initiative

This material was developed in the public domain. No copyright applies.

About the Authors

Edward L. Baker, M.D., M.P.H., serves as Director of the CDC Public Health Practice Program Office. The mission of this office is to strengthen the public health system through information systems development, distance learning, leadership development, community planning, and systems research. Prior to taking this position, Dr. Baker served as Deputy Director and Assistant Director of the National Institute for Occupational Safety and Health (NIOSH), a CDC component, from 1985 to 1990. In that capacity, he provided leadership in occupational health surveillance and in development of the OSHA standard for prevention of blood-borne disease in the workplace.

Andrew Friede, MD., M.P.H., is the Chief of the Public Health Information Systems Branch, Information Resources Management Office, Centers for Disease Control and Prevention (CDC). He joined CDC's Information Resources Management Office in 1987 where he has led a large group in development of CDC WONDER/PC, an integrated information and communications public health information system that provides access to some 40 databases for 3,000 users as well as specialized features used by many CDC surveillance programs. Dr. Friede is also a principal participant in the CDC INPHO project.

Anthony D. Moulton, Ph.D., Robert W. Woodruff Health Sciences Center, Emory University, is an assistant to the Information Network for Public Health Officials (INPHO) initiatives of the Centers for Disease Control and Prevention and the Georgia Division of Public Health.

David A. Ross, Sc.D., is Assistant Director for Information and Communication Services in the Public Health Practice Program Office, CDC. Dr. Ross is directing the CDC Information Network for Public Health Officials (CDC INPHO) program.

D.2 FEDERAL EMERGENCY MANAGEMENT AGENCY FEDERAL RESPONSE PLAN ORGANIZATIONAL MODEL

FEMA Experience:
Applicability To The
National Center For Information Systems Security Assurance

D.2.1 Background

FEMA is an independent federal agency with more than 2,600 full time employees: at FEMA headquarters in Washington D.C., at regional and area offices across the country, at the Mount Weather Emergency Assistance Center, and at the FEMA training center in Emmitsburg, Maryland. FEMA also has nearly 4,000 standby disaster assistance employees who are available to help out after disasters. Often FEMA works in partnership with other organizations that are part of the nation's emergency management system. These partners include state and local emergency management agencies, 27 federal agencies and American Red Cross.

FEMA's Mission is to provide leadership and support to reduce the loss of life and property and protect our nation's institutions from all types of hazards through a comprehensive, risk-based, all-hazards emergency management program of mitigation, preparedness, response and recovery.

FEMA accomplishes its mission through a very broad range of activities, including:

- helping equip local and state emergency preparedness...
- coordinating the federal response to a disaster...
- making disaster assistance available to states, communities, businesses and individuals...
- advising on building codes and flood plain management...
- teaching people how to get through a disaster...
- training emergency managers...supporting the nation's fire service...
- administering the national flood and crime insurance programs...

In particular, FEMA fully or partially funds emergency management programs and staff in all 56 states and territories, and helps design and equip emergency operations in thousands of localities. An important objective of this assistance is effective preparedness through planning. Emergency Operations Plans are updated periodically and submitted to FEMA for review.

D.2.2 Concept of Operations

The Federal Emergency Management Agency's Federal Response Plan (for Public Law 93-288, as amended) describes FEMA's Concept of Operations to address the consequences of any disaster or emergency situation in which there is a need for Federal response assistance under the authorities of the Stafford Act. It is applicable to natural disasters; technological emergencies

involving radiological or hazardous material releases; and other incidents requiring Federal assistance under the Act.

The Response Plan describes the basic mechanisms and structures by which the Federal government will mobilize resources and conduct activities to augment State and local response efforts. To facilitate the provision of Federal assistance, the Plan uses a functional approach to group the types of Federal assistance which a State is most likely to need under twelve Emergency Support Functions (ESFs). Each ESF is headed by a primary agency, which has been selected based on its authorities, resources and capabilities in the particular functional area. Other agencies have been designated as support agencies for one or more ESF based on their resources and capabilities to support the functional area. The twelve ESFs serve as the primary mechanism through which Federal response assistance will be provided to assist the State in meeting response requirements in an affected area. Federal assistance will be provided to the affected State under the overall coordination of the Federal Coordinating Officer (FCO) appointed by the Director of FEMA on behalf of the President.

Federal assistance provided under P.L. 93-288, as amended, is to supplement State and local government response efforts. ESFs will coordinate with the FCO and the affected State to identify specific response requirements and will provide Federal response assistance based on State-identified priorities.

Each ESF will provide resources using its primary and support agency authorities and capabilities, in coordination with other ESFs, to support its missions. ESFs will allocate available resources to each declared State based on priorities identified in conjunction with the State and in coordination with the FCO. If resources are not available within the declared State, the ESF will seek to provide them from a primary or support agency area or region. If the resource is unavailable from an area or region, the requirement will be forwarded to the appropriate ESF headquarters office for further action.

One or more disasters may affect a number of States and regions concurrently. In those instances, the Federal government will conduct multi-State response operations; for each declared State, an FCO will be appointed to coordinate the specific requirements for Federal response and recovery within that State. Under multiple State declarations, ESF departments and agencies will be required to coordinate the provision of resources to support the operations of all of the declared States.

D.2.3 Legislative History/Authorities

In 1988, Public Law 93-288 was amended by Public Law 100-707 and retitled as the Robert T. Stafford Disaster Relief and Emergency Assistance Act (Public Law 93-288, as amended). The Stafford Act provides the authority for the Federal government to respond to disasters and emergencies in order to provide assistance to save lives and protect public health, safety, and property.

In providing response assistance under the Federal Response Plan, Federal departments and agencies are covered under the authorities of P.L. 93- 288, as amended. Under P.L. 93-288, the President may direct any Federal agency to utilize its authorities and resources in support of State and local assistance efforts. This authority has been further delegated to the Director, FEMA, the Associate Director, State and Local Programs and Support (SLPS), and to the FEMA Regional Directors in carrying out the provisions of the Stafford Act.

Response by departments and agencies to lifesaving and life protecting requirements under the Plan has precedence over other Federal response activities, except where national security implications are determined to be of a higher priority. Support from departments and agencies will be provided to the extent that it does not conflict with other emergency

D.2.4 Relationships with Other Government Agencies

General Information

Numerous federal agencies and departments are partners in the nation's emergency management system. In planning, they participate in training exercises and conduct a variety of activities to help the nation prepare for disasters. For example, the Federal Communications Commission and the Commerce Department's National Weather Service provide on-going warning and disaster tracking services. In a catastrophic disaster, FEMA coordinates the federal response, working with 27 federal partners and the American Red Cross to provide emergency food and water, medical supplies and services, search and rescue operations, transportation assistance, environmental assessment, and more. The National Disaster Medical System is a partnership set up to provide emergency medical services in a disaster, involving FEMA, the Department of Health and Human Services, the Department of Defense, the Veterans Administration, as well as public and private hospitals across the country.

- National emergency management organizations. Emergency preparedness and response requires the efforts of many people. FEMA works in partnership with national organizations dedicated to assisting the public in preparation for and response to a disaster. FEMA supports the efforts of the National Emergency Management Association (NEMA), whose membership includes state emergency managers, and the National Coordinating Council on Emergency Management (NCCEM), whose membership includes local emergency managers.

- State emergency management departments. When a disaster overwhelms local resources, the task of coordinating response moves to the next level -- the state. States take a leading role in response to any large-scale disaster, even those so major that federal assistance is requested. FEMA supports the state emergency management in many ways, from funding state planning to working directly with state agencies to managing a large-scale response.

- Local emergency management agencies. Local emergency management programs are the heart of the nation's emergency management system. FEMA supports them with funding for emergency planning and equipment, by offering training courses for emergency

managers and firefighters, by conducting exercises for localities to practice their response, and by promoting ways to minimize disasters' effects. FEMA also builds partnerships with mayors, county boards and other elected and appointed officials who share responsibility for emergency management.

- Partnerships with the private sector. Disaster requires the full resources of a community to help people respond and recover. FEMA encourages all sectors of society -- from business and industry to volunteer organizations -- to work together in disaster preparation, response and recovery. FEMA assists in coordinating activities of a variety of players, including private contractors, hospitals, volunteer organizations and area businesses. It is through these partnerships of people working together that communities are able to put the pieces back together.

Relationships with Other U.S. Government Agencies

The Federal Emergency Management Agency's Federal Response Plan provides standing mission assignments to the designated departments and agencies with primary and support responsibilities to carry out Emergency Support Functions (ESFs). Federal departments and agencies designated as primary agencies serve as Federal executive agents under the FCO in accomplishing the ESF response missions. Upon activation of an ESF, a primary agency is authorized, in coordination with the Federal Coordinating Officer (FCO) and the State, to initiate and continue actions to carry out the ESF missions described in the ESF Annexes to the Plan, including tasking of designated support agencies to carry out assigned ESF missions.

At the national level, primary agencies are responsible to plan and coordinate with their support agencies for the delivery of ESF-related assistance. Primary agencies are responsible for preparing and maintaining the ESF annexes and appendices to the Plan to reflect the policies, procedures regarding assistance to be provided, and associated responsibilities of the designated primary and support agencies.

Support agencies will assist the primary agencies in preparing and maintaining ESF annexes and appendices, developing national and regional operating procedures, and providing support for ESF operations.

EMERGENCY SUPPORT FUNCTION #1: TRANSPORTATION

The purpose of this Emergency Support Function (ESF) is to provide for the coordination of Federal transportation support to State and local governmental entities, voluntary organizations, and Federal agencies requiring transportation capacity to perform disaster assistance missions following a catastrophic earthquake, significant natural disaster, or other event requiring Federal response.

PRIMARY AGENCY: Department of Transportation

SUPPORT AGENCIES:

- Department of Agriculture
- Department of Defense
- Department of Energy
- Department of State
- General Services Administration
- Interstate Commerce Commission
- Tennessee Valley Authority
- Postal Service

EMERGENCY SUPPORT FUNCTION #2: COMMUNICATIONS

The purpose of this Emergency Support Function (ESF) is to assure the provision of Federal telecommunications support to Federal, State, and local response efforts following a Presidentially declared emergency, major disaster, extraordinary situation and other emergencies under the Federal Response Plan. This ESF supplements the provisions of the National Plan for Telecommunications Support in Non-Wartime Emergencies, hereafter referred to as the National Telecommunications Support Plan (NTSP).

PRIMARY AGENCY: National Communications System

SUPPORT AGENCIES:

- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of the Interior
- Department of Transportation
- Federal Communications
- Commission
- Federal Emergency Management
- Agency
- General Services Administration

EMERGENCY SUPPORT FUNCTION #3: PUBLIC WORKS AND ENGINEERING

The purpose of this Emergency Support Function (ESF) is to provide Public Works and Engineering support to assist the State(s) in needs related to lifesaving or life protecting following a major or catastrophic disaster.

PRIMARY AGENCY: Department of Defense; U.S. Army Corps of Engineers

SUPPORT AGENCIES:

- Department of Agriculture
- Department of Commerce

- Department of Energy
- Department of Health and Human Services
- Department of the Interior
- Department of Labor
- Department of Transportation
- Department of Veterans Affairs
- Environmental Protection Agency
- General Services Administration
- Tennessee Valley Authority

EMERGENCY SUPPORT FUNCTION #4: FIREFIGHTING

The purpose of this Emergency Support Function (ESF) is to detect and suppress wildland, rural, and urban fires resulting from, or occurring coincidentally with, a catastrophic earthquake, significant natural disaster or other event requiring Federal response assistance.

PRIMARY AGENCY: Department of Agriculture; Forest Service

SUPPORT AGENCIES:

- Department of Commerce
- Department of Defense
- Department of the Interior
- Environmental Protection Agency
- Federal Emergency Management Agency

EMERGENCY SUPPORT FUNCTION #5: INFORMATION AND PLANNING

Information and Planning: collect, process and disseminate information about a potential or actual disaster or emergency to facilitate the overall activities of the Federal government in providing response assistance to an affected State.

PRIMARY AGENCY: Federal Emergency Management Agency

SUPPORT AGENCIES:

- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Education
- Department of Energy
- Department of Health and Human Services
- Department of the Interior
- Department of Justice
- Department of Transportation
- Department of the Treasury

- American Red Cross
- Environmental Protection Agency
- General Services Administration
- National Aeronautics and Space
- Administration
- National Communications System
- Nuclear Regulatory Commission

EMERGENCY SUPPORT FUNCTION #6: MASS CARE

The purpose of this Emergency Support Function (ESF) is to coordinate efforts to provide sheltering, feeding, and emergency first aid following a catastrophic earthquake, significant natural disaster or other event requiring Federal response assistance; to operate a Disaster Welfare Information (DWI) System to collect, receive, and report information about the status of victims and assist with family reunification supplies to disaster victims following a disaster.

PRIMARY AGENCY: American Red Cross

SUPPORT AGENCIES:

- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Health and Human Services
- Department of Housing and Urban Development
- Department of Transportation
- Department of Veterans Affairs
- Federal Emergency Management Agency
- General Services Administration
- Postal Service

EMERGENCY SUPPORT FUNCTION #7: RESOURCE SUPPORT

The purpose of this Emergency Support Function (ESF) is to provide logistical/resource support following a catastrophic earthquake, other significant natural disaster or other event requiring Federal response.

PRIMARY AGENCY: General Services Administration

SUPPORT AGENCIES:

- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Energy
- Department of Health and Human Services

- Department of Labor
- Department of Transportation
- Department of Veterans Affairs
- Federal Emergency Management Agency
- National Communications System
- Office of Personnel Management

EMERGENCY SUPPORT FUNCTION #8: HEALTH AND MEDICAL SERVICES

The purpose of this Emergency Support Function (ESF) is to provide United States Government coordinated assistance to supplement State and local resources in response to public health and medical care needs following a significant natural disaster or man-made event. Assistance provided under ESF #8 - Health and Medical Services, is directed by the Department of Health and Human Services (HHS) through its Executive Agent, the Assistant Secretary for Health (ASH), who heads the United States Public Health Service (PHS). Resources will be furnished when State and local resources are overwhelmed and medical and/or public health assistance is requested from the Federal Government.

