Protecting the Homeland

Report of the Defense Science Board Task Force

on

DEFENSIVE INFORMATION OPERATIONS 2000 Summer Study Volume II

March 2001

Office of the Undersecretary of Defense
For Acquisition, Technology, and Logistics
Washington, D.C. 20301-3140

This 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 no necessarily represent the official position of the Department of Defense.

This report is unclassified.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	March 2001	Final Technical, 2001

4. TITLE AND SUBTITLE
Defense Science Board Task Force on Defensive Information Operations, 2000 Summer Study, Vol. II (Protecting the Homeland)

5. FUNDING NUMBERS
N/A

6. AUTHOR(S)
Mr. Larry Wright
Task Force Chairman

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Defense Science Board
Office of the Under Secretary of Defense (AT&L)
3140 Defense Pentagon
Room 3D865
Washington DC 20301-3140

8. PERFORMING ORGANIZATION REPORT NUMBER
N/A

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Defense Science Board
Office of the Under Secretary of Defense (AT&L)
3140 Defense Pentagon
Room 3D865
Washington DC 20301-3140

10. SPONSORING/MONITORING AGENCY REPORT NUMBER
N/A

11. SUPPLEMENTARY NOTES
N/A

12a. DISTRIBUTION AVAILABILITY STATEMENT
Distribution Statement A: Unlimited Distribution

12b. DISTRIBUTION CODE
A

13. ABSTRACT *(Maximum 200 words)*

14. SUBJECT TERMS

15. NUMBER OF PAGES
184

16. PRICE CODE
N/A

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
UNCLASSIFIED	UNCLASSIFIED	N/A	N/A

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

DEFENSE SCIENCE
BOARD

MAR 28 2001

MEMORANDUM FOR PRINCIPAL DEPUTY UNDER SECRETARY OF DEFENSE
(ACQUISITION, TECHNOLOGY & LOGISTICS)

SUBJECT: Final Report of the Defense Science Board (DSB) Summer Study Task Force on Defensive Information Operations

I am pleased to forward the final report of the DSB Task Force on Defensive Information Operations. The Task Force was tasked to review and evaluate DoD's ability to provide information assurance to carry out Joint Vision 2010 in the face of information warfare attack.

In their report, the Task Force states that DoD cannot today defend itself from an Information Operations attack by a sophisticated nation state adversary. To that end, I agree with their belief that if Joint Vision 2020 is to be the path to the future, these vulnerabilities must be addressed.

I endorse all of the Task Force's recommendations and propose you review the Task Force Chairman's letter and report.

William Schneider
DSB Chairman

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

March 1, 2001

DEFENSE SCIENCE BOARD

Memorandum for the Chairman, Defense Science Board

Subject: Report of the Defense Science Board Task force on Defensive Information Operations

The Department of Defense has adopted Joint Vision 2020 as its approach to conflict in the future. Both Information Superiority and Decision Superiority are key components of JV2020, and future warfighting plans will be increasingly reliant upon high-speed interconnected information networks to identify targets, create and transmit plans, disseminate and share information, and carry out battles. This construct for the military is based on the ability to detect and track the enemy, move that information across continents, integrate and analyze it, then decide and take action, often under very tight time constraints; sometimes within minutes. It is the protection of this information upon which this Defense Science Board Task Force concentrated its efforts.

The threats to the DoD infrastructure are very real, non-traditional and highly diversified. Within the past year, the Love Bug Virus spread to over one million computers in just five hours: far more rapidly than defenses or law enforcement could respond. Attacks vary widely from those perpetrated by trusted insiders, to remote attacks by individuals, organized groups, or nation states, employing new approaches we do not yet understand. China has made clear its intention to use Information Operations (warfare) as an asymmetric response in any conflict with the United States. Various components of Information Operations, including psychological operations, computer network attack, and computer network defense were used during the Kosovo crisis. More recently, both the Israelis and the Palestinians used cyber attacks as an integral part of heightened conflict in the Middle East. Furthermore, those attacks were magnified by the participation of thousands of civilians "called to cyber arms" by their colleagues.

The vulnerabilities of these United States are greater than ever before, and we know that over twenty countries already have or are developing computer attack capabilities. Moreover, the Department of Defense should consider existing viruses and "hacker" attacks to be to real "Information Operations or Warfare", what early aviation was to Air Power. In other words, we have not seen anything yet! And the importance of this is magnified by the increased reliance the DoD places on having just the right information at the right place, at the right time: JV2020!

These vulnerabilities, inextricably intertwined with our civilian infrastructure, when coupled with known and expected capabilities of potential adversaries raise serious questions about the readiness of the DoD to conduct Defensive Information Operations. To address these challenges, this task force focused on issues and opportunities in five major areas:

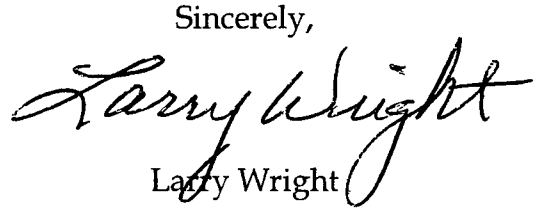
- Architecture for Information Assurance
- Technology Challenges and Applications
- Organization, Operations and Readiness
- Policy Implications
- Legal Implications

The report is provided in two volumes. Volume I presents the overall observations, findings and primary recommendations for each of the five focus areas -- addressed at the decision maker level. Volume II provides a detailed report for each of the five focus areas, with more specific recommendations including courses of action, cost estimates, and anticipated level of effort - addressed at the implementation level. While there is no hierarchy implicit in these topics, recommendations pertaining to some will be easier and less costly. Others, like the architecture, will have the greatest impact, take the most time, and be the most expensive. Even so, it is only the successful integration of all of the recommendations that will provide the DoD with the Information Infrastructure needed to achieve the goals the joint vision.

It is the view of this task force, that DoD cannot today defend itself from an Information Operations attack by a sophisticated nation state adversary. If Joint Vision 2020 is to be the path to the future, these vulnerabilities and shortfalls must be addressed. The topics and recommendations discussed herein are essential to achieving that goal.

Now is the time to make some difficult decisions and invest the required significant resources. Successful information-intensive industries have shown the way to embrace change. But the DoD challenge is more difficult: not only to embrace change, but also to build trust and security to a degree no business could afford.

Sincerely,



Larry Wright

TABLE OF CONTENTS

DSB VOLUME I – DEFENSIVE INFORMATION OPERATIONS

DSB VOLUME II –ANNEXES

TABLE OF FIGURES

EXECUTIVE SUMMARY

There is nothing more difficult to take in hand, more perilous to conduct, or more uncertain in its success, than to take the lead in the introduction of a new order to things. ***-Niccolo Machiavelli***

In its 1996 report, the Defense Science Board (DSB) recommended that the Pentagon invest an additional $3 billion to strengthen defenses of its information networks. This report was viewed by some as unrealistic and prophetic by others, but in all cases it faced a readership with a very uneven appreciation of the effects of disruptive technology and discontinuous change. The defense establishment has increased its intellectual capital on the subject of Defensive Information Operations (DIO) considerably since 1996. However, it has yet to fully accommodate the realities of an information intensive future in its architecture, processes, and investments. Technology has continued to evolve and the problems have become much more difficult and complex. DoD must now accomplish more than anyone could have imagined in 1996. Perhaps more important is the dawning realization that incremental modifications to our existing institutions and processes will not produce the adaptation we need.