PRIMARY AGENCY: Department of Health and Human Services; U.S. Public Health Service

SUPPORT AGENCIES:

- Department of Agriculture
- Department of Defense
- Department of Justice
- Department of Transportation
- Department of Veterans Affairs
- Agency for International Development
- American Red Cross
- Environmental Protection Agency
- Federal Emergency Management Agency
- General Services Administration
- National Communications System
- Postal Service

EMERGENCY SUPPORT FUNCTION #9: URBAN SEARCH AND RESCUE

The purpose of this Emergency Support Function (ESF) is to describe the use of Federal Urban Search and Rescue (US&R) assets following an event requiring a Federal response, including locating, extricating and providing for the immediate medical treatment of victims trapped in collapsed structures.

PRIMARY AGENCY: Department of Defense

SUPPORT AGENCIES:

- Department of Agriculture
- Department of Health and Human Services
- Department of Labor
- Department of Transportation
- Agency for International Development
- Environmental Protection Agency
- Federal Emergency Management Agency
- General Services Administration

EMERGENCY SUPPORT FUNCTION #10: HAZARDOUS MATERIALS

The purpose of this Emergency Support Function (ESF) is to provide Federal support to State and local governments in response to an actual or potential discharge and/or release of hazardous materials following a catastrophic earthquake or other catastrophic disaster.

PRIMARY AGENCY: Environmental Protection Agency

SUPPORT AGENCIES:
- Department of Agriculture
- Department of Commerce
- Department of Defense
- Department of Energy
- Department of Health and Human Services
- Department of the Interior
- Department of Justice
- Department of Labor
- Department of State
- Department of Transportation
- Federal Emergency Management Agency
- General Services Administration
- Nuclear Regulatory Commission

EMERGENCY SUPPORT FUNCTION #11: FOOD

The purpose of this Emergency Support Function (ESF) is to identify, secure, and arrange for the transportation of food assistance to affected areas following a major disaster or emergency or other event requiring Federal response.

PRIMARY AGENCY: Department of Agriculture

SUPPORT AGENCIES:
- Department of Defense
- Department of Health and Human Services
- Department of Transportation

- American Red Cross
- Environmental Protection Agency
- Federal Emergency Management Agency

EMERGENCY SUPPORT FUNCTION #12: ENERGY

The purpose of this Emergency Support Function (ESF) is to facilitate restoration of the Nation's energy systems following a catastrophic earthquake, natural disaster, or other significant event requiring Federal response assistance. Power and fuel are critical to save lives and protect health, safety, and property, as well as carry out other emergency response functions.

PRIMARY AGENCY: Department of Energy

SUPPORT AGENCIES:

- Department of Agriculture
- Department of Defense
- Department of State
- Department of Transportation
- General Services Administration
- National Communications System
- Nuclear Regulatory Commission
- Tennessee Valley Authority

ATTACHMENT 1

COMPENDIUM OF EMERGENCY AUTHORITIES AND DIRECTIVES

PUBLIC LAW 78-410, "PUBLIC HEALTH SERVICE ACT," SECTION 216, 42 U.S.C. 217 ---

This provision authorizes the President, in time of war or upon Presidential declaration of an emergency, to utilize the Public Health Service to the extent and in the manner that in his judgment will promote the public interest.

PUBLIC LAW 78-410, "PUBLIC HEALTH SERVICE ACT," SECTION 311 U.S.C. 243 ---

This provision authorizes the Secretary of Health and Human Services to develop (and may take such action as may be necessary to implement) a plan under which personnel, equipment, medical services, and other resources of the Public Health Service and other agencies under the jurisdiction of the Secretary may be effectively used to control epidemics of any disease or condition, as specified, and to meet other health emergencies or problems involving or resulting from disasters or any such disease.

PUBLIC LAW 78-410, "DEFENSE HEALTH SERVICE ACT," SECTION 319 ---

This provision authorizes the Secretary of Health and Human Services to take appropriate action to respond to a "public health emergency" resulting from disease, disorder, or other cause. The Secretary must consult with the Director of the National Institute of Health, Administrator of the Alcohol, Drug Abuse, and Mental Health Administration, Commissioner of the Food and Drug Administration, or the Director of the Center, for Disease Control before determining that an emergency exists, and he must act through that official in responding to the emergency.

PUBLIC LAW 81-774, "DEFENSE PRODUCTION ACT OF 1950, AS AMENDED," 50 U.S.C. 2061, TITLE I, SECTION 101(a) AND 101(b) ---

This provision authorizes the President to establish performance priorities and to allocate materials and facilities to promote the national defense.

PUBLIC LAW 93-288, AS AMENDED BY PUBLIC LAW 100-707, "ROBERT T. STAFFORD DISASTER RELIEF AND EMERGENCY ASSISTANCE ACT," NOVEMBER 23, 1988 ---

The Robert T. Stafford Disaster Relief and Emergency Assistance Act, P.L. 93-288 as amended, provides an orderly and continuing means of assistance by the Federal Government to State and local governments in carrying out their responsibilities to alleviate the suffering and damage which result from disasters. The President, in response to a State Governor's request, may declare an "emergency" or "major disaster," in order to provide Federal assistance under the Act.

The President, in Executive Order 12148, delegated all functions, except those in Section 301, 401, and 409, to the Director, Federal Emergency Management Agency (FEMA). The Act provides for the appointment of a Federal Coordinating Officer who will operate in the designated area with a State Coordinating Officer for the purpose of coordinating state and local disaster assistance efforts with those of the Federal Government.

PUBLIC LAW 95-124, "EARTHQUAKE HAZARDS REDUCTION ACT OF 1977," 42 U.S.C. 7701 AND 7704 ---

The Earthquake Hazards Reduction Act of 1977, as amended by P.L. 96-472 and P.L. 99-105, provides for the establishment of the National Earthquake Hazards Reduction Program (NEHRP) to reduce the risk to life and property from future earthquakes in the United States. FEMA is designated as the agency with primary responsibilities to plan and coordinate the NEHRP, which has five major elements: Hazard Delineation and Assessment; Earthquake Prediction Research; Seismic Design and Engineering Research; Preparedness Planning and Hazard Awareness; and, Fundamental Seismological Studies. Planning for the Federal response to a catastrophic earthquake is a major aspect of Preparedness Planning and Hazard Awareness under the NEHRP.

PUBLIC LAW 95-313, "COOPERATIVE FORESTRY ASSISTANCE ACT OF 1978" ---

This Act authorizes the Secretary of Agriculture to assist in the prevention and control of rural fires through coordination among Federal, State, and local agencies; and to provide prompt and adequate assistance whenever a rural fire emergency overwhelms, or threatens to overwhelm, the firefighting capability of the affected State or rural area.

PUBLIC LAW 96-510, "COMPREHENSIVE ENVIRONMENTAL RESPONSE, COMPENSATION, AND LIABILITY ACT OF 1980," SECTION 104(i), 42 U.S.C. 9604(i) ---

More popularly known as "Superfund", CERCLA was passed to provide the needed general authority for Federal and State governments to respond directly to hazardous substances incidents.

PUBLIC LAW 101-640, "WATER RESOURCES DEVELOPMENT ACT OF 1990," TITLE III, SECTION 302, 5(A)(1), NOVEMBER 28,1990 ---

This Act amends 33 U.S.C. 701n)a)(1) by replacing the term "flood emergency preparation" to include "preparation for emergency response to any disaster" and includes a provision that "The emergency fund may be expended for emergency dredging for restoration of authorized projects for Federal navigable channels and waterways made necessary by flood, drought, earthquake, or other natural disasters."

UNITED STATES CONGRESS ACT OF JANUARY 5, 1905, AS AMENDED, 36 U.S.C. ---

The American National Red Cross Congressional Charter assigning the authority and responsibility for the American Red Cross to undertake activities for the relief of individuals suffering from a disaster.

COMMUNICATIONS ACT OF 1934, AS AMENDED ---

This Act gives the Federal Communications Commission emergency authority to grant Special Temporary Authority on an expedited basis to operate radio frequency devices.

OLDER AMERICANS ACT OF 1965, AS AMENDED, SECTION 310, 42 U.S.C. 3030 - --

This provision authorizes the Commissioner of the Administration on Aging to reimburse States for social services provided to older Americans following a Presidentially- declared disaster.

FOOD STAMP ACT OF 1977, SECTION 5(h)(1), IMPLEMENTED BY PROPOSED FINAL RULEMAKING AT 46 CFR 8922 AND 46 CFR 8923 ---

Authorizes the Department of Agriculture to make food stamps available to low income households in any disaster situation in which normal channels of retail food distribution have been restored and the existing Food Stamp Program cannot handle applications from affected households. Food stamp assistance must be requested by a State.

INTERSTATE COMMERCE ACT, EMERGENCY RATES, 49 U.S.C. 10724 AND 11121 TO 11128 ---

These authorities allow the Interstate Commerce Commission (ICC) to authorize a common carrier to give reduced rates for service and transportation in an emergency. Further, these authorities permit the ICC to suspend any car service rule or practice, take action during emergencies to promote car service in the interest of the public and commerce; to require joint or common use of facilities when that action will best meet the emergency; to direct preferences or priorities in transportation, embargoes, or movement of traffic under permits; and to reroute traffic.

"ROBERT T. STAFFORD DISASTER RELIEF AND EMERGENCY ASSISTANCE ACT (P.L. 93-288, AS AMENDED)," IMPLEMENTED BY FOOD DISTRIBUTION REGULATIONS, PARTS 250.1(b) AND 250.8(e) ---

These provisions allow any person/household temporarily displaced by a disaster to obtain USDA foods in congregate feeding provided by volunteer organizations such as the American Red Cross and the Salvation Army; no formal approval is required from USDA. Additionally, low income families can receive household distributions of food in situations where a Food Stamp Program is not available (e.g., commercial channels of trade are disrupted); formal USDA approval is required.

EXECUTIVE ORDER 10480, AS AMENDED, "FURTHER PROVIDING FOR THE ADMINISTRATION OF THE DEFENSE MOBILIZATION PROGRAM," AUGUST 14, 1953 --

Part II of the Order delegates to the Director, FEMA, with authority to redelegate, the priorities and allocation functions conferred on the President by Title I of the Defense Production Act of 1950, as amended.

EXECUTIVE ORDER 12148, "FEDERAL EMERGENCY MANAGEMENT," JULY 20, 1979 ---

Executive Order 12148 transferred functions and responsibilities associated with Federal emergency management to the Director, FEMA. Assigns the Director, FEMA, the responsibility to establish Federal policies for and to coordinate all civil defense and civil emergency planning, management, mitigation, and assistance functions of Executive Agencies.

EXECUTIVE ORDER 12472, "ASSIGNMENT OF NATIONAL SECURITY AND EMERGENCY PREPAREDNESS TELECOMMUNICATIONS FUNCTIONS," APRIL 3, 1984 ---

Executive Order 12472 establishes the National Communications System (NCS). The NCS consists of the telecommunications assets of the entities represented on the NCS Committee of Principals and an administrative structure consisting of the Executive Agent, the NCS Committee of Principals, and the Manager. The NCS Committee of Principals consists of representatives from those Federal departments, agencies, or entities, designated by the President, which lease or own telecommunications facilities or services of significance to national security or emergency preparedness.

EXECUTIVE ORDER 12656, "ASSIGNMENT OF EMERGENCY PREPAREDNESS RESPONSIBILITIES," November 18, 1988 ---

Assigns emergency preparedness responsibilities to Federal departments and agencies.

EXECUTIVE ORDER 12657, "FEMA ASSISTANCE IN EMERGENCY PREPAREDNESS PLANNING AT COMMERCIAL NUCLEAR POWER PLANTS," November 18, 1988 ---

Assigns FEMA and other Federal agencies certain emergency planning responsibilities related to commercial nuclear power plants.

EXECUTIVE ORDER 12777, "IMPLEMENTATION OF SECTION 311 OF THE FEDERAL WATER POLLUTION ACT OF OCTOBER 18, 1972, AS AMENDED, AND THE OIL POLLUTION ACT OF 1990," OCTOBER 18, 1991 ---

Refers to certain activities of the National Response Team and the Regional Response Team under the National Contingency Plan.

7 CFR, PART 250.1(B)(10)&(11) ---

Refers to Section 409 and 410 b of P.L. 93-288, as amended, Robert T. Stafford Disaster Relief and Emergency Assistance Act, which reads, "The Secretary of Agriculture shall utilize funds appropriated under Section 32 of the Act of August 1935 (7 USC 612 c) to purchase food commodities necessary to provide adequate supplies for use in any area of the United States in the event of a major disaster or emergency in such area."

28 CFR, PART 65, "EMERGENCY FEDERAL LAW ENFORCEMENT ASSISTANCE"; FINAL RULE ---

These Department of Justice regulations implement the Emergency Federal Law Enforcement Assistance functions vested in the Attorney General by the Justice Assistance Act of 1984 (Public Law 98-473). Those functions were established to assist State and/or local units of government in responding to a law enforcement emergency. The Act defines the term "law enforcement emergency" as an uncommon situation which requires law enforcement, which is or threatens to become of serious or epidemic proportions, and with respect to which State and local resources are inadequate to protect the lives and property of citizens, or to enforce the criminal law. Emergencies which are not of an ongoing or chronic nature, such as the Mount Saint Helens volcanic eruption, are eligible for Federal law enforcement assistance. Such assistance is defined as funds, equipment, training, intelligence information, and personnel. Requests for assistance must be submitted in writing to the Attorney General by the chief executive officer of a State. The Plan does not cover the provision of law enforcement assistance. Such assistance will be provided in accordance with the regulations referred to in this paragraph [28 CFR Part 65, implementing the Justice Assistance Act of 1984] or pursuant to any other applicable authority of the Department of Justice.

40 CFR PART 300, "NATIONAL OIL AND HAZARDOUS SUBSTANCES POLLUTION CONTINGENCY PLAN" (NCP) ---

The purpose of the NCP is to effectuate the powers and responsibilities for responding to nonradiological oil and hazardous substances discharges, releases, or substantial threats of releases as specified in the Comprehensive Environmental Response, Compensation and Liability Act, as amended, (CERCLA) and the authorities established by Section 311 of the Clean Water Act, as amended. The plan is required by section 105 of CERCLA, 42 U.S.C. 9605, and by section 311(c)(2) of the Clean Water Act, as amended, 33 U.S.C. 1321(c)(2).

44 CFR PART 322, AS AMENDED, "DEFENSE PRODUCTION: PRIORITIES AND ALLOCATION AUTHORITY (DMA-3)" ---

The Order delegates the functions of the Director, FEMA, under Title I of the Defense Production Act, as amended, to those offices and agencies named in Section 201 of Executive

Order 10480 with respect to the areas of responsibility designated and to the Secretary of Transportation with respect to priorities and allocations for civil transportation services.

FEDERAL COMMUNICATIONS COMMISSION REPORT AND ORDER OF AUGUST 4, 1981 ---

This order modified parts 2, 90, and 99 of the Commission Rules and Regulations to establish a disaster radio response capability for local government and State radio services.

"FEDERAL RADIOLOGICAL EMERGENCY RESPONSE PLAN" ---

This document is to be used by Federal agencies in peacetime radiological emergencies. It primarily concerns the off-site Federal response in support of State and local governments with jurisdiction for the emergency. The Federal Radiological Emergency Response Plan (FRERP) provides the Federal government's concept of operations based on specific authorities for responding to radiological emergencies, outlines Federal policies and planning assumptions that underlie this concept of operations and on which Federal agency response plans were based, and specifies authorities and responsibilities of each Federal agency that may have a significant role in such emergencies.

"NATIONAL PLAN FOR TELECOMMUNICATIONS SUPPORT IN NON-WARTIME EMERGENCIES," JANUARY 1992 ---

This plan provides guidance in planning for and providing telecommunications support for Federal agencies involved in emergencies, major disasters, and other exigencies, excluding war.
DEPARTMENT OF DEFENSE DIRECTIVE 3025.1, "MILITARY SUPPORT TO CIVIL AUTHORITIES (MSCA)," 1992 ---

This directive outlines Department of Defense (DOD) policy on assistance to the civilian sector during disasters and other emergencies. Use of DOD military resources in civil emergency relief operations will be limited to those resources not immediately required for the execution of the primary defense mission. Normally, DOD military resources will be committed as a supplement to non-DOD resources which are required to cope with the humanitarian and property protection requirement caused by the emergency. In any emergency, commanders are authorized to employ DOD resources to save lives, prevent human suffering, or mitigate great property loss. Upon declaration of a major disaster under the provisions of P.L. 93-288, as amended, the Secretary of the Army is the DOD Executive Agent, and the Director of Military Support is the action agent for civil emergency relief operations. Military personnel will be under command of and directly responsible to their military superiors and will not be used to enforce or execute civil law in violation of 18 U.S.C. 1385 except as otherwise authorized by law. Military resources shall not be procured, stockpiled, or developed solely to provide assistance to civil authorities during emergencies.

FEDERAL PREPAREDNESS CIRCULAR 8, "PUBLIC AFFAIRS IN EMERGENCIES" --

This Circular establishes the Interagency Committee on Public Affairs in Emergencies (ICPAE) to coordinate public information planning and operations for management of emergency information. The Circular was reviewed in draft by the ICPAE and will receive formal department and agency review.

AMERICAN RED CROSS DISASTER SERVICES REGULATIONS AND PROCEDURES, ARC 3003, JANUARY 1984 ---

This document details the delegation of disaster services program responsibilities to officials and units of the American Red Cross. Also defined are Red Cross administrative regulations and procedures for disaster planning, preparedness, and response.

AMERICAN NATIONAL RED CROSS MASS CARE PREPAREDNESS AND OPERATION PROCEDURES AND REGULATIONS, ARC 3031 ---

This document details the Red Cross mass care preparedness and operating regulations and procedures.

AMERICAN NATIONAL RED CROSS NATIONAL BOARD OF GOVERNORS DISASTER SERVICES POLICY STATEMENT, JULY 1, 1977 ---

This document outlines the basic policies of the American Red Cross disaster services program, and the disaster relief services to be provided by units of the American Red Cross on a uniform and nationwide basis.

STATEMENT OF UNDERSTANDING BETWEEN THE FEDERAL EMERGENCY MANAGEMENT AGENCY AND THE AMERICAN NATIONAL RED CROSS, JANUARY 22, 1982 ---

The statement of understanding between FEMA and the American National Red Cross describes major responsibilities in disaster preparedness planning and operations in the event of a war-caused national emergency or a peacetime disaster, outlines areas of mutual support and cooperation, and provides a frame of reference for similar cooperative agreements between State and local governments and the operations headquarters and chapters of the ARC.

D.3 NATIONAL DRUG INTELLIGENCE CENTER

A Quick Look at the National Drug Intelligence Center (NDIC)
for Lessons Applicable to the Formation of a
National Defensive Information Warfare Center

D.3.1 Background and Legislative History

During the cocaine epidemic of the late 1980s, U.S. public opinion demanded greater Federal Government efforts to combat a nationwide drug problem. Members of Congress and the Executive Branch both reacted with pronouncements and policy moves. In 1988, the Office of National Drug control policy (ONDCP) was created and the Defense Department was given increased responsibility for counter-narcotics support actions. As policy makers attempted to cope with the increased public interest, the dimensions and dynamics of the situation were not fully understood, partially because of the lack of strategic intelligence regarding narcotics organizations. The National Drug Control Strategy of 1989 noted:

> A comprehensive thrust against drug trafficking enterprises and organizations requires a different kind of intelligence....Greater emphasis needs to be devoted to automating this information for law enforcement purposes and analyzing it [and other data] to produce a better understanding of the structure and infrastructure of trafficking organizations and their allied enterprises.

In 1989 and early 1990, the ONDCP negotiated a constituency supporting the case for establishing a National Drug Intelligence Center (NDIC). In January 1990, the ONDCP publicly endorsed the NDIC and, in June 1990, the Administration introduced legislation to establish the organization. The NDIC outlined by ONDCP emphasized modernization of law enforcement intelligence rather than making narcotics intelligence the purview of the intelligence community as some critics had feared. The proposal envisioned the Center as a focal point for consolidating and coordinating relevant intelligence gathered by law enforcement agencies and analyzing it to develop a full understanding of the drug trafficking organizations. The processed intelligence would be distributed to Federal, State and local officials for use. NDIC would maintain computer databases, coordinate collection and tasking and assess interagency efforts. The NDIC was seen to be an interagency organization to include Treasury, State, Justice, and Defense assets. Supervision of the NDIC would be the responsibility of the Attorney General. The Intelligence Community's supporting role included foreign collection and methodological and technical assistance. The NDIC was envisioned as being a small, efficient organization in Washington, DC.

With the formal Administration proposal to create the NDIC, the field of action for forming it shifted to the Congress. The House passed the measure, but differences arose in the Senate concerning the need for and location of the Center. In the end, after significant Congressional

negotiations and compromise, the NDIC was authorized. The compromise placed the NDIC in Johnstown, Pennsylvania, made the DOD the executive authority for the project, and restricted the Justice Department role in the Center itself to participation. A summary of relevant key dates and legislation is provided in Table 1.[1]

D.3.2 Concept of Operations

The multi-agency National Drug Intelligence Center is located in Johnstown, Pennsylvania. It is organized with a Director and three Deputy Directors. The Director is a Department of Justice position. The Deputy Director for Operations is a DEA position; the Deputy Director for Administration is an FBI position; and the Deputy Director for Technology is a DOD position currently filled by DIA. The staff of approximately 300 is composed of intelligence analysts (from Federal law enforcement agencies [LEAs]), special agents (from DOJ), technical experts (from DOD), administrative support, liaison staff from other agencies, and specialized contractor support. The Center also has a small liaison office in the Washington DC area to facilitate coordination.

Generally, the Federal LEAs have stand-alone terminals at the Center which can be used to receive data released to the Center and send material to the owning agency, but cannot directly access agency network systems or databases. However, the Center has made some progress in negotiating direct access in some cases. PCs in a designated Operational Research Center allow analysts access to open source material such as Reuters, AP, and Nexis/Lexis. Desktop PCs throughout the NDIC allow analysts to exchange information among themselves via a LAN, but they are not connected outside the facility. Analysts generally focus on specific organizations as targets. They correlate and fuse information on crop production and facilities, financial practices, chemical sources, transportation and distribution assets, communications and other topics to produce strategic organizational drug intelligence (SODI) pertaining to the infrastructure of a drug trafficking organization.

The Center both responds to specific requests for intelligence products and strives to develop and maintain a strategic organizational drug intelligence database, library and index system. The Center also has a deployable document exploitation team that can assist LEAs with reviewing, cataloging, analyzing and exploiting various documents which are seized in drug raids.

Senior personnel at the Center acknowledge that rivalry among the LEAs—largely as a result of a "scoring system" that keys future funding to arrest and prosecution statistics—adversely affects the degree of information sharing and coordination that is achieved today. However, they indicate a belief in a positive trend as the mutual confidence builds from personal interaction by representatives from the different agencies.

[1] This paragraph abstracted from Executive-Legislative Relations in the Creation of the National Drug Intelligence Center, Donald J. Carey, LT., U.S. Navy, September 1991.

Table 1. A Summary of Milestones in Establishing the NDIC

1986

PL 99-570$ 1.7 Million approved for anti-drug measures.

1988

PL 11-463Defense Appropriations Bill includes $ 300 Million for narcotics interdiction.

PL 100-690$ 2.8 Billion approved for anti-drug measures; creation of Office of National Drug Control Policy with Cabinet-level "Drug Czar" position; required national drug control strategy be submitted to Congress within 180 days of confirmation; provided death penalty for traffickers.

1989

PL 101-164Authorized $ 3.18 Billion in new anti-drug funding

PL 101-231Authorized drug fighting assistance for Columbia, Bolivia and Peru

September 19891989 Drug Control Strategy released

December 1989Panama invaded, Gen. Noriega arrested on drug charges

1990

January 19901990 Drug control Strategy released

June 1990Legislation to establish NDIC sent to Congress

PL 101-511FY 1991 Defense Appropriations Act provided $ 10 Million for NDIC in Johnstown

PL 101-515Department of Justice prevented from expending funds on NDIC.

1991

February 19911991 National Drug Control Strategy released

FY 1992 Defense Appropriations Bill Provided $ 40 Million for NDIC

October 1991NDIC opened in Johnstown, PA.

D.3.3 Relationships Between NDIC and Other Government Agencies

The NDIC has the responsibility for developing technical and organizational protocols (Memoranda of Agreement) required for access to information provided by other organizations. Technical protocols specify the hardware and software interfaces to allow NDIC access to the Agencies' information. Organizational protocols, documented in memoranda of agreement, specify restrictive procedures for accessing data and assure the protection by NDIC of both data source and success as specified by the originator of the information. The other Government agencies NDIC is working to establish protocols with to preclude duplication of effort and redundancy include: Treasury, U.S. Coast Guard, Immigration and naturalization Service, Customs Service, CIA, NSA, FBI, DEA and selected DOD organizations.

D.3.4 Relationships Between NDIC and International Agencies

Currently, NDIC has no direct relationships with international agencies such as Interpol or with law enforcement agencies of other nations, although they are deemed desirable. At this time, such relationships are the closely guarded province of other Federal agencies. This situation exists regarding State and local authorities as well—such relationships are the province of the Federal law enforcement agencies.

D.3.5 Observations on Potential Lessons Learned and Pitfalls

- It is essential to develop a constituency in both the Congress and the Administration in order to establish a IW-D Center.
- A high level advocate who can articulate the need for the Center is essential.
- There are likely to be concerns regarding the integration of the intelligence community or its use in support of a IW-D Center.
- The preliminary operations concept of the Center needs to allow for Congressional compromises regarding physical location.
- Interagency sensitivities regarding information use and sharing may be nearly as strong as those of civilian organizations that may be involved in the Center.
- Funding for the Center should be as stable as possible through the formative period for establishing a capability.
- High quality "human capital" is a must.

APPENDIX E

THINK PIECES

The following discussions were a part of the Task Force deliberations and judged worthy of inclusion in the Task Force Report for reference only.

E.1 INFORMATION INFRASTRUCTURE ASSURANCE PRINCIPLES

Information assurance is a term which can be used to describe the needed IW-D capabilities (and associated protection) of an information infrastructure. Some basic definitions are needed to understand the principles:

- Availability of Service - An assured level of service, capacity, quality, timeliness, and reliability.
- Denial of Service - The opposite of availability of service.
- Information Integrity - Complete, sound, unaltered, and unimpaired information.
- Corruption of Information - The opposite of information integrity.
- Information Assurance - The availability of services and information integrity.
- Disruption - Denial of service or corruption of information resulting from a single event, cause, or source; whether direct or indirect; whether accidental, intentional, rare or common.
- Stress Level - Military situations under which the infrastructure is expected to operate. These include:
  - Peacetime (natural disasters, sabotage, equipment and service failures, unintentional acts)
  - Crisis/mobilization (terrorism, low intensity conflict, conventional war)
  - Simultaneous two-theater engagements
  - Limited nuclear war (nuclear terrorism, uncoordinated/accidental, theater nuclear)
  - Expanded nuclear (coordinated attack)
  - Post-attack (recovery and reconstitution).

In the traditional systems engineering context, availability is a function of the reliability and maintainability of the system while integrity of data is a function of the quality (or grade of service) of the system transporting the data. In addition, these measures of system performance are traditionally based on design assumptions that disruptions are random in nature (e.g., component failures, human errors, and acts of nature).

Information assurance is not just a function of the reliability, maintainability, and quality of the network or infrastructure. Information assurance addresses the capability of an infrastructure to endure a variety of disruptions ranging from natural disasters to accidents to intentional disruptions by the enemies or by insiders. For example:

- A lightning strike on a critical node in the network can cause node failure; or, an earthquake or hurricane cannot only physically disrupt the network but can also cause network congestion, another source of disruption.

- Inadvertently erasing a data base containing terrain data critically needed for a cruise missile strike can compromise a key part of an offensive strike.
- Corruption of key network management data by a network manager can cause many networks to fail.
- An enemy agent located in a safe haven can introduce viruses that can cause a network to become overloaded and ineffective or cause the entire network to break down at a critical juncture.

This perspective on disruptions poses challenges for the intelligence, operations, and training communities in defining the threat, which is essential for a reasonable articulation of information assurance principles.