The reality seems compelling. At some future time, the United States will be attacked, not by hackers, but by a sophisticated adversary using an effective array of information warfare tools and techniques. Two choices are available: adapt before the attack or afterward. This report offers a realistic set of options to adapt before the attack.

A specific example of progress coming hand-in-hand with new vulnerabilities is the Department's embrace of Web-based technologies, which offer great flexibility and ease of operation. On the other hand, the concomitant vulnerabilities of such an approach mean that defensive measures have never been more important.

In Joint Vision 2020 (JV2020), future warfighting plans will be increasingly reliant upon high-speed interconnected information networks to identify targets, create and transmit plans, disseminate and share information, and carry out battles. This construct for the military is based on the ability to detect and track the enemy, move that information across continents, fuse it and analyze it, then decide and take action, often under very tight time constraints, sometimes within minutes. It is the protection of this information upon which this task force concentrated its efforts.

In the view of the task force, DoD is "betting the farm" on having assured information in its information networks, now collectively referred to as the Global Information Grid (GIG). The GIG is a fundamental tenet of the Department's Joint Vision 2020. Without a considerable effort to provide information assurance, such a complex system will introduce inherent, and perhaps crippling, vulnerabilities into the military force structure.

The Defense Department's networks, both non-classified and classified, as well as its tactical systems, depend on commercially available telecommunications. Rather than laying cable and launching communications satellites itself, the Defense Department leases the vast majority of those services from private industry, which tends to use the most cost-effective option rather than the most secure. Interdependencies are poorly understood and all segments of critical networks

are difficult to identify. If there is a weakness in any part of the network, the effect could range from a minor annoyance to disruption of a major military operation.

Together with DoD-unique software and systems, this commercial infrastructure forms the underpinning of the GIG upon which Joint Vision 2020 depends. The GIG is being developed from legacy and new systems, growing in capability with every "node" a system engineer connects to it, and becoming increasingly vulnerable. Each component's vulnerability to information operations exposes others on the grid to danger as well.

Most will now agree that the Information Operations (IO) threat is very real, and non-traditional. There are numerous examples of the damage that can be done even by simple tools. The Love Bug spread to an estimated one million computers in just five hours, far more rapidly than defenses or law enforcement could respond. Additionally, our defenses are not focused on detecting "low and slow" attacks, so it is certainly possible that such attacks have taken place. Attacks vary widely and include everything from those perpetrated by trusted insiders to remote attacks and new approaches we don't yet understand. U.S. vulnerabilities are greater than in 1996, and in excess of 20 countries already have or are developing computer attack capabilities. DoD should consider existing viruses and low level attacks to be to "real" Information Operations what early aviation was to air power.

Furthermore, DoD is vulnerable in so many other ways: there are several operating systems in use, and in excess of 700 applications–all collectively using greater than 100 million lines of software code. Few of these have been checked for malicious code, and new hardware and software is installed virtually every day.

This task force concludes that the GIG is a weapon system and must be treated as such. The United States is in an arms race, and experience suggests that as U.S. defensive capabilities increase, so will the adversary's offense. Although the GIG is a powerful management and technical concept and a key enabler of JV2020, there is currently no security or Information Assurance (IA) architecture planned that addresses the emerging threat. The task force identified the need for the Department to develop and implement such an architecture and provides a target architecture and processes for achieving it.

The task force offers a series of recommendations for successful implementation and execution of DIO based on the concept of defense-in-depth (DiD). In other words, complex systems of systems require a variety of defenses. The good news is that some of the most important, such as improved training, coupled with updated policies and procedures, can have an immediate impact without any technical risk. Another important aspect of defense-in-depth is that it will provide some protection against an adversary's denial and deception efforts.

In order to maintain confidence in the information moving on the GIG, DoD must be assured that sources of information and a system's integrity have not been compromised. This cannot be achieved without Department-wide coherence in system design, construction, operation, and evaluation, and a commitment to the necessary investments. For example, in order to evaluate the security and effectiveness of the GIG, DoD needs to establish a distributed test bed to evaluate and improve IA and develop technical metrics of IA effectiveness. The department must be able to measure and evaluate the ability of information systems to detect an attack, react to protect themselves, and recover.

The task force found that the Department is not yet building the means to achieve and retain information superiority in the presence of a robust information warfare threat. Although substantial progress is evident in the perception of the threat, the Department has yet to implement a program of Defensive Information Operations that can underwrite the information superiority needed for success in Joint Vision 2020. Frankly, the risk of failure is high given today's capability and direction. This task force outlines recommendations that would reduce this risk significantly.

Several key recommendations center on the GIG. For example:

- Implement a consistent security architecture for every node on the network that forms the GIG, supported by strong policies, processes and technologies.
- Move all of the Pentagon's public Web sites off the NIPRNET and into a more controlled environment, with encryption and digital identity "keys."
- Watch over the GIG with a host of different intrusion-detection systems.
- Constantly improve the security of the GIG through continued research and development on key problem areas such as reconstitution.
- Create a new Deputy Secretary of Defense (DepSecDef)-led Board to oversee implementation of the GIG and this new security architecture.

The Department has a set of legacy information systems and networks from which the GIG must evolve. Once the security architecture for the GIG has been established as recommended in this report, the Department should identify those legacy systems that are most mission-critical, those that are mission-essential and those that are neither. Such a prioritization was prepared in response to the Year 2000 (Y2K) software concern in DoD systems; this same approach could now be effective in setting priorities for system upgrades, vulnerability assessments and security enhancements to the evolving GIG.

Technology must be a key enabler of the GIG. For decades, sound computer and telecommunications security relied on two fundamental precepts. First, protect the perimeters, the physical environment and equipments. Secondly, protect – by encryption – information in transit from one security enclave to another. These precepts are still very necessary, but in the new networked world, they are no longer adequate. Today, DoD must establish a robust defense-in-depth strategy to respond to known and anticipated vulnerabilities in the Defense Information Infrastructure (DII). A critical ingredient of an effective DiD strategy will be investments in high leverage Research and Development (R&D) activities. Examples of areas that must be researched include: scalable global access control, malicious code detection and mitigation, mobile code security, fault tolerance, integrity restoration, recovery and reconstitution, and a number of other important technologies. Regarding scalable access control, Public Key Infrastructure (PKI) with Public Key Enabled (PKE) applications must be a key component of the GIG security architecture. The task force believes that current FYDP funds for incorporation of PKI/PKE must be increased by a factor of two.

Sometimes a shift in requirements will permit a shift in resources to address the new requirements. In the case of computer network defense, however, DoD must continue perimeter defense efforts and developments, and simultaneously provide additional R&D for technologies

to support defense-in-depth. While there are some initiatives ongoing under the Defense Advanced Research Projects Agency's (DARPA's) Third Generation Security Initiative, this DSB task force proposes additional R&D over the FYDP (by a factor of two) to develop key technologies for Information Assurance. The task force notes that these technologies are needed by DoD whether it chooses to permit the Services to develop independent service architectures, or whether the GIG is developed as proposed in this report.