There are substantial differences between designing a typical information system and designing a resilient information infrastructure capable of enduring in the face of intentional disruptions. A typical information system design assumes that all of the system components will normally operate properly, with the common failure mode being failure of individual components. A resilient information infrastructure design must be based on the assumption that only some of the components will operate properly at any point in time. A typical information system design will incorporate central control mechanisms, synchronized clocks, and other techniques to use resources efficiently. A resilient information infrastructure design must be based on some decentralization of control and independent operation of portions of the infrastructure. Information system design is typically based on efficiency while a resilient information infrastructure design must be based on effectiveness. For example, the entire field of fault tolerant computing is based on the introduction of redundancy into otherwise efficient systems in order to make them more effective, particularly against random disruptions. Similarly, the design of a resilient infrastructure will assure diversity of hardware and software so that a common failure mode will not result in an infrastructure failure.

In the context of information assurance, network operation, management, and maintenance should be viewed from a war fighting perspective. Personnel performing these functions (and users in some cases), should be able to detect, differentiate among, warn of, respond to, and recover from disruptions. Recovery from disruptions resulting from failures or attacks might involve repair, reconstitution, or the employment of reserve assets. In some cases, network managers may have to isolate portions of the network to preclude the spread of disruption. Given the speed with which disruptions can propagate through networks, these capabilities may need to be available in automated form within the network itself. Finally, there must be some means to manage and control these capabilities.

The underlying philosophy in information assurance and in satisfying the IW-D need must be that of risk management and not of risk avoidance. There are not enough resources to armor plate the infrastructure. Risk management suggests that the threat be defined, that measures be undertaken to reduce the realization of the threat, that countermeasures to threat occurrence be based on realistic application of resources and that response to and recovery from threat occurrences be

part of the infrastructure. Finally, it will be necessary to assume some degree of risk while maintaining some minimum infrastructure operating capability.

Based on a review of existing documentation, a list of information assurance principles has been developed and is presented below. Because the infrastructure and the concept of information assurance are still under development, the list is not exhaustive.

The following operational information is required from CJCS and the Commanders-in-Chief (CINCs) of the Unified and Specified (U&S) Commands to quantify some of the principles:

- Information Transfer Priorities - Priorities for the transfer of voice, data, imagery, and video information based on a process developed by the JCS and based on the existing process used to establish priorities for voice and messages.
- Minimum Operating Capability - The minimum set of fixed and deployed capabilities required for each stress level, based on operations tempo and forces supported.
- Normal Operating Capability - A specified set of fixed and deployed capabilities required for peacetime and crisis/mobilization stress levels, based on operations tempo and forces supported. (In coordination with CJCS and the CINCs, DISA will, in its role as the central manager of the DII, specify this set.)
- Expected Disruptions - The expected level of disruptions to be sustained over time at each stress level. (This is normally based on intelligence estimates of enemy capabilities, insider threats, natural disasters, and other anticipated causes.)
- Minimum Assured Resiliency - The capability to sustain a specified number of simultaneous, worst-case disruptions at each stress level while still maintaining the Minimum Operating Capability.
- Desired Resiliency - The capability to sustain Expected Disruptions while maintaining a Normal Operating Capability. (In coordination with CJCS and the CINCs, DISA will, in its role as the central manager of the DII, specify this set.)

Information Assurance Principles:

- The infrastructure shall be considered a potential battlefield.
- The infrastructure shall provide Minimum Resiliency.
- The infrastructure shall detect substantial disruption, differentiate accidental disruption from intentional disruption, provide ample warning of disruption, respond to and recover from disruption, and be repairable at a rate sufficient to sustain Minimum Operating Capability under Expected Disruptions.
- The infrastructure shall detect large classes of event sequences that are likely or anticipated to lead to disruption and provide mechanisms so that disruptions from these events are:

- Prevented when possible within cost constraints
- Limited in the extent of their effect when prevention is not feasible
- Responded to prior to actual disruption when detected in time
- Traced to their source whenever possible within cost constraints.

- The infrastructure network and system control functions shall be designed to operate without dependence on the normal operation of the network or processes being controlled.
- The infrastructure responses to disruption shall be prioritized and shall take into account factors such as time, value, criticality, and locality as related to the information being transported.
- Changes to the infrastructure shall be analyzed and simulated prior to implementation to ensure that the infrastructure maintains assurance attributes during and after these changes.
- The infrastructure operations, management, and maintenance personnel and information assurance capabilities shall be regularly tested under realistic conditions to ensure that they perform and operate properly. Prior to testing, proposed tests must be simulated to assess expected behavior and ensure that the tests do not unduly degrade the infrastructure. After testing, expected and actual behavior must be reconciled and addressed.
- The infrastructure shall be designed to be flexible with respect to information assurance attributes so that as requirements, technologies, and processes are altered over time, the infrastructure will retain the Desired Resiliency specified by DISA.
- The infrastructure shall be capable of retaining the Desired Resiliency during infrastructure expansion, contraction, modification, and connection to combined forces infrastructures.
- New infrastructure components shall be designed such that:
  - If they are disrupted, they do not react so as to disrupt neighboring components
  - Disrupted neighboring components do not disrupt the new component regardless of the neighboring component's behavior
  - Disrupted components are quarantined until they return to normal operating behavior
  - Network and system management services are notified of disruptions and quarantines.
- Techniques for limiting the spread of disruptions (e.g., firewalls) shall be used where applicable, particularly in the design of network protocols and in gateways between networks.
- The infrastructure training and readiness programs shall be designed to ensure that personnel tasked with operating, managing, and maintaining the infrastructure are prepared for operations under stress, and that ample personnel and resources are

available to operate and sustain the infrastructure at the Minimum Operating Capability during Expected Disruptions.

- Sufficient inventory of and/or manufacturing capability for parts, equipment, tools, supplies, and support systems shall be maintained to enable operation, repair, and reconstitution of the infrastructure under all stress levels.
- The infrastructure users shall be licensed to operate on the information highway. Licensing procedures shall include knowledge of the network, rules of the road, information assurance, and incident response processes and capabilities.

The goal in postulating these information assurance principles is to eventually outline a set of specifications (on the order of A-Level specifications) that will shape the design and integration of the infrastructure or that can be used as a part of the specifications for the acquisition of services from the local and long-distance carriers and from information processing vendors. In order to bridge the gap between the information assurance principles and a set of specifications, it will be necessary to develop strategies for providing the attributes. Some elements that might be considered in developing those strategies include:

- Capacity
- Diversity
- Co-location of network components at hardened subscriber sites
- Provision of uninterruptable power to selected sites
- Selected redundancy in network components
- Use of diverse transmission media
- Redundant network access links for key subscribers
- Precedence (priority) mechanisms
- Congestion control mechanisms
- Transportable reserve assets for reconstitution of damaged portions of the network
- Infrastructure restoration and reconstitution
- Multiple inter-network gateways
- Personal reliability program for network managers
- End-to-end network control (that does not depend on the network to operate)
- Scalable infrastructure components
- Repairability.

Successful implementation of information assurance will require a multi-disciplinary team capable of formulating a comprehensive set of requirements, knowledgeable of current and emerging technologies, capable of overseeing the design of the infrastructure from an information assurance perspective, and capable of managing the implementation of information assurance in the infrastructure.

E.2 "Raise the Bar" Exercise

The goal is to maximally improve DoD's information assurance as quickly as possible but "do it on the cheap" without involving unnecessarily complex technology, and without awaiting the outcome of R&D efforts now underway or that could be imagined.

It can be played two ways:

1. Assume that a given pot of money is available, take as a goal maximizing the protection of DoD information assets and internal systems soonest (i.e., little or no R&D), and decide how and on what to spend it.

2. As above in item [1] except first compile a reasonable list of actions to be taken, and then estimate the cost to do them.

Below are some options from which to select, but not a comprehensive or complete list by any means. The sequence in the list is happenstance.

1. Provide users of the most sensitive systems commercially available tokens of some sort to improve the user identification/ authentication act of logging on; e.g., SecurID cards.

2. The same as item [1] except do it for all users in an operational entity; e.g., the command-control chain, tactical logistics, forward air bases.

3. Increase the level of effort in the USAF program (briefed to us) by a factor of 3 to get it done sooner. Alternately, pick a different factor of speedup.

4. Examine the other military services to ascertain whether corresponding programs would be effective for them, or whether variations on the USAF approach would be more sensible.

5. Implement [4] with a projected time-to-complete of X years.

6. Industrial organizations who have had serious intrusions into their systems and who appreciate the importance of protecting against them have mounted massive internal programs to make every employee aware of the issue, of individual responsibility, and of the actions being taken by the organization. Notable among such examples is Citibank.

Mount an intensive all-hands awareness program of information assurance in some/all/each of the military services. Alternately, confine the program to those organizational entities that are "closest" to the information assets and in best position to take appropriate steps if informed.

7. Survey all installed info-systems in the military structure that are based on COTS software and/or hardware. Compile a corresponding list of the known security flaws and fixes for each of them, and institute an aggressive effort to make sure that all such fixes are properly installed,

tested, and made operational in (say) 18 months, and that the relevant operational staffs are also well informed and trained.

8. Make the recently published NIST Handbook of computer security required reading for all personnel associated with the operations, maintenance, installation, design, procurement and upgrade of both hardware and software in key [or: all] information systems [Alternate: do this initially for all information systems based on COTS; but later, add the embedded systems as well].

Make this handbook also required reading for every training or educational course given to military personnel.

9. Survey all acquisitions of information systems and computer-containing weapon systems now underway and take such steps as necessary to guarantee that up-front design consideration has been given to information assurance, netsec, infosec and opsec.

10. Compile an inventory of all weapon systems that contain embedded computers and for each, define and characterize the line of responsibility, organization(s) and physical locations which support the deployed system. Hence, identify vulnerabilities and weak spots that might be exploited by an opponent; create plans to remedy these risks on a quick response basis.

11. Survey all deployed weapon systems that are computer-based with especial attention to all phases of maintenance and upgrades of software and hardware and to daily operations. The object is to identify places and means by which subversive actions could be taken to degrade or perturb weapon performance. The level of effort might be such that candidates for this examination will need to be ranked in order of importance and operational vulnerability.

12. As in item [11] but do for all support systems, whether CONUS or field deployed, that are not COTS-based but use specialized software and/or hardware.

13. As in [12] but for COTS-based systems.

14. Reconsider any/all of the prior suggestions from the point of view of likely geographic, cultural and infrastructure circumstances in which U.S. military forces might have to operate in the next (say) decade; e.g., SWA, Adriatic theater, mid-East, Korea. Object: to judge whether a different prioritization of effort would be suggested or warranted.

15. Begin an assessment of the civilian-infrastructure aspect of the issue; e.g., identify the military bases essential for an OCONUS deployment and do so for several different durations of engagement (e.g., weeks, months, years). Identify for each the present arrangements for provision of electrical power, of other energy sources, of communications -- especially telephone and PSN-based, and of off-base medical, personnel, or commissary requirements.

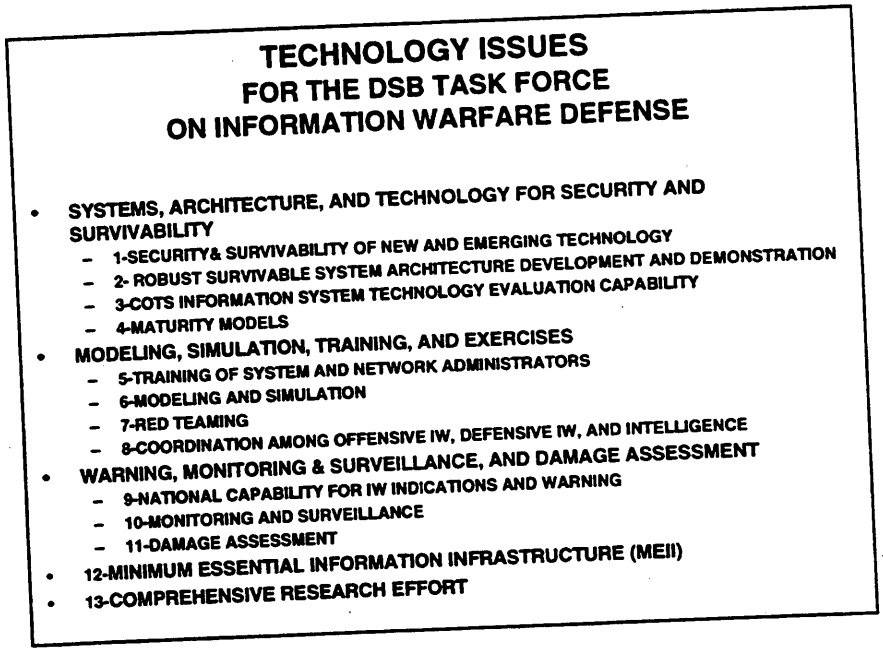
16. As in [14], but for long-term overseas bases; e.g., Europe, Japan/Korea/Okinawa.

17. Any/all of the above for the intelligence systems (sensors, ground stations, antenna farms, electronic establishments) rather than for the operational forces and the support structure.

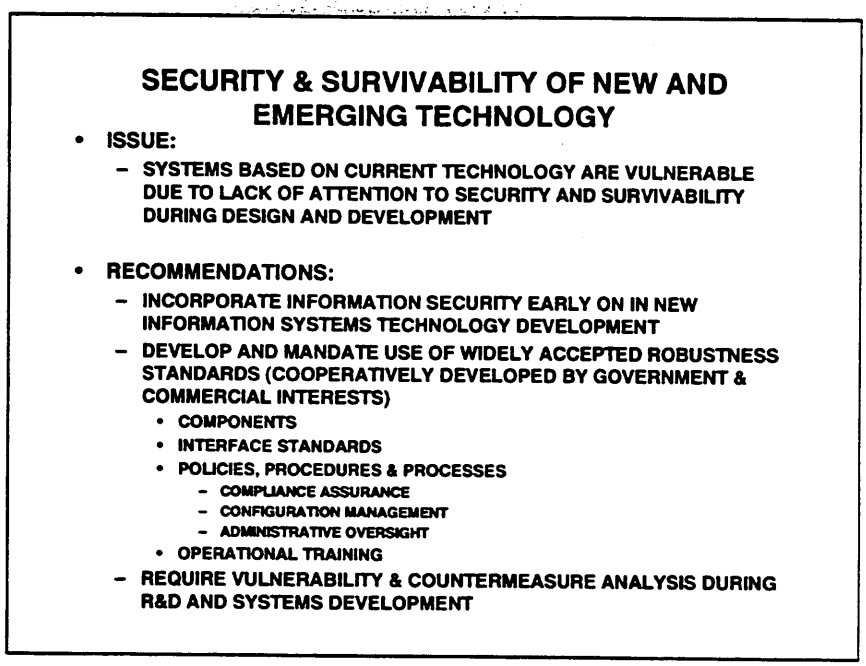
APPENDIX F

TECHNOLOGY ISSUES

This appendix provides background information on issues and recommendations developed by the Technology Panel of the Task Force. It is provided for reference and further discussion of the issues and recommendations contained in the basic report. Technology recommendations made by the full Task Force are included in the basic report.



Issues developed by the Technology Panel are presented in a set of key technology areas for Information Warfare Defense, which are grouped as shown.



SECURITY AND SURVIVABILITY OF NEW AND EMERGING TECHNOLOGY

Current system vulnerabilities are due in part to lack of attention to security and survivability issues during design and development of computing and communicating technologies. Now that the collective vulnerability due to dependence on these technologies is recognized, it is equally important to recognize the need to address security and survivability concerns in the development of new technologies. Security and survivability must be treated as critical requirements in the conceptualization and development of new and emerging technologies. While new technology is in its earliest conceptual stages, there are unique opportunities to influence developments so as to minimize vulnerabilities and strengthen security.

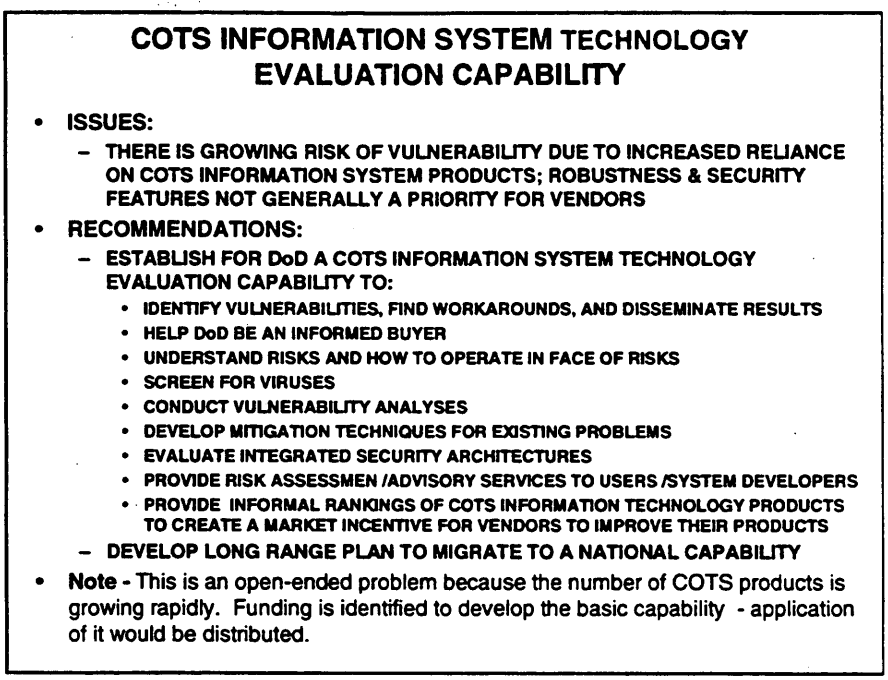
Information security needs to be incorporated early on in new information systems technology development. It is essential that the government and commercial developers of products for information systems cooperate in the evolution of common standards for robust products and practices. Information security and survivability should be incorporated early on in the development of new information systems. It is recommended that significant attention be given to stimulating and encouraging this process. Areas where commonality of robustness standards and practices should be pursued include: component hardware and software products; security interfaces; system management policies, procedures, and processes addressing such issues as compliance assurance, configuration management, administrative oversight, and robust systems operational training programs.

Since a significant level of research in the information technology area is funded by the DoD, security and survivability should become required aspects of funded programs. In addition, a DoD funded research activity should be directed at vulnerability- and countermeasures-oriented analyses of new ideas and emerging technologies, and making the results widely available to the research community.

ROBUST SURVIVABLE SYSTEM ARCHITECTURE DEVELOPMENT AND DEMONSTRATION

- ISSUE:
  - LACK OF COMPREHENSIVE, PRINCIPLED, DEMONSTRABLY-EFFECTIVE APPROACH FOR ARCHITECTURE, DESIGN, AND ANALYSIS OF SECURE, SURVIVABLE INFORMATION SYSTEMS

- RECOMMENDATIONS:
  - BUILD UPON EXISTING/EMERGING INFORMATION AND SOFTWARE ENGINEERING PRINCIPLES
    - FAULT TOLERANT SYSTEMS
    - TRUSTED SYSTEMS
    - ARCHITECTURE FOR SECURE, DISTRIBUTED SYSTEMS WHICH CAN OPERATE WHILE UTILIZING INSECURE SUBNETS AND SUBSYSTEMS
    - CONSISTENCY MECHANISMS FOR DISTRIBUTED SYSTEMS
  - DEVELOP NEW THEORY FOR ROBUST SYSTEMS
    - MODELS FOR ROBUST SYSTEMS: ATTACKS AND SURVIVAL TECHNIQUES
    - FORMAL METHODS FOR DISTRIBUTED, HETEROGENEOUS SYSTEMS
    - ANALYSIS TECHNIQUES FOR RED / BLUE CONFLICTS
  - DEVELOP SECURITY / SURVIVABILITY ARCHITECTURE PRINCIPLES
    - ADAPTIVE SYSTEM-OF-SYSTEMS ARCHITECTURE WITH ALLOCATION OF HIGH-PRIORITY TASKS TO SURVIVING SUBSYSTEMS
    - INTEGRATION OF SECURITY MANAGEMENT AND SYSTEM MANAGEMENT
    - ACCOMMODATION OF LEGACY & COTS SUBSYSTEMS (E.G., VIA WRAPPERS)
  - DEMONSTRATE EFFECTIVENESS OF SURVIVABLE ARCHITECTURE PRINCIPLES, THEORY, AND DESIGN
    - SHOW EXPERIMENTALLY IN EXISTING AND EMERGING TESTBEDS AND NETWORKS



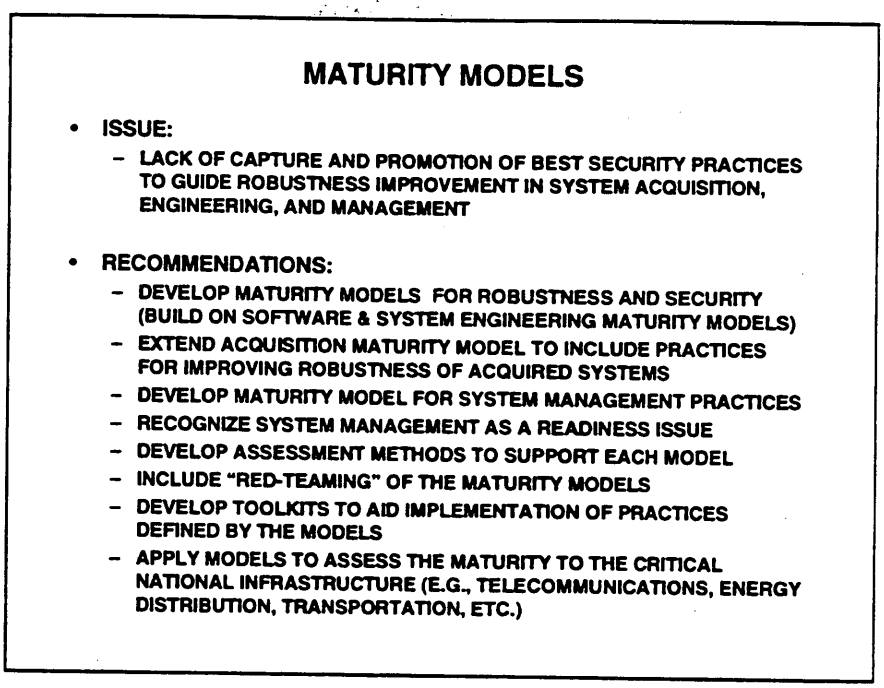
COTS INFORMATION SYSTEM TECHNOLOGY EVALUATION CAPABILITY

Economic pressures are driving the DoD toward use of COTS information systems technology, rather than custom mil-spec systems. Unfortunately manufacturers are not motivated to develop defensive IW features in their products, since commercial customers generally are not demanding them, and such features typically impact performance. Thus the DoD must take special measures to insure that the COTS approach provides adequate DIW protection for DoD applications. It is recommended that a COTS information system technology evaluation capability be established within the DoD, in order to characterize vulnerabilities in COTS products, and to develop means for dealing with their deficiencies. Basic DIW performance/certification criteria should be developed, focusing initially on DoD needs but conforming to best commercial practices insofar as possible. A major long term goal is to foster collaboration with the commercial marketplace, and plans should be developed to migrate toward a national joint DoD/commercial technology evaluation capability, rather than unilaterally setting rigid DoD requirements that ultimately will be resisted or ignored by industry. This organization or set of organizations should identify product vulnerabilities, discover workarounds, and disseminate the results. The idea is to understand the risks and learn to operate in the face of them. Currently many DoD organizations would have to analyze these products themselves; a central facility would leverage scarce expertise and save money. Such a center could serve a role like a **"Consumer's Union,"** and informal rankings of products could be provided, which could act as a spur to vendors to improve their products.

R&D is needed, preferably with joint government/industry support and working with both the offensive and defensive IW communities, to develop means for identifying product vulnerabilities to both established and emerging threats, disseminating information on such weaknesses, and developing corrective measures. Such a technology evaluation center should

also provide risk assessment/advisory services to system developers and users, perhaps based on the current Internet model of cooperation.

Note - Implementation of this recommendation is not trivial. The intent is to develop the capability, which will undoubtedly need to be tailored for different products. The tailoring/application of the capability should be distributed. One possibility is to require that before a COTS product is incorporated into a DoD system,, the capability must have been applied. Program offices could take results from previous application of the capability or pay for its application. The expectation is that this will create a market incentive for vendors to submit (and even pay for) their system for test. The funding proposed is only for development of the capability.



MATURITY MODELS

The trend toward increased use of commercial off-the-shelf software, open systems and wide area networks, is placing the information assets of many organizations at risk. These organizations may not be aware of the risks associated with these new environments, and may not be aware of the key engineering and network management practices that can be used to mitigate the risks. Acquisition and engineering managers lack comprehensive models and analytic techniques to evaluate the impact of architectural and other design choices on system robustness before major implementation investments have been made. Once networked systems are placed into operation, network operators often depend on practices and tools that were developed to assure the integrity of proprietary networks that had limited external connectivity and that were based on custom-designed software. Integrity assurance techniques developed for these restricted environments are not adequate for open, wide area networks or for an environment characterized by rapidly changing technologies and threats, and are typically focused on classical security issues.

Organizations that acquire and operate networked systems are in need of models, guidelines and tools that are effective at helping them acquire and operate systems that are highly resistant to attack, that are able to limit the damage from successful attacks, and that are capable of rapid recovery from attack. As missions, technology and threats evolve, these organizations also need system robustness assessment methods that allow them to adapt to the changing environment. Models, methods, and tools should be developed and refined concurrently to insure that management practices are aligned with the technology that supports them. The areas indicated below should be addressed.

Robustness Engineering Models

It is recommended that existing Software and Systems Engineering Capability Maturity Models be extended to describe the key engineering practices and technologies needed to allow organizations to specify and analyze non-functional attributes, such as security, as the system architecture and implementation design develops. The models should provide guidance on the process of analyzing robustness attributes, and making engineering tradeoffs. The models should be validated through empirical tests that demonstrate their ability to reflect the desired robustness attributes of the delivered systems.

Robust Systems Acquisition Maturity Model

It is recommended that the existing acquisition maturity model be extended to provide descriptions of the key practices acquisition organizations should follow to improve the robustness (including security) of acquired systems. This model should insure that the acquisition process specifies and monitors the use of robust system engineering practices for custom software, and specifies the use of robustness evaluation for off-the-shelf software.

Survivable Network Management Model

While it is unrealistic to expect that robust survivable systems can be achieved only through good management practices, it is widely recognized that without good management practices it will not be possible to secure critical systems against information warfare attacks. There is a need to develop and adhere to standardized policies, procedures and practices for management of information systems. Management and validation of information systems must be given the same priority as that given to achieving and maintaining readiness of weapons systems. It is recommended that a model be developed that provides a description of the key practices an organization should have in place to improve the robustness and survivability of its installed, networked information systems. The model should be structured as a set of key practices where each practice definition contains: (1) a description of the key practice; (2) a rationale for implementing the process; (3) guidance on how to implement the practices that helps organizations balance the value of the assets being protected with the costs of various forms of implementing the practice, the effectiveness of each form or practice, and the magnitude of the threat.

But more than a Network Management Model is needed. Automated tools are needed which will allow integrated management of large, complex, heterogeneous networks, with automated enforcement of an organization's survivability and security management models.

Robustness Assessment Methods

It is recommended that robustness assessment methods be designed to allow an organization, with minimal outside expertise, to analyze its practices against each of the system robustness models for the purpose of identifying its current state and developing robustness/survivability improvement strategies and plans. The assessment methods must:

- be suitable for self-assessment;
- yield detailed results that tell an organization where it is, where it should be, and how to get there;
- take advantage of a knowledge base that tracks threats and vulnerabilities; and
- be self-tailoring to the organization being assessed.

Robustness Improvement Toolkits

It is recommended that robustness improvement toolkits be developed that provide the tools needed to support the assessment methods and the key practices defined by the models. Tools must be structured to encapsulate knowledge of system robustness practices to leverage scarce human resources in order to help people understand which tools to use for what purposes, and promote commercialization of the tools and a community of vendors to extend and maintain them over time.