Another category of recommendations addresses readiness of systems and people. The readiness of its warfighters to accomplish their missions must be of singular importance to DoD. It is clear that a significant number of nations (more than twenty at present count) are building capabilities for conflict in a cyber world. China has made clear its intentions to use Information Operations (warfare) as an asymmetric response in any conflict with the United States. Various components of Information Operations, including psychological operations, computer network attack and computer network defense were used during the Kosovo crisis. More recently, both the Israelis and the Palestinians have used cyber attacks as an integral part of heightened conflict in the Middle East. Furthermore, those attacks have been magnified by the participation of thousands of civilians "called to cyber arms" by their colleagues. The significant vulnerabilities of the DoD Information Infrastructure, coupled with known and expected capabilities of our potential adversaries to assault the DII, raises serious questions about DoD readiness to conduct Defensive Operations. It is the view of the task force that DoD cannot today defend itself from an Information Operations attack by a sophisticated, nation state adversary.

Further, the task force found that DIO is not adequately integrated into mission planning and execution within the Services and the Unified and Specified Commands. Therefore, the Secretary of Defense (SecDef), through the Chairman of the Joint Chiefs, should issue specific guidance to make DIO a key element of all military planning and operations, and fold that process into the Joint Military Readiness Reporting system. To address the finding that the DoD is not moving fast enough to identify its private sector dependencies and vulnerabilities, the Joint Program Office (JPO), Dahlgren, Virginia should be chartered and resourced to assist local commanders in identifying and assessing key infrastructure dependencies and vulnerabilities.

The necessity of Red Teams to provide a world-class threat evaluation of our defensive capabilities is worthy of special emphasis. During the past three and one-half years, the National Security Agency (NSA) Red Teams have conducted 37 assaults of DoD networks – 99% of which were undetected even though the attacks used tools known by the network operators to exist. Thirty-seven attacks in three and one-half years hardly represents the level of effort envisioned in the 1996 DSB task force recommendations. The Task Force urges that dramatically more effort be placed in this critical area. One approach would be to use the processes, which worked well in the Department's Y2K remediation efforts. Categorizing networks and systems as mission-critical, mission-essential, or otherwise, as was done for Y2K, could help prioritize DoD's assessment efforts. For example, if DoD concluded that it had 500 mission critical systems, and that an assessment must be made on each of those every other year, it would be possible to conduct 100 of those assessments by Red Team and 400 of them by Vulnerability Assessments. Thus, DoD's Red Teams would need to be increased five-fold (roughly ten per year with existing resources, and fifty per year needed to meet the new goals) to implement the new program. The task force believes the SecDef should formalize and empower DIO Red Teaming throughout DoD by expanding the number, scope and frequency of assessments, specifically including the development and applications of three distinct levels of assessments: Red Teams,

Vulnerability Evaluations and Vulnerability Assessments. Vulnerability Evaluation and Vulnerability Assessment teams could be augmented using outsourced resources to implement these programs relatively quickly.

The task force also addressed the human resources problem and found that the DoD shortage of IT professionals is serious and growing. People will continue to be both the principal source of strength in Information Operations, and DoD's greatest potential vulnerability. In highly networked environments, the risk assumed by one is imposed upon many--with the potential for damage, disruption, denial or corruption of the DII. DoD has over 2,000,000 users on 10,000 networks, managed by 100,000-125,000 systems administrators. (No one is certain how many there actually are.) These dynamics raise several issues for DoD about acquiring and retaining skilled staff and operating the DII, while simultaneously preserving the security, integrity and readiness of the Information Infrastructure. In large part, these personnel issues highlighted in the 1996 DSB report remain, and in fact have become more severe in light of the dramatic increase in networked communications and computers with the attendant shared risk and vulnerabilities.

Recommendations for more aggressive recruitment and proficiency pay, as well as training programs, are suggested to redress the shortage of IT professionals. The Department has the authority to provide proficiency pay to IT professionals but has not used it. Given a current shortage of over 800,000 IT professionals in the United States alone, the DoD must pull out all of the stops to acquire and retain key IT staff. Furthermore, a comprehensive program which provides career paths for IT professionals, coupled with outsourcing where feasible, and an innovative program to attract high school graduates into DoD to become systems administrators in exchange for world class training, are all necessary to provide DoD the cadre of IT professionals needed to man and operate the DII.

Insiders are DoD's first line of defense and also potentially the most dangerous cyber threat. The task force believes that the DepSecDef should mandate an innovative and effective security program for critical IT professionals to mediate this threat. Over 100,000 systems administrators provide a diverse and broad opportunity for our potential adversaries to find a weak link, possibly someone susceptible to blackmail or coercion. Additionally, a disgruntled systems administrator could, with high knowledge of internal computer and communications processes, cause very serious damage to the DII at the time most likely to inhibit DoD's ability to achieve its objectives.

The task force found that the DoD workforce at all levels is ill-prepared to execute the DIO mission because training efforts are fragmented, inadequately scoped, and poorly documented. Hence, the SecDef and Military Departments, among others, should establish policy to develop and implement formal Education, Training and Awareness (ETA) programs for DIO throughout DoD.

The task force addressed several policy and legal issues associated with DIO as well. Some of these issues cannot be meaningfully addressed solely within DoD, even though DoD will be affected by the outcome of the debate surrounding them. The task force divided the issues into sets including:

- Moving toward a common terminology. The way an issue is defined often clarifies or obscures the lines of authority for dealing with it. Consequently, definitions often

serve as surrogates for struggles over turf. DIO issues cut across numerous overlapping authorities and areas of responsibility, both in government and the private sector. The nation needs an authoritative document, perhaps an Executive Order, which provides common and unifying definitions for a wide range of concepts. Such a lexicon would be useful for clarifying legal matters, mitigating resource fights, and illuminating the public debate.

- The requirement for government-wide coordination. Today, coordinating the U.S. response to a broad Information Operations attack would fall to several disparate agencies and private organizations. A single "Commander in Chief (CINC)-like" organization is needed to recognize the implications of seemingly unrelated events in widely separated sectors, to coordinate national infrastructure "triage", and to ensure a coherent response from both government and industry. Some elements of this "homeland defense" are in place, but authorities are dispersed among government and civil elements, and are generally held in reserve for a more conventional emergency. A recognized national level, full-time point of contact is needed.

- Improving information sharing among agencies. The task force received mixed reports on the degree to which information is shared among the Defense, Intelligence, Law Enforcement, and other relevant communities. There are several reasons for this: the newness of the IA threat, differing perceptions on what information may and should be shared (for example, law enforcement, sensitive information or very sensitive intelligence sources,) "turf" protection, and legal or regulatory barriers. This issue warrants resolution early in the new administration, with agreement among the SecDef, the Attorney General and the Director of Central Intelligence

- Identifying and protecting critical infrastructure. DoD is increasingly reliant on a broad range of virtual infrastructure services provided by the private sector, municipal utilities, and other non-DoD sources. These dependencies have direct implications regarding the availability and reliability of DoD's GIG. To ensure a detailed assessment of potential risks inherent in these interdependent, underlying infrastructures, the Department should accelerate actions to identify critical infrastructure dependencies on the private sector; work with sector-lead agencies to ensure that its regulations are incorporated into the information-sharing processes with the owners and operators of critical infrastructures; and modify or develop a process to assess the fiscal impact of infrastructure impact.

Because so much of military infrastructure is also the civil infrastructure, the DoD, and in fact the nation, needs a national coordinator for Defensive Information Operations. Currently, there is a National Coordinator for Infrastructure Assurance and Counter-terrorism, but his office can do little beyond encourage cooperation. In a major crisis or attack on our critical infrastructures, decision-makers would quickly find that authorities to act and control resources are spread widely throughout government. A truly effective crisis response and proactive defense will require more coherence and concentration of authority. An individual with such authority does not necessarily have to reside within the country's national security apparatus but will have to tap into it through the National Security Council when necessary.

This DSB Task Force report provides a series of recommendations necessary for the successful implementation, execution, and protection of the Defense Information Infrastructure. The recommendations are presented in sections relating to: the implementation of an architecture consistent with the goals of Joint Vision 2010/2020, Research and Development of crucial technologies, Readiness of DoD forces, and Policy and Legal initiatives. While there is no hierarchy implicit in these four topics, recommendations pertaining to some will be easier and less costly. Others, like the architecture, will have the greatest impact, take the most time, and be the most expensive. Even so, it is only the successful integration of all of the recommendations that will provide the DoD with the Information Infrastructure needed to achieve the goals of JV2020.

Now is the time to make some hard decisions and invest the required significant resources. Successful information-intensive industries have shown us the way to embrace change. But the DoD challenge is more difficult: not only to embrace change, but also to build trust and security to a degree no business could afford. Like any other weapons system, if we design defenses today, as the GIG is becoming a reality, it will be expensive, but possible. If the Department waits, it will be impossible at any cost.

On the surface, this might seem simply as an endorsement of the current DoD GIG architecture. It is much more. Several years ago the DSB adopted and built upon work of the Army Science Board regarding a Joint Technical Architecture. Several DSB reports now have reiterated the clear need for DoD to *adopt* and *enforce* an architecture across DoD which would insure that the systems built by the services would be fully interoperable and secure. Newly identified critical needs for Information Assurance, coupled with DoD's new JV2020 *require* that the GIG be developed and operated like the critical weapons system it must become.

CHAPTER 1. INTRODUCTION

"The dogmas of the quiet past are inadequate to the stormy present. The occasion is piled high with difficulty, and we must rise with the occasion. As our case is new, so we must think anew and act anew." -Abraham Lincoln

1.1 Terms of Reference

In 1996, the Defense Science Board (DSB) completed a study of information warfare defense. In that study, the task force argued for greater DoD focus on the emerging information warfare threat and for specific changes in investment, organization and policy. The 1996 task force recommended that the Pentagon invest an additional $3 billion to strengthen defenses of its information networks. The Department accepted a number of the suggestions made by the 1996 task force, but technology has continued to evolve and significant investment shortfalls persist. With the Department's embrace of Web-based technologies, defensive information operations (DIO) are even more vital now than they were four years ago. The attached report and the supporting volume display today's state of affairs in defensive information operations and offer timely recommendations to meet current DIO needs.[1]

The terms of reference for this DSB task force are found in Appendix A. The task force was requested to accomplish two goals:

1. Evaluate the Department's response to the 1996 DSB task force on information warfare defense, to include:
   - What is the status of action on the recommendations?
   - Where there are shortfalls, what are the barriers to action and what should be done?
   - What important aspects did the 1996 task force miss that should have been addressed?
   - What recommendations of other important reports that have addressed information assurance issues should the Department consider?

2. Determine:
   - Adequacy of the process toward the information assurance goals needed to carry out Joint Vision 2020
   - Adequacy of the Department's readiness to project and sustain power in the face of information warfare attacks
   - The appropriate role(s) and capability of DoD to provide information assurance in support of Homeland Defense and in support of Critical Infrastructure Protection

[1] As defined by Defense Department Instruction 3600.1, Defensive Information Operations includes a broad range of issues such as operations security, electronic warfare countermeasures, counter-deception, counter-propaganda, counter-intelligence, computer network defense, etc. During the initial sessions of this DSB task force, it was agreed that the principal focus of its deliberations would be on information assurance and computer network defense.

- Recommendations for research and development which are uniquely in DoD's interest, and thus not likely to be accomplished by the private sector in the time required to meet DoD's defensive information operations objectives
- Areas in which DoD should seek strong partnering relationships outside DoD, such as with the Critical Infrastructure Assurance Office (CIAO)

1.2 Today's Threat Environment

The American Homeland is becoming increasingly vulnerable to non-traditional attack, including information warfare or information operations (IO), the focus of this report. Rapid advances in technology have and will continue to create new vulnerabilities and challenges to U.S. security. Within DoD alone, there are several operating systems and over 700 different software applications comprising between 50 and 100 million lines of code. New commercial-off-the-shelf (COTS) applications are implemented every day, and although some positive testing is performed to determine if the software will do what it is supposed to do, virtually no negative testing is done to determine what unanticipated capabilities may be imbedded in the software. Compound this situation with Murphy's Law, natural events, inadequate configuration controls, and general system fragility, and one realizes the vulnerability of the system upon which DoD depends today.

Recent studies by both the Government Accounting Office (GAO) and the Computer Security Institute found that the number of cyber security threats to both the government and the private sector is on the rise. The damage, both to physical infrastructures and to the psychological health of U.S. institutions that could be caused by a successful attack could prove immense, and the Department of Defense is not exempt from this danger. Examples of this threat are listed below:

- The Love Bug and Melissa viruses caused military units to take down e-mail service. This virus also spread to classified systems. The Joint Warfare Analysis Center (JWAC) was down for one week and Scott Air Force Base took four of fourteen e-mail servers off-line because of the virus. Furthermore, the Love Bug virus spread to a million computers, in the private sector in just five hours.
- The National Security Agency (NSA) conducted thirty-seven Red Team exercises during the last three and one-half years. Ninety-nine percent of those attacks went undetected. The Red Teams only used tools and techniques downloaded from the Internet. Since DoD has on the order of 10,000 networks with over 2,000,000 users, merely thirty-seven Red Team exercises are inadequate to assess the readiness or security of DoD networked systems.
- The ELIGIBLE RECEIVER exercise demonstrated how the Secure Internet Protocol Router Network (SIPRNET) could be compromised.
- Solar Sunrise was an incident brought about by two California teens and one Israeli teen. It occurred in February 1998, compromising 500 Domain Name Servers during the crisis with Iraq, and raised concerns of major asymmetric attack on logistics, medical and resource systems. Additionally, the average number of transmission "hops" was eight, making attribution extremely difficult and time consuming.

- The extent of potential damage from Moonlight Maze is unknown.

The Department is facing this non-traditional threat daily. The threat ranges from attacks by nation-states to attacks by groups of transnational actors and individuals. The task force finds that this threat is changing at a rate faster than that at which the Department is responding. In fact, there is a belief that the Department is not in a position to know when and to what extent its information systems have been attacked. The low and slow attack typically displays the following characteristics:

- The initial attack may go undetected for a long period of time, particularly if initiated or aided by an insider.
- Since there is not usually an immediate outcome from a low and slow attack, it is unclear what may have been left behind for later implementation. Potential insertions include logic bombs, trap doors, Trojan horses, and viruses that can be implemented at the time and place of the intruder's choosing.
- The motive for these attacks is also difficult to determine, since the outcome or ultimate execution of the attack may not come until months or years after the insertion.