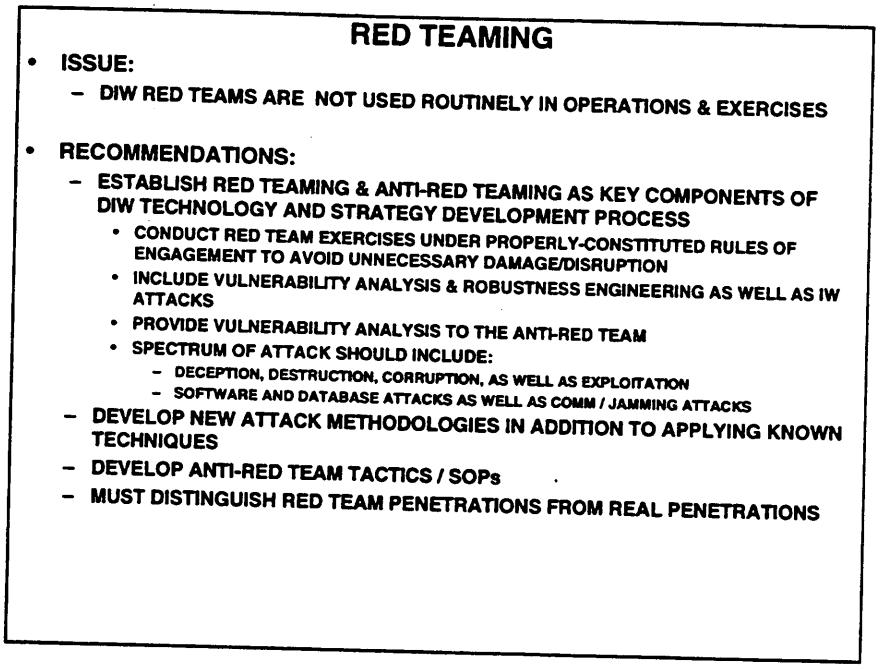
As these models and practices evolve, it is recommended that they be applied to and evaluated for effectiveness against critical elements of the national, information-dependent infrastructure, such as energy distribution, telecommunications, and transportation systems.

TRAINING OF SYSTEM AND NETWORK ADMINISTRATORS

- ISSUES:
  - IW VULNERABILITY IS USUALLY THE RESULT OF HUMAN ERROR, INSUFFICIENT TRAINING AND LACK OF KNOWLEDGE; TECHNOLOGY ALONE IS INSUFFICIENT TO CLOSE THE GAP
- RECOMMENDATIONS:
  - GIVE HIGH PRIORITY TO TRAINING OF SYSTEM AND NETWORK ADMINISTRATORS TO FORM SKILLED CADRE
  - ESTABLISH RECOGNIZED CAREER PATH
    - CRITERIA FOR SELECTION AND CERTIFICATION
    - NEC / MOS / AFSC
  - DEVELOP INFRASTRUCTURE FOR SECURITY TRAINING
    - TECHNIQUES, CURRICULUM, TOOLS, TEST BEDS
    - EXPLOIT SIMULATION TECHNOLOGY

MODELING AND SIMULATION

- ISSUE:
  - CURRENT MODELING AND SIMULATION EFFORTS DO NOT INCLUDE DIW
- RECOMMENDATIONS
  - DEVELOP MODELING AND SIMULATION ENVIRONMENTS TO SUPPORT DIW TRAINING, TACTICS DEVELOPMENT, TECHNOLOGY & TOOLS EVALUATION
  - TASK THE DEFENSE MODELLING AND SIMULATION OFFICE (DMSO) AND J8 AS ACTIONABLE ORGANIZATIONS TO MANAGE THIS EFFORT
  - SPECIFICALLY INCLUDE MODELS & SIMULATIONS OF C4I SYSTEM AND ITS CRITICAL COMPONENTS & RESOURCES, AND MODES OF FAILURE UNDER IW ATTACK; THESE C4I MODELS ARE LACKING IN CURRENT SIMULATION SYSTEMS
  - INTEGRATE WITH PLANNING AND C4I FUNCTIONS TO FACILITATE 'WHAT IF" EXERCISES FOR PLANNING, OPERATIONS ANALYSIS, MISSION REHEARSAL AND TRAINING, AND IW GAMING
  - PURSUE DEVELOPMENT OF SIMULATIONS THAT MINIMIZE BUILT-IN ASSUMPTIONS ON HUMAN TACTICAL BEHAVIOR BY INCLUDING DYNAMIC HUMAN INTERPLAY
  - LEVERAGE OFF CURRENT DISTRIBUTED INTERACTIVE SIMULATION EFFORTS (COORDINATE WITH DMSO)

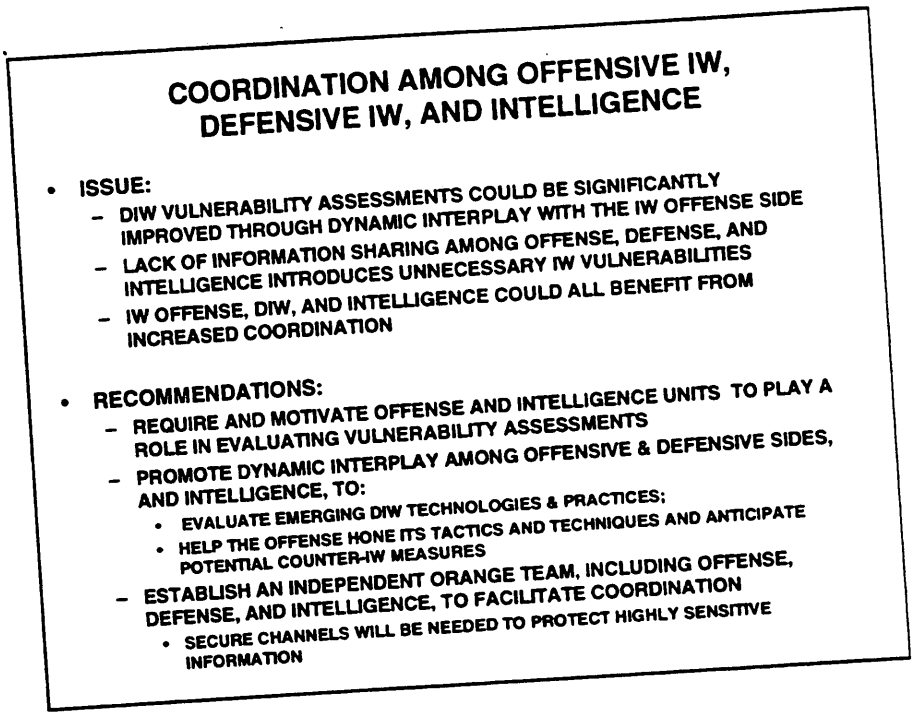


RED TEAMING

Red Teaming is an essential component of the DIW strategy and technology development process, but it is recommended that the concept be extended to include vulnerability analyses as well as carefully planned attacks during experimental activities in controlled testbeds and during training/planning exercises. The Red Team exercises should be conducted under proper rules of engagement to avoid unnecessary damage or disruption to information systems. The vulnerability analyses should be utilized by an Anti-Red Team to perform robustness engineering and to plan for fighting the Information War during the exercises as well as during operations.

Emphasis should be given to developing new attack methodologies in addition to reuse and application of current attacker techniques. For example, attacks should be designed which exploit the system's survivability features, which must be assumed known to a sophisticated attacker. In formulating these attack strategies, models should first be developed for system vulnerability and its likely defenses, and these models should be exploited in the attack strategies. Vulnerability analyses and Red Team attacks should be conducted at the application and system level, as well as at the subsystem level, with the goal of uncovering how operations can be perturbed (e.g., the planning and execution of an air tasking order or the deployment of sensors and communication assets), and how supporting communication links, or specific computers and network nodes can be compromised.

In addition to Red Teams, it is recommended that Anti-Red Teams (DIW Teams) be formed and tasked to prepare for and fight Red Team attacks. These activities will provide the basis for developing strategies and tools for use during operations to detect and respond to Information Warfare attacks. The Anti-Red Team should also be charged with providing inputs to the system designers and builders to assure the incorporation of robustness features. Network managers should be included as part of the DIW teams to assure that damage containment and service restoral techniques are effectively exercised as part of the counter-IW operation.



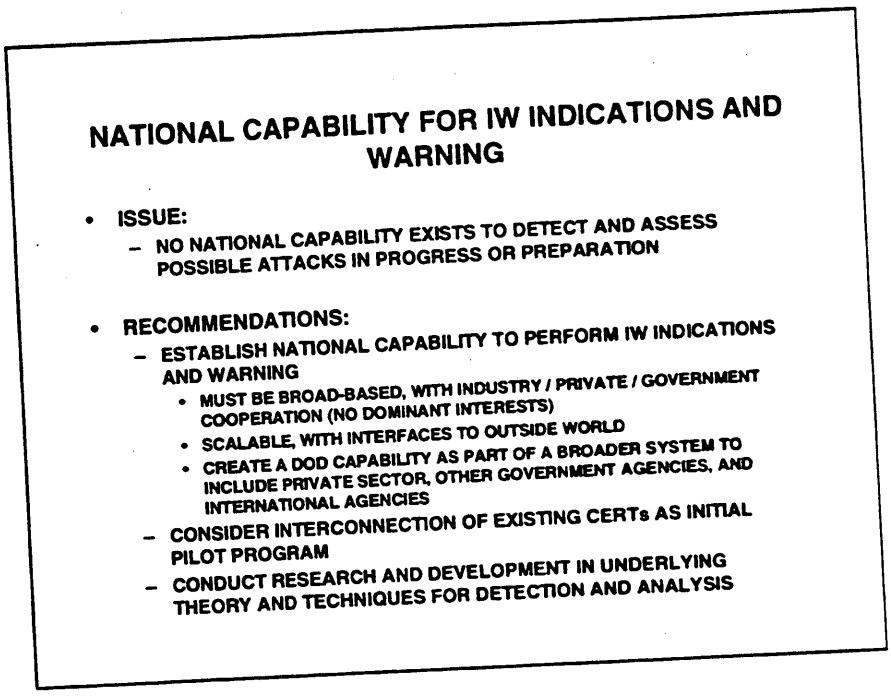
COORDINATION AMONG OFFENSIVE IW, DEFENSIVE IW, AND INTELLIGENCE

In any adversarial situation, the offensive side enjoys an inherent advantage over the defensive side, since they own the initiative, and need discover and exploit only one flaw in a defensive perimeter to achieve their ends. In contrast, the defensive side must attempt to foresee and protect against every conceivable form of assault. The situation prevails in the IW context, and it is clear that the defensive side would greatly benefit in developing risk management strategies and protective mechanisms from an awareness of the offensive side's view of the vulnerability profile and preferred set of attack techniques and approaches. The friendly offensive IW team would also benefit by interplay with its DIW allies, which would enable the offense to hone its tactics and techniques and anticipate potential counter-IW tactics. In addition, intelligence units should work together with both offense and defense to increase overall effectiveness of IW and to avoid unnecessary vulnerabilities.

It is recommended that a mechanism and a forum be developed to support a continuing, dynamic dialogue and interplay among the offensive, defensive, and intelligence communities. This activity should include information exchange on new vulnerability discoveries and attack techniques on the one hand, and red team vulnerability assessments of emerging defensive techniques and technologies on the other hand.

To provide an objective mechanism for facilitating and coordinating this dynamic interplay, an independent "ORANGE" team could be formed, devoid of vested interests on either the offensive, defensive, or intelligence sides. The orange team can also play the role of umpire and objective score keeper in red-team/vulnerability assessment war gaming activities. In general this type of 3-way interaction will lead to a better understanding of the fundamental exploitable

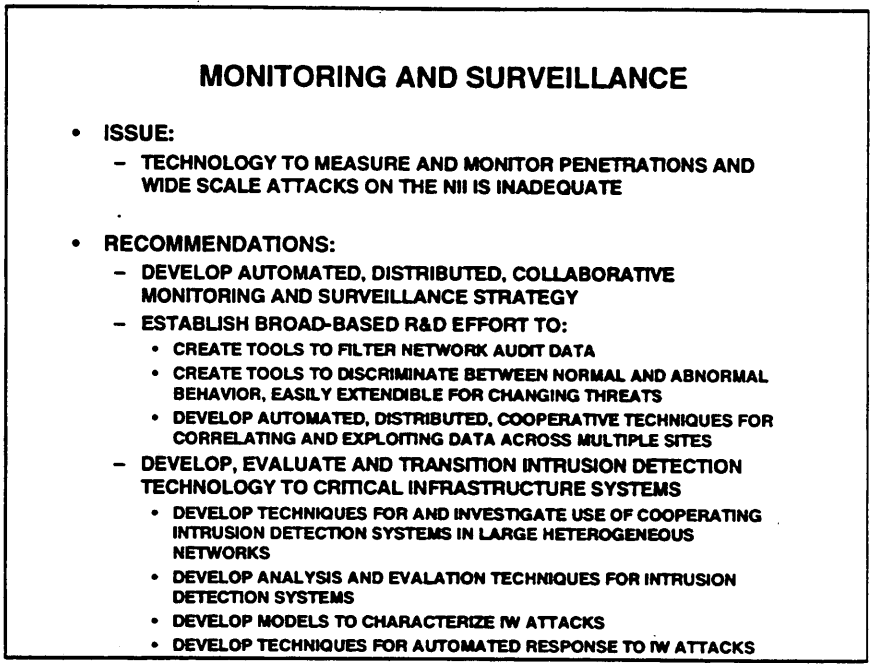
flaws typically occurring in system and communication software, distributed system architecture, communications infrastructure, and system management policies and procedures. This will also lead to new tools to address these particular areas of weakness, such as a tool for scanning developmental software to uncover design and/or implementation flaws, and leading ultimately to more reliable, robust end products.



NATIONAL CAPABILITY FOR IW INDICATIONS AND WARNING

At present, no integrated, national capability exists to detect and assess possible IW attacks in progress or preparation. Several civilian and military computer emergency response team centers have evolved, however, to provide expert diagnosis and recovery assistance for computer systems and networks that have been attacked and seriously affected by hostile actions. There is a need to detect and counter such attacks before costly information corruption and network damage occurs.