There is a growing lack of confidence in the information network as well as in the integrity of the data contained therein. The information warfare threat applies to systems within and outside the borders of the United States. A perimeter defense philosophy is currently the predominant solution across DoD. The problem with this approach is that it leads to a strategy of risk avoidance rather than risk management. Perimeter defense does not equal defense-in-depth, as illustrated in Figure 1. Perimeter defense relies on an outer "barrier" that is intended to prevent unauthorized access to a network (top left Figure 1). Once the "barrier" is in place, authorized users must be given access - usually through passwords or other identifiers (top right Figure 1). As work progresses, secondary users are often identified and granted access on a temporary basis, or restricted to specific levels of data (bottom left Figure 1). Finally, due to operational need and "convenience" still others are granted access (bottom right Figure 1). The end result is a network that started out with the expectation of security, and ended up with no clear idea of who is really in the network. This "Swiss Cheese Effect" is a nightmare for network security personnel, as intruders gain access through stolen passwords, backdoors, data manipulation, and corruption of the system. In this regard, it is noteworthy that DoD has authorized over 100 "legitimate" accesses into the SIPRNET from the Non Secure Internet Protocol Router Network (NIPRNET).

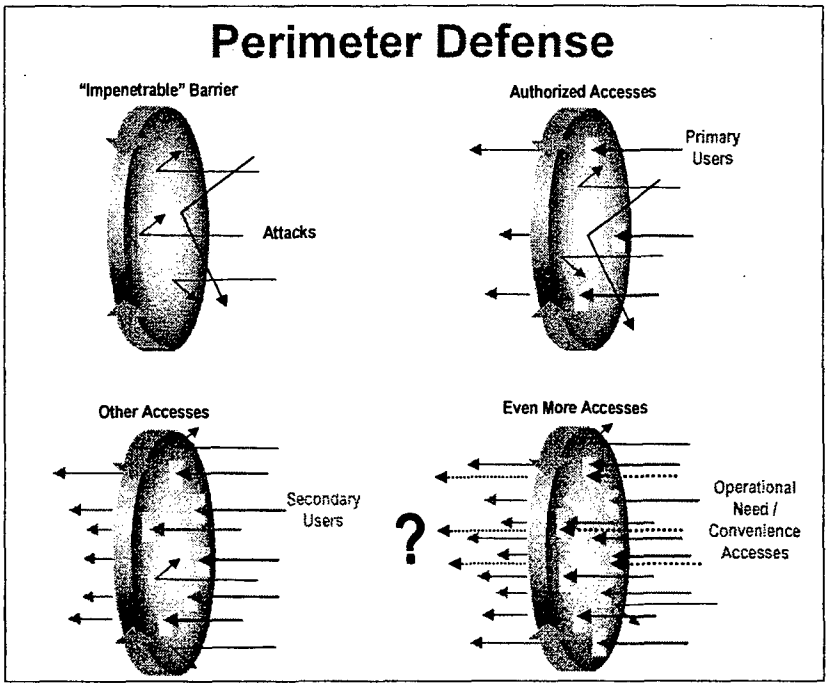


Figure 1. Perimeter Defense

Defense-in-depth uses a layered approach, with multiple firewalls, intrusion detection devices, and network security tools (see Figure 2). As intrusions are detected, intruders can be shut down, denied further access, tracked for future legal action, and/or counterattacked. The tolerance level, demonstrated by the left-most layer of Figure 2, represents those intrusions that may be unavoidable – often the insider threat. These are threats that must be managed. Consequence management requires back-up systems, redundancy, heightened awareness, integrity restoration, and recovery and reconstitution. These are the keys to graceful degradation rather than catastrophic failure.

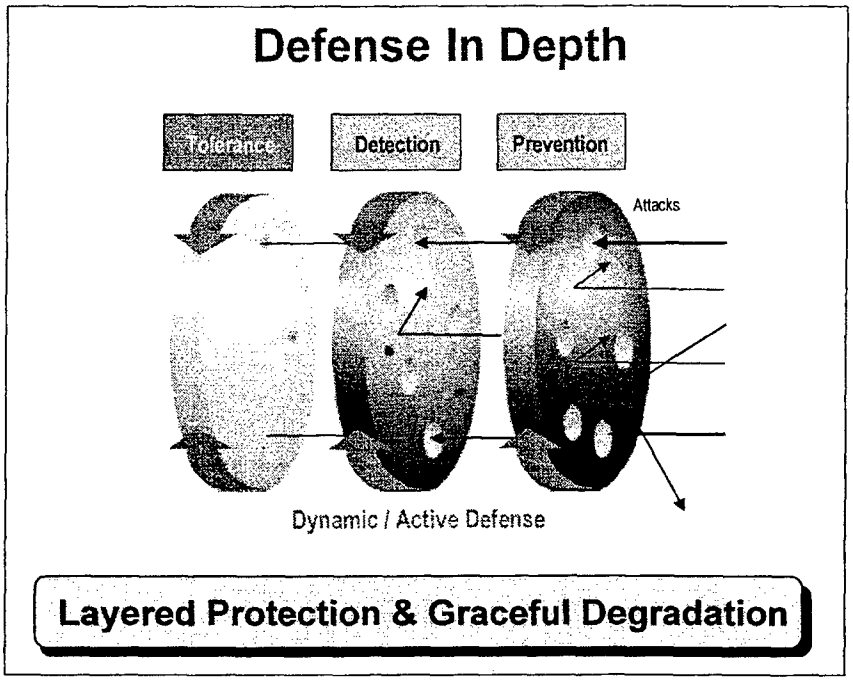


Figure 2. Defense-in-Depth

The potentially devastating impact of the insider threat warrants specific attention. As an example, there are currently between 100,000 and 125,000 system administrators in DoD alone. Consider the access these individuals have, making them the ultimate insiders, and making personnel reliability a critical factor. The Gartner Group published a report in October 1999, entitled "Information Security Hits the Front Page: How Safe Is Safe Enough?" One highly emphasized point throughout the report was the danger and likelihood of the insider threat. Figure 3 illustrates the group's conclusions.

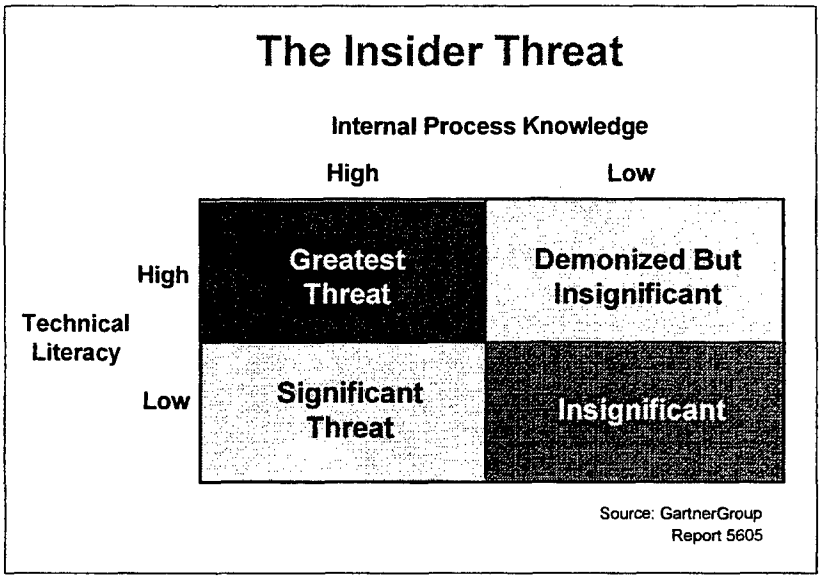


Figure 3. The Insider Threat

A person with low technical literacy and low internal knowledge is an insignificant threat (bottom right Figure 3). A person with high technical literacy and low internal knowledge can be a bother (demonized) but is insignificant (top right Figure 3). However, a person with low technical literacy and high internal knowledge (the "dumb" insider) is a significant threat (bottom left Figure 3). Finally, a person with high technical literacy and high internal knowledge (the "smart" insider) is the greatest threat (top left Figure 3). These insiders are potentially the most damaging threat, and the hardest to detect.