It is recommended that a National Capability Center for Indications and Warning be formed, capable of continuously gathering and analyzing monitoring data derived from government as well as commercial infrastructure systems. The center should be charged with searching for and detecting early signs and precursors of a wide scale, coordinated attack and providing warnings to U.S. government and private sector organizations. Towards that end, a phased approach is recommended, beginning with a DoD-specific organization which is scalable and extensible, and evolving towards a pan government and private sector organization. Roles of the organization should include gathering and analysis of voluntarily contributed data, dissemination of findings, and acting as a clearing house to coordinate feedback and responses from the community. The center should also act as focal point for conducting R&D on techniques and tools for attack detection and analysis. As an initial, limited scale pilot program, an interconnection of existing DoD emergency response centers should be considered.



MONITORING AND SURVEILLANCE

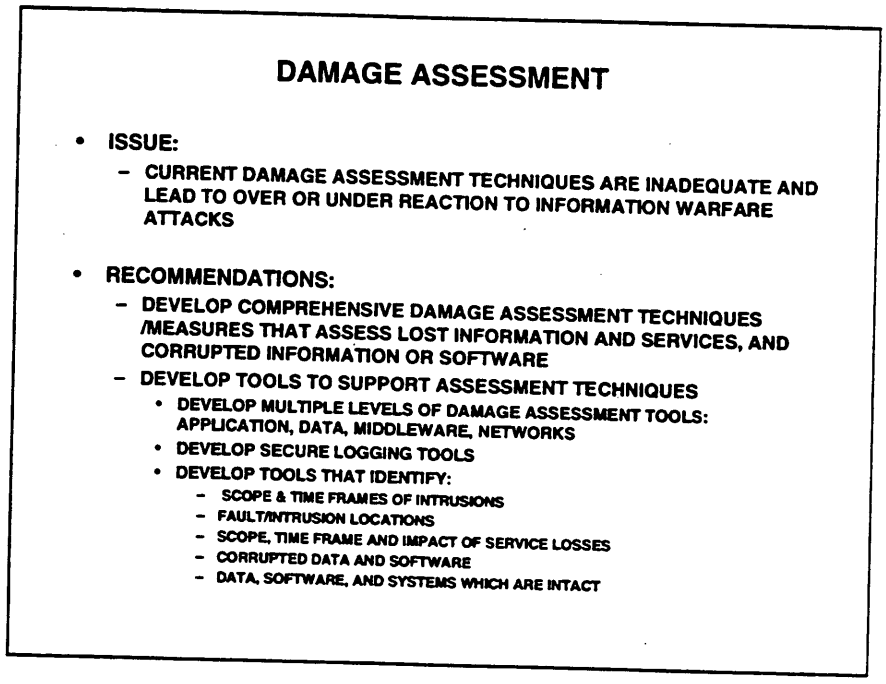
Current technology to detect, monitor and characterize local penetrations and wide scale attacks on the National Information Infrastructure (NII) is inadequate. A wide scale, coordinated, multi-faceted IW attack on the national information-dependent infrastructure represents a major distributed measurement and analysis challenge. In order to detect attacks of such scale and likely degree of subtlety, it will be necessary to extract and correlate data across many sites, since measurements at any single site may not be sufficient to reveal the emerging overall pattern. The types of attack mounted may involve techniques and degrees of sophistication beyond simple, standard intrusion detection tactics.

It is recommended that an investment be made in developing a distributed monitoring and surveillance strategy for large scale networks, along with an associated set of supporting network architectural and instrumentation principles. Further, it is recommended that a broad based research and development effort be established to develop: 1) flexible, field modifiable, trainable tools to leverage human network and security administrators in filtering network audit data, discriminating between normal and abnormal behavior, and recognizing network attacks; 2) applied pattern recognition techniques (e.g., statistical model based, or neural net) capable of adaptation, learning and coping with temporal pattern sequences; and 3) techniques and strategies for automated, collaborative, distributed pattern recognition and problem solving, supporting the correlation and exploitation of data gathered across multiple sites in a large scale network.

There is a critical need to develop, evaluate and transition intrusion detection technology and methodology to critical infrastructure systems, in particular telecommunication systems. To meet this need it is recommended that significant R&D efforts be focused in 1.) development and investigation of techniques for cooperative intrusion detection in large scale heterogeneous

networks characterized by different transmission speeds, different networking technologies and various security policies 2.) development of analysis and evaluation techniques and standard metrics for intrusion detection systems 3.) development of models to characterize IW attacks 4.) development of techniques for automatic response to incoming attacks. Such techniques should include strategies for degraded modes of operation, determining attack origin and restoral of services.

Specific emphasis should be given to demonstrating and transitioning results of the development efforts to the telecommunications and other critical infrastructure industries. This will involve adapting technologies for specific environments and evaluating and demonstrating performance in realistic scenarios and testbeds.

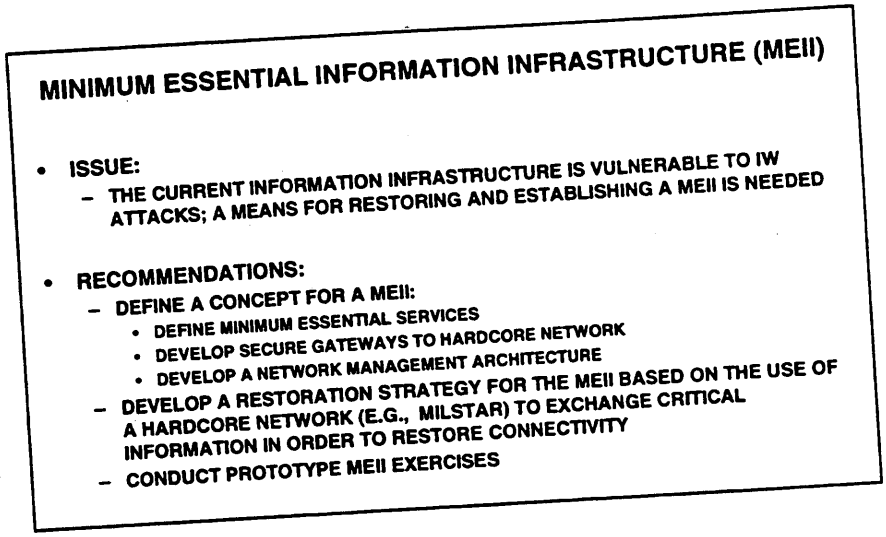


DAMAGE ASSESSMENT

In order to determine the appropriate response for a detected attack, it is important to correctly assess the associated damage. Failure to correctly assess damage could lead to costly over reaction (e.g., removing operational systems from service and/or unnecessarily rebuilding software and data bases), or dangerous under reaction (e.g., attempts to continue operations with corrupted data and software). Currently, there are no proven methods for reliably assessing the extent and nature of damage associated with information warfare attacks.

It is recommended that research and associated tool development be pursued with the objective of producing acceptable measures and techniques for damage assessment of both technological and business assets. These tools need to be able to assess damage at multiple levels, from application to networks, and to coalesce the results of the assessments at these levels. It is also recommended that secure logging tools and standard instrumentation packages for damage assessment be developed, which can be provided to all DoD sites where they are needed. Attention will have to be paid to adequately protecting such logs from tampering by an intruder. In addition, to coherently understand and deal with existing and potential future damage, it should be part of damage assessment to locate fault/intrusion sites for containment and purging purposes.

An important sub-problem in damage assessment is to identify information system components which remain undamaged and operational. Those components must be used to continue operations, as well as to help in the damage assessment process. Reliable damage assessment methods are needed for the information warfare communities and for other government and business interests, for a wide range of threats.



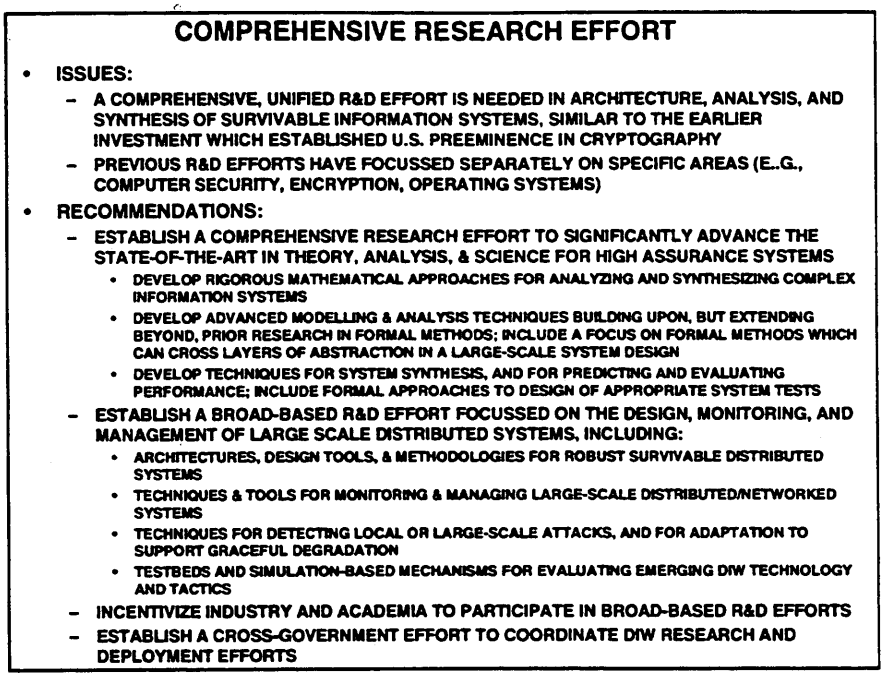
MINIMUM ESSENTIAL INFORMATION INFRASTRUCTURE

The current information infrastructure which supports telecommunications, power, transportation, etc., is susceptible to IW attacks, and in particular to wide scale coordinated attacks aimed at disabling or disrupting government as well as commercial systems. It is recommended that a strategy and overall architecture concept be developed for a minimum essential information infrastructure which can serve as a means for restoring services and adapting to wide scale outages. The technical feasibility of using Milstar assets as a means for determining available connectivity and providing modest but critical packet data service for exchange of routing, node status, and other essential network management information, should be investigated. In this role, Milstar would be supplemented with available commercial resources as possible and as needed.

The concept should consider the applications and deployment of secure gateways connected to Milstar ground station equipment and reallocated Milstar assets as a hardcore network for use in restoring critical connectivity. The authentication of commercial wireline and wireless network access through the gateway to the hardcore network is a critical issue which must be addressed.

In addition to an overall MEII architectural concept, minimum essential services, an operational concept, and a management structure must be developed. A strategy must be developed for transitioning from peacetime or normal operational activities to the minimum essential information infrastructure. It will be important to execute the transition strategy in the context of exercises.

This activity spans government, industry, and private interests, therefore it is recommended that an organization like NSTAC be commissioned to develop and define the concept of an MEII in cooperation with the DoD.



COMPREHENSIVE RESEARCH EFFORT

The development of robust survivable distributed systems resistant to information warfare attack, as well as other types of failure, requires major advances in theory, modeling and technology, and the combined efforts of a vigorous research community embracing academia, industry and government. Prior R&D efforts have focused on specific areas, such as computer and network security, encryption technology, operating system environments with multi-level security features, and coping with benign network outages caused by single node failures, etc. Little attention has been paid to the ab initio design and implementation of systems capable of surviving willful malicious attack, or detecting and tolerating corrupted software. Even less attention has been paid to the non-ab-initio case, where the system must incorporate legacy subsystems which are not under the designer's control. A comprehensive research effort is required, similar to the earlier investment in cryptographic theory, higher mathematics and associated technology, which led to U.S. preeminence in cryptography. The area of robust survivable systems offers an opportunity for a unifying theme to constitute a broad-based research effort covering the full range of 6.1, 6.2, 6.3 research, to stimulate fresh and/or revolutionary ideas and comprehensive problem solutions.

A fundamental and essential underpinning of any proposed technology base for designing and implementing large scale, robust, survivable distributed systems is a science and associated suite of design technologies for high-confidence/high assurance systems. Ideally such a set of tools would afford designers and implementers a means for describing, constructing and verifying the anticipated behavior of a complex system at all levels of abstraction. These design technologies must be capable of capturing behavioral descriptions, system properties and design descriptions in ways which enable the timely creation and performance validation of a given system implementation. Such a capability is needed because it is impossible to either anticipate or

exercise all possible interactions among the large number of constituent elements and subsystems that typically comprise any system of meaningful, real world complexity. These technologies should be bound together by a unifying, fundamental mathematical logic which would allow an integrated treatment of all hierarchies of a complex system design, from logic gates to networks of computer networks.