Finally, the threat pertains to information systems under the ownership of the U.S. Government as well as many that are not under such ownership but are critical to military success. This critical dependency implies that attacks on the commercial infrastructure may have significant impact on operations within DoD. The incidence of attacks is growing significantly in both areas, as illustrated in Figure 4.

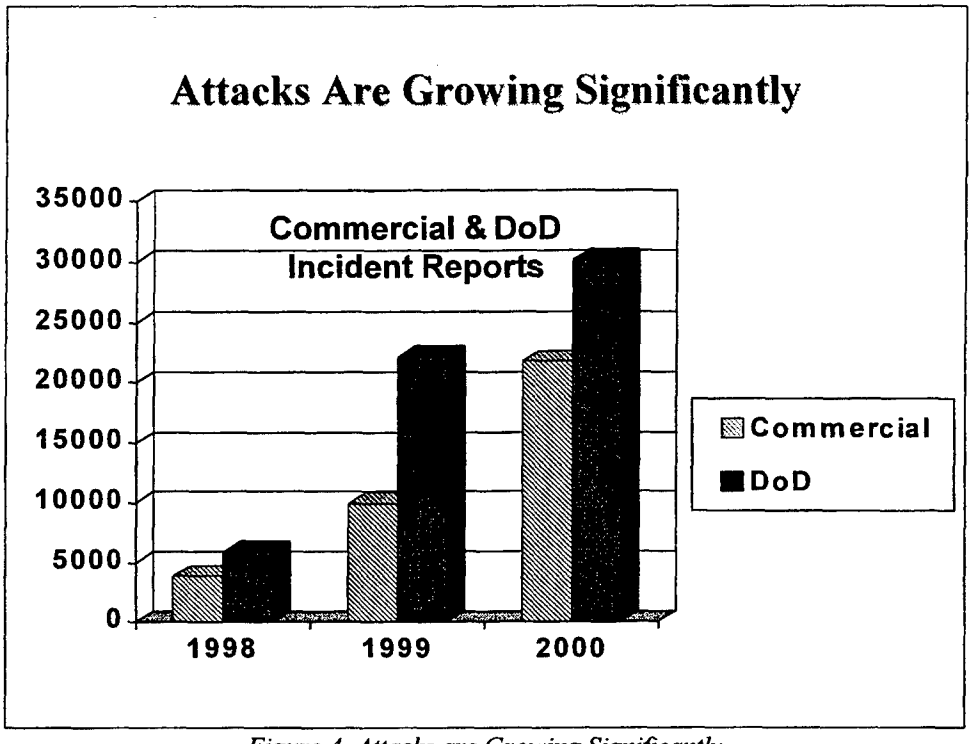


Figure 4. Attacks are Growing Significantly

The United States has thus far been fortunate not to have been attacked in such a way that its ability to plan, mobilize, deploy, and execute military operations in a crisis has been impaired. However, the use of Information Operations (IO) on both side during the Kosovo campaign and the more recent use of IO by the parties in the Mideast conflict provide insight into the broad spectrum of IO tools and techniques that are evolving. An October 26, 2000 article in the Washington Post makes the point:

> *"What distinguishes this cyber-conflict from past ones, such as last year's Kosovo war, is that it is not exclusively, or even mainly, a cat-and-mouse game of highly specialized hackers attempting to play havoc with one another's sites.*
>
> *Thousands of Israeli and Arab youngsters apparently have also joined in the contest, sending the other side nasty, racist, and occasionally pornographic e-mails and, within their own camps, circulating Web site addresses with simple instructions for how to ping, zap, and crash the enemy's electronic fortress.*
>
> *One aspect of cyber warfare we did not consider in previous discussions of Strategic Cyber Defense was its ability to empower the average citizen as a warrior. Much as the Internet has truly enabled freedom of speech, it has extended the military fighting force to every citizen with a computer. Now, just as the revolutionary war military consisted of every able-bodied male citizen who owned a gun, the Cyber Military may come to be seen as every able-minded citizen who owns a computer. (A true transition of the military to the information age?)"*

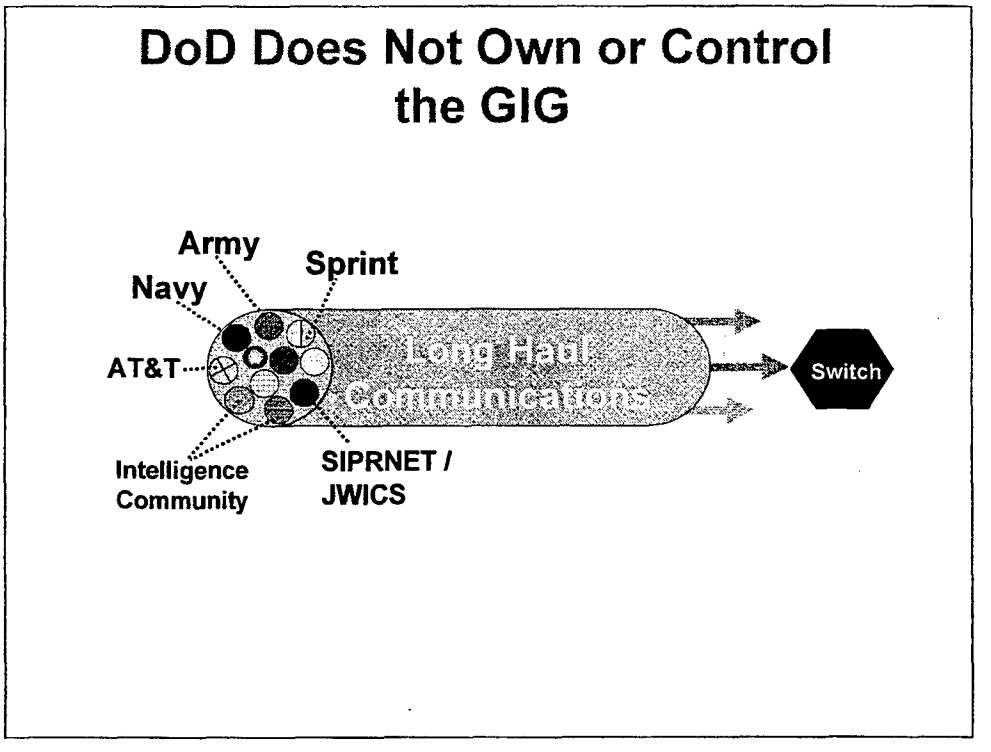


Figure 5. Long Haul Communications

At the same time as the number of our potential adversaries has increased, so has the vulnerability of Defense Department systems increased, in substantial measure the result of increased reliance on the private sector. More than 90% of DoD military communications ride on the commercial telecommunications backbone. DoD should not assume that the global commercial services on which it depends will be available, particularly if subjected to a technically advanced Information Operations threat, sponsored and empowered by a nation-state. "The Defense Department has more than 25,000 computer networks that handle everything from weapons systems command and control to inventory to payroll. Roughly 11% of Defense Department networks, such as satellite links, are considered mission-critical."[2]

1.3 Information Operations:

In many circles within the U.S. defense and broader international security community, the term *Information Operations* is increasingly being used to encompass a far greater set of information-age "*warfare*" concepts than was attributed to it in the past. These emerging new warfare concepts are directly tied to the prospect that the ongoing rapid evolution of cyberspace, the global information infrastructure, could bring both new opportunities and new vulnerabilities. At least one of these vulnerabilities is the prospect that the information revolution could put at risk high-value national assets outside the traditional battle space boundaries, very possibly inside the continental United States. This possibility will affect U.S. national security strategy, and thus U.S. military strategy. Assets that are critical to the conduct of military operations could also be put at risk, compounding this problem.

[2] NetworkWorld, 1/15/01

The spectrum of IO spans from peace, to crisis, to hostilities, and back to peace, and has characteristics actions and effects at the strategic, operational, and tactical levels. Many systemic issues arise when addressing this subject, as shown in Figure 6.

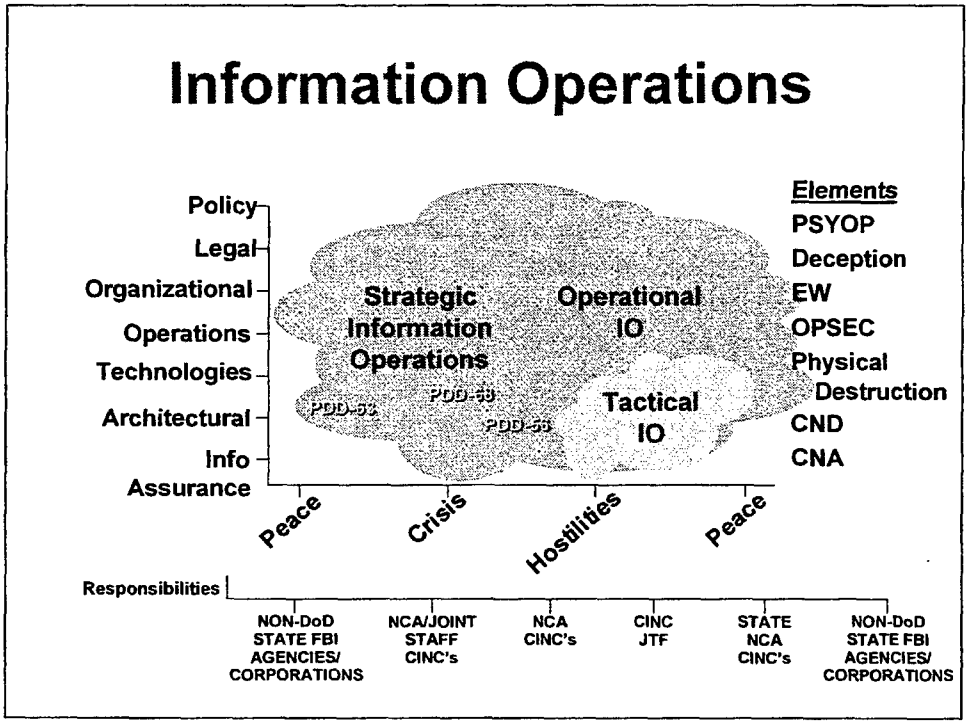


Figure 6. Information Operations Systemic Issues

Information Operations responsibilities cross the boundaries between DoD and non-DoD entities, and complicate the issues of authority, supervision, hand-off, response, and coordination. The task force addressed these issue areas in categories including policy, legal, organization, operations, technologies, architectures, and information assurance.

The concept of *Strategic Information Operations* warrants further identification and definition. In essence, this is the intersection of evolving information warfare and post-cold war "strategic warfare" concepts, and warrants special recognition and attention as a legitimate new facet of warfare, one with profound implications for both U.S. military strategy as well as overall U.S. national security strategy and policy.

A fundamental aspect of Strategic Information Operations is that *there is no front line.* Strategic targets in the United States may be just as vulnerable to attack as in-theater command, control, communications, and intelligence targets. As a result, there exists a need for broadening strategic understanding beyond the single traditional regional theater of operations to four distinct theaters of operation: 1) the battlefield, 2) the allied or regional zone of the interior, 3) the intercontinental zone of communication and deployment, and 4) the U.S. zone of the interior.

The post-cold war "over there" focus contained in the persistent emphasis on the regional component of U.S. military strategy has been rendered incomplete and is of declining relevance to the likely future international strategic environment. When responding to information warfare attacks of this character, military strategy can no longer afford to focus on conducting and supporting operations only in a region of concern. These changing concepts will, and should, drive DoD's concepts for Defense Information Operations.

What are the basic features of Strategic Information Operations as best understood today? The following represent a synthesis of observations about these basic features. There is, most definitely, a cascading effect inherent in these observations; each helps to create the enabling conditions for subsequent ones.

Low Entry Cost: Interconnected networks may be subject to attack and disruption not just by states but also by non-state actors, including dispersed groups and even individuals. Potential adversaries could also possess a wide range of capabilities. Thus, the threat to U.S. interests could be multiplied substantially and will continue to change as more complex systems are developed and requisite expertise is more widely diffused.

Cyber attacks have moved beyond the domain of the mischievous teenager and are now being learned and used by terrorist organizations as the latest weapon in a nation's arsenal. In June 1998 and February 1999, the Director of the Central Intelligence Agency testified before Congress that several terrorist organizations believed information warfare to be a low-cost opportunity to support their causes. Both Presidential Decision Directive 63 (PDD-63), issued in May 1998, and the President's National Plan for Information Systems Protection, version 1.0, issued in January 2000, call on the legislative branch to build the necessary framework to encourage information sharing to address cyber security threats to our nation's privately held critical infrastructure. [3]

Effective attribution and swift response to attacks would nullify the appeal of the low cost of entry by making the chances of "getting caught" much higher. Perceived increased risk by the attacker should be an added deterrent to preventing information warfare attacks.

Blurred Traditional Boundaries: Given the wide array of possible opponents, weapons, and strategies, it becomes increasingly difficult to distinguish between foreign and domestic sources of information warfare threats and actions. It may not be known who is under attack by whom, or who is in charge of the attack. This greatly complicates the traditional role distinction between domestic law enforcement, on the one hand, and national security and intelligence entities on the other.