APPENDIX G

LIST OF ACRONYMS

ABIS	Advanced Battlefield Information System
ACTD	Advanced Concepts Technology Demonstration
Active X	See Appendix G, Glossary
Arch	Architecture
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ATD	Advanced Technology Demonstration
C2	Command and Control
C3	Command, Control and Communications
C3I	Command, Control, Communications and Intelligence
C4I	Command and Control, Communications, Computers and Intelligence
C4ISR	Command and Control, Communications, Computer Intelligence, Surveillance and Reconnaissance
CDR	Commander (USN designation of rank)
CIA	Central Intelligence Agency
CINC	Commander in Chief
CIO	Chief Information Officer
CIP	Critical Infrastructure Protection
CJCS	Chairman, Joint Chiefs of Staff
Conv.	Conventional
CONUS	Continental United States
Coord.	Coordination
CSA	CINCs/Service/Agencies
CSAAS	Combat Support Agency Assessment System
CSPAR	CINCs Preparedness Assessment Report
Ctr	Center
DASD	Deputy Assistant Secretary of Defense
DCI	Director of Central Intelligence
DEPSECDEF	Deputy Secretary of Defense
Des	Design
DIA	Defense Intelligence Agency
DII	Defense Information Infrastructure
DIS	Defense Investigative Service
DISA	Defense Information Systems Agency
DoC	Department of Commerce
DoD	Department of Defense
DoDD	Department of Defense Directive
DoE	Department of Energy

DoJ	Department of Justice
DoT	Department of Transportation
EEI	Essential Elements of Information
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
GAO	Government Accounting Office
GII	Global Information Infrastructure
HUMINT	Human Intelligence
I&W/TA	Indication and Warning/Threat Assessment
IC	Intelligence Community
Info.	Information
Intel	Intelligence
IT	Information Technology
IW	Information Warfare
IW-D	Information Warfare-Defense
JAVA	See Appendix G, Glossary
JWCA	Joint Warfare Analysis Center
MEII	Minimum Essential Information Infrastructure
Mil Deps	Military Departments
NCS	National Communications System
NEC	National Economic Council
NII	National Information Infrastructure
NRC	National Research Council
NSA	National Security Agency
NSC	National Security Council
NSIE	Network Security Information Exchange
NSTAC	National Security Telecommunications Advisory Board
Nuc.	Nuclear
OCONUS	Outside of CONUS
Off	Office
OMB	Office of Management and Budget
Ops	Operations
OSTP	Office of Science and Technology Policy
OUSD(A&T)	Office of the USD(A&T)
OUSD(P)	Office of the USD(P)

Plan	Planning
PSA	Principle Staff Assistant
PSN	Public Switched Network
Ret.	Retired
SECDEF	Secretary of Defense
SORTS	Status of Resources and Training System
TOR	Terms of Reference
Treas	Department of the Treasury
U.S.	United States
USAF	United States Air Force
USD(A&T)	Under Secretary of Defense for Acquisition and Technology
USD(C)	Under Secretary of Defense, Comptroller
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USD(P)	Under Secretary of Defense for Policy
USN	United States Navy
VADM	Vice Admiral
WARM	War-time Mode

APPENDIX H

GLOSSARY

Source: Joint Pub 1-02 , Department of Defense Dictionary of Military and Associated Terms, 23 March 1994. The DOD Dictionary of Military and Associated Terms," is promulgated for mandatory use by the Office of the Secretary of Defense, Military Departments, Joint Staff, combatant commands, and Defense agencies. Those terms approved for both DOD and NATO use are marked with an asterisk within parentheses, i.e., (*). Other sources are indicated by brackets, e.g., [CJCSI 3210.01, 1996].

acoustic warfare(*)--Action involving the use of underwater acoustic energy to determine, exploit, reduce or prevent hostile use of the underwater acoustic spectrum and actions which retain friendly use of the underwater acoustic spectrum. There are three divisions within acoustic warfare: 1. acoustic warfare support measures. That aspect of acoustic warfare involving actions to search for, intercept, locate, record and analyze radiated acoustic energy in water for purpose of exploiting such radiations. The use of acoustic warfare support measures involves no intentional underwater acoustic emission and is generally not detectable by the enemy. 2. acoustic warfare countermeasures. That aspect of acoustic warfare involving actions taken to prevent or reduce an enemy's effective use of the underwater acoustic spectrum. Acoustic warfare countermeasures involve intentional underwater acoustic emissions for deception and jamming. 3. acoustic warfare counter-countermeasures. That aspect of acoustic warfare involving actions taken to ensure friendly effective use of the underwater acoustic spectrum despite the enemy's use of underwater acoustic warfare. Acoustic warfare counter-countermeasures involve anti-acoustic warfare support measures and anti-acoustic warfare countermeasures, and ma not involve underwater acoustic emissions.

acoustic warfare counter-countermeasures--See acoustic warfare Part 3.

acoustic warfare countermeasures--See acoustic warfare Part 2.

acoustic warfare support measures--See acoustic warfare Part 1

active air defense(*)--Direct defensive action taken to nullify or reduce the effectiveness of hostile air action. It includes such measures as the use of aircraft, air defense weapons, weapons not used primarily in an air defense role, and electronic warfare. See also air defense.

Active X--A name for a version of Distributed Object Linking and Embedding (OLE) that enables sharing of data, links, and controls over a network (primarily for interoperability among Windows-based software).

antiair warfare--A U.S. Navy/U.S. Marine Corps term used to indicate that action required to destroy or reduce to an acceptable level the enemy air and missile threat. It includes such measures as the use of interceptors, bombers, antiaircraft guns, surface-to-air and air-to-air missiles, electronic attack, and destruction of the air or missile threat both before and after it is

launched. Other measures which are taken to minimize the effects of hostile air action are cover, concealment, dispersion, deception (including electronic), and mobility. See also counter air.

antisubmarine operation--Operation contributing to the conduct of antisubmarine warfare.

antisubmarine warfare(*)--Operations conducted with the intention of denying the enemy the effective use of submarines.

attack assessment--An evaluation of information to determine the potential or actual nature and objectives of an attack for the purpose of providing information for timely decisions. See also damage estimation.

biological operation(*)--Employment of biological agents to produce casualties in personnel or animals and damage to plants or materiel; or defense against such employment

biological operation(*)--Employment of biological agents to produce casualties in personnel or animals and damage to plants or materiel; or defense against such employment.

biological warfare--See biological operation.

C2-protection--See command and control warfare.

chemical warfare--All aspects of military operations involving the employment of lethal and incapacitating munitions/agents and the warning and protective measures associated with such offensive operations. Since riot control agents and herbicides are not considered to be chemical warfare agents, those two items will be referred to separately or under the broader term "chemical," which will be used to include all types of chemical munitions/agents collectively. The term "chemical warfare weapons" may be used when it is desired to reflect both lethal and incapacitating munitions/agents of either chemical or biological origin. Also called CW. See also chemical operations, herbicide, riot control agent.

combined warfare--Warfare conducted by forces of two or more allied nations in coordinated action toward common objectives.

command and control warfare--The integrated use of operations security (OPSEC), military deception, psychological operations (PSYOP), electronic warfare (EW), and physical destruction, mutually supported by intelligence, to deny information to, influence, degrade, or destroy adversary command and control capabilities, while protecting friendly command and control capabilities against such actions. Command and control warfare applies across the operational continuum and all levels of conflict. Also called C2W. C2W is both offensive and defensive: a. counter-C2--To prevent effective C2 of adversary forces by denying information to, influencing, degrading, or destroying the adversary C2 system. b. C2-protection--To maintain effective command and control of own forces by turning to friendly advantage or negating adversary efforts to deny information to, influence, degrade, or destroy the friendly C2 system. See also command and control; electronic warfare; intelligence; military deception; operations security; psychological operations.

counterguerrilla warfare(*)--Operations and activities conducted by armed forces, paramilitary forces, or nonmilitary agencies against guerrillas.

damage estimation--A preliminary appraisal of the potential effects of an attack. See also attack assessment.

directed-energy protective measures--That division of directed-energy warfare involving actions taken to protect friendly equipment, facilities, and personnel to ensure friendly effective uses of the electromagnetic spectrum that are threatened by hostile directed-energy weapons and devices.

directed-energy warfare--Military action involving the use of directed-energy weapons, devices, and countermeasures to either cause direct damage or destruction of enemy equipment, facilities, and personnel, or to determine, exploit, reduce, or prevent hostile use of the electromagnetic spectrum through damage, destruction, and disruption. It also includes actions taken to protect friendly equipment, facilities, and personnel and retain friendly use of the electromagnetic spectrum. Also called DEW. See also directed energy; directed-energy device; directed-energy weapon; electromagnetic spectrum; electronic warfare.

directed-energy weapon--A system using directed energy primarily as a direct means to damage or destroy enemy equipment, facilities, and personnel. See also directed energy; directed energy device.

economic warfare--Aggressive use of economic means to achieve national objectives.

electromagnetic intrusion--The intentional insertion of electromagnetic energy into transmission paths in any manner, with the objective of deceiving operators or of causing confusion. See also electronic warfare.

electronic warfare--Any military action involving the use of electromagnetic and directed energy to control the electromagnetic spectrum or to attack the enemy. Also called EW. The three major subdivisions within electronic warfare are: electronic attack, electronic protection, and electronic warfare support. a. electronic attack--That division of electronic warfare involving the use of electromagnetic or directed energy to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying enemy combat capability. Also called EA. EA includes: 1) actions taken to prevent or reduce an enemy's effective use of the electromagnetic spectrum, such as jamming and electromagnetic deception, and 2) employment of weapons that use either electromagnetic or directed energy as their primary destructive mechanism (lasers, radio frequency weapons, particle beams). b. electronic protection--That division of electronic warfare involving actions taken to protect personnel, facilities, and equipment from any effects of friendly or enemy employment of electronic warfare that degrade, neutralize, or destroy friendly combat capability. Also called EP. c. electronic warfare support--That division of electronic warfare involving actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate sources of intentional and unintentional radiated electromagnetic energy for the purpose of immediate threat recognition. Thus, electronic warfare support provides information required for immediate decisions involving electronic warfare operations and other tactical actions such as threat avoidance, targeting, and homing. Also called ES. Electronic warfare support data can be used to produce signals intelligence (SIGINT), both communications intelligence (COMINT), and electronics intelligence (ELINT). See also command and control warfare; communications intelligence; directed energy; directed-energy device; directed-energy warfare; directed-energy

weapon; electromagnetic compatibility; electromagnetic deception; electromagnetic hardening; electromagnetic jamming; electromagnetic spectrum; electronics intelligence; frequency deconfliction; signals intelligence; spectrum management; suppression of enemy air defenses.

guerrilla warfare(*)--Military and paramilitary operations conducted in enemy-held or hostile territory by irregular, predominantly indigenous forces. See also unconventional warfare.

indications and warning--Those intelligence activities intended to detect and report time-sensitive intelligence information on foreign developments that could involve a threat to the United States or allied military, political, or economic interests or to U.S. citizens abroad. It includes forewarning of enemy actions or intentions; the imminence of hostilities; insurgency; nuclear/non-nuclear attack on the United States, its overseas forces, or allied nations; hostile reactions to United States reconnaissance activities; terrorists' attacks; and other similar events.

information warfare--Actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. [CJCSI 3210.01, 1996]

integrated warfare--The conduct of military operations in any combat environment wherein opposing forces employ non-conventional weapons in combination with conventional weapons.

JAVA--An object-oriented, platform-independent programming language, often used to create small cross-program executable software applications called applets that are downloaded from remote sites and that execute automatically.

mine warfare--The strategic, operational, and tactical use of mines and mine countermeasures. Mine warfare is divided into two basic subdivisions: the laying of mines to degrade the enemy's capabilities to wage land, air, and maritime warfare; and the countering of enemy-laid mines to permit friendly maneuver or use of selected land or sea areas.

naval coastal warfare--Coastal sea control, harbor defense, and port security, executed both in coastal areas outside the United States in support of national policy and in the United States as part of this Nation's defense. Also called NCW.

naval special warfare--A specific term describing a designated naval warfare specialty and covering operations generally accepted as being unconventional in nature and, in many cases, covert or clandestine in character. These operations include using specially trained forces assigned to conduct unconventional warfare, psychological operations, beach and coastal reconnaissance, operational deception operations, counterinsurgency operations, coastal and river interdiction, and certain special tactical intelligence collection operations that are in addition to those intelligence functions normally required for planning and conducting special operations in a hostile environment. Also called NSW.

nuclear warfare(*)--Warfare involving the employment of nuclear weapons. See also postattack period; transattack period.

operations security--A process of identifying critical information and subsequently analyzing friendly actions attendant to military operations and other activities to: a. Identify those actions

that can be observed by adversary intelligence systems. b. Determine indicators hostile intelligence systems might obtain that could be interpreted or pieced together to derive critical information in time to be useful to adversaries. c. Select and execute measures that eliminate or reduce to an acceptable level the vulnerabilities of friendly actions to adversary exploitation. Also called OPSEC. See also command and control warfare; operations security indicators; operations security measures; operations security planning guidance; operations security vulnerability.

perception management--Actions to convey and/or deny selected information and indicators to foreign audiences to influence their emotions, motives, and objective reasoning; and to intelligence systems and leaders at all levels to influence official estimates, ultimately resulting in foreign behaviors and official actions favorable to the originator's objectives. In various ways, perception management combines truth projection, operations security, cover and deception, and psychological operations. See also psychological operations.

political warfare--Aggressive use of political means to achieve national objectives.

psychological operations--Planned operations to convey selected information and indicators to foreign audiences to influence their emotions, motives, objective reasoning, and ultimately the behavior of foreign governments, organizations, groups, and individuals. The purpose of psychological operations is to induce or reinforce foreign attitudes and behavior favorable to the originator's objectives. Also called PSYOP. See also perception management.

psychological warfare--The planned use of propaganda and other psychological actions having the primary purpose of influencing the opinions, emotions, attitudes, and behavior of hostile foreign groups in such a way as to support the achievement of national objectives. Also called PSYWAR.

strategic air warfare--Air combat and supporting operations designed to effect, through the systematic application of force to a selected series of vital targets, the progressive destruction and disintegration of the enemy's war-making capacity to a point where the enemy no longer retains the ability or the will to wage war. Vital targets may include key manufacturing systems, sources of raw material, critical material, stockpiles, power systems, transportation systems, communication facilities, concentration of uncommitted elements of enemy armed forces, key agricultural areas, and other such target systems.

tactical warning--1. A warning after initiation of a threatening or hostile act based on an evaluation of information from all available sources. 2. In satellite and missile surveillance, a notification to operational command centers that a specific threat event is occurring. The component elements that describe threat events are: Country of origin--country or countries initiating hostilities. Event type and size--identification of the type of event and determination of the size or number of weapons. Country under attack--determined by observing trajectory of an object and predicting its impact point. Event time--time the hostile event occurred. Also called integrated tactical warning. See also attack assessment; strategic warning.

tactical warning and assessment--A composite term. See separate definitions for tactical warning and for attack assessment.

unconventional warfare--A broad spectrum of military and paramilitary operations, normally of long duration, predominantly conducted by indigenous or surrogate forces who are organized, trained, equipped, supported, and directed in varying degrees by an external source. It includes guerrilla warfare and other direct offensive, low visibility, covert, or clandestine operations, as well as the indirect activities of subversion, sabotage, intelligence activities, and evasion and escape. Also called UW.

22 JAN 1997
Ref: 97-F-0073

Mr. David A. Banisar
Electronic Privacy Information Center
666 Pennsylvania Avenue, S.E., Suite 301
Washington, D.C. 20003

Dear Mr. Banisar:

This letter responds to your January 9, 1997, Freedom of Information Act (FOIA) request. The telephone conversation with Commander Voorhies of this Directorate on January 21, 1997, refers.

As agreed in the telephone conversation with Commander Voorhies, the enclosed document is provided as responsive to your request. There are no chargeable costs for processing your FOIA request in this instance.

Sincerely,

"Signed"
A. H. Passarella
Director
Freedom of Information
and Security Review

Enclosure:
As stated

Prepared by VOORHIES:gjv:1/22/97:DFOI:gr__pk__yl__wh__

R/R Please

#834