Not only are borders becoming more porous, but they are also increasingly irrelevant in cyberspace. According to a long-time Central Intelligence Agency (CIA) operative and Federal Bureau of Investigation (FBI) consultant, "globalization and technology were lowering traditional boundaries between what constitutes an international or domestic threat, and terrorists, drug cartels, spies, and hackers were all leaping those boundaries with impunity." [4]

Expanded Role For Perception Management: Opportunities for information warfare agents to manipulate information that is essential to public perceptions may increase. For example, political action groups and other non-government organizations can use the Internet to galvanize

---

[3] Statement of Representative Tom Davis on the Introduction of The Cyber Security Information Act of 2000, April 12, 2000.

[4] John McGaffin, in Covert Attack, by James Kitfield, National Journal, September 16, 2000 p. 2858.

political support, as the Zapitistas in Chiapas, Mexico, were able to do. Furthermore, the possibility arises that the very "facts" of an event can be manipulated via multimedia techniques and widely disseminated. Conversely, there may be decreased capability to build and maintain domestic support for controversial political actions. One clear implication is that future U.S. administrations may include a robust Internet component as part of any public information campaign.

Lack Of Strategic Intelligence: For a variety of reasons, traditional intelligence gathering and analysis methods will be of limited use in meeting the Strategic Information Operations challenge. Collection targets will be difficult to identify using existing national technical means; allocation of intelligence resources will be difficult because of the rapidly changing nature of the threat; and vulnerabilities as well as target sets will not be well understood. In sum, the United States may have great difficulty identifying potential adversaries, their intentions, and their capabilities.

Difficulty Of Tactical Warning And Attack Assessment: Warning and attack characterization/assessment involving information warfare presents fundamentally new problems in a cyberspace environment. A basic problem exists: distinguishing between attacks and other events such as accidents, system failures, or hacking by thrill-seekers. This challenge is exacerbated by the speed of events in cyberspace. The main consequence of this feature is that the United States may not know when an attack is underway, who is attacking, or how the attack is being conducted.

Difficulty With Building And Sustaining Coalitions: Many allies and coalition partners will be vulnerable to information warfare attacks on their core information infrastructures. For example, the dependence on cellular phones in developing countries could well render telephone communications in those nations highly susceptible to disruption or deception. Other sectors in the early stages of exploiting the information revolution, such as the energy or financial sectors, may also present vulnerabilities that an adversary might attack to undermine coalition participation. Such attacks might also serve to sever weak links in the execution of coalition plans.

Vulnerability of the United States Homeland: As stated earlier, information warfare has no front line. Potential battlefields are anywhere networked systems allow access. Current trends suggest that the United States economy will rely on increasingly complex, interconnected network control systems for such necessities as oil and gas distribution management, electric grids, telephone service, air traffic control and much, much more. The vulnerability of these systems is currently poorly understood. This lack of understanding and recognition inhibits a thorough assessment of the vulnerabilities that may exist in both the technology-driven control systems and in the fiscal marketing processes that can directly impact energy distribution systems. In addition, the means of deterrence and retaliation are uncertain and may rely on traditional military instruments in addition to information warfare threats. In summary, the United States homeland may no longer provide a sanctuary from outside attack.

1.4 Joint Vision 2020 and the Importance of Information Assurance

The Department has outlined a vision of the future – Joint Vision 2020 (JV2020). JV2020 builds upon and extends the conceptual template established by Joint Vision 2010, which guides the continuing transformation of America's Armed Forces.

The primary purpose of those forces has been and will be to fight and win the nation's wars. The overall goal of the transformation described in JV2020 is the creation of a force that is dominant across the full spectrum of military operations – persuasive in peace, decisive in war, preeminent in any form of conflict. The overarching focus of this vision is full spectrum dominance – achieved through the interdependent application of dominant maneuver, precision engagement, focused logistics, and full dimensional protection (see Figure 7).

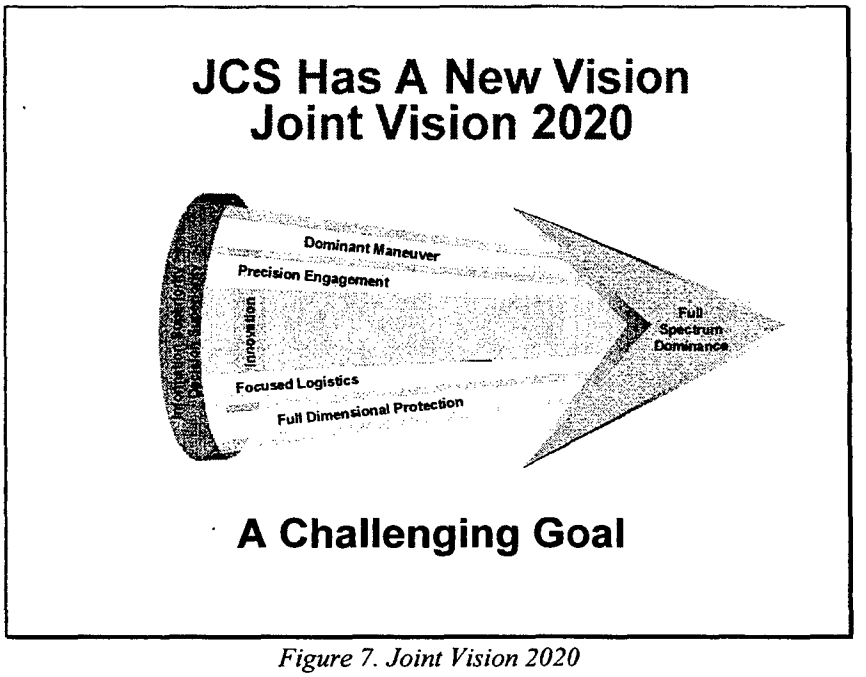


Figure 7. Joint Vision 2020

The evolution of these elements over the next two decades will be strongly influenced by two factors. First, the continued development and proliferation of information technologies will substantially change the conduct of military operations. These changes in the information environment make information superiority a key enabler of the transformation of the operational capabilities of the joint force and the evolution of joint command and control. Second, the U.S. Armed Forces will continue to rely on a capacity for intellectual and technical innovation. The pace of technological change, especially as it fuels changes in the strategic environment, will place a premium on our ability to foster innovation in our people and organizations across the entire range of joint operations. The overall vision of the capabilities required in 2020, as introduced above, rests on the assessment of the strategic context in which U.S. forces will operate.

Information, information processing, and communications networks are at the core of every military activity. Throughout history, military leaders have regarded information superiority as a key enabler of victory. However, the ongoing "information revolution" is creating not only a quantitative, but also a qualitative change in the information environment that by 2020 will result in profound changes in the conduct of military operations. In fact, advances in information

capabilities are proceeding so rapidly that there is a risk of outstripping our ability to capture ideas, formulate operational concepts, and develop the capacity to assess results.

The ability to achieve information superiority is a pacing item in realizing the goals of Joint Vision 2020. The inadequacies of current service information infrastructures prevent commanders from realizing the full benefit of the current family of intelligence, surveillance, and reconnaissance (ISR) systems – space-based, airborne, or surface – much less profiting from advances in sensors and weapons. Because of uncertainties regarding the availability of crucial information when needed, commanders are driven to develop unique, local-only Reconnaissance, Surveillance, and Target Acquisition (RSTA) systems. Overall, this tendency has resulted in redundant investment in, and proliferation of, "stovepipe" communication and sensor systems. As shown below, there are many interdependencies among force elements, with information systems being the glue that holds such elements together (Figure 8).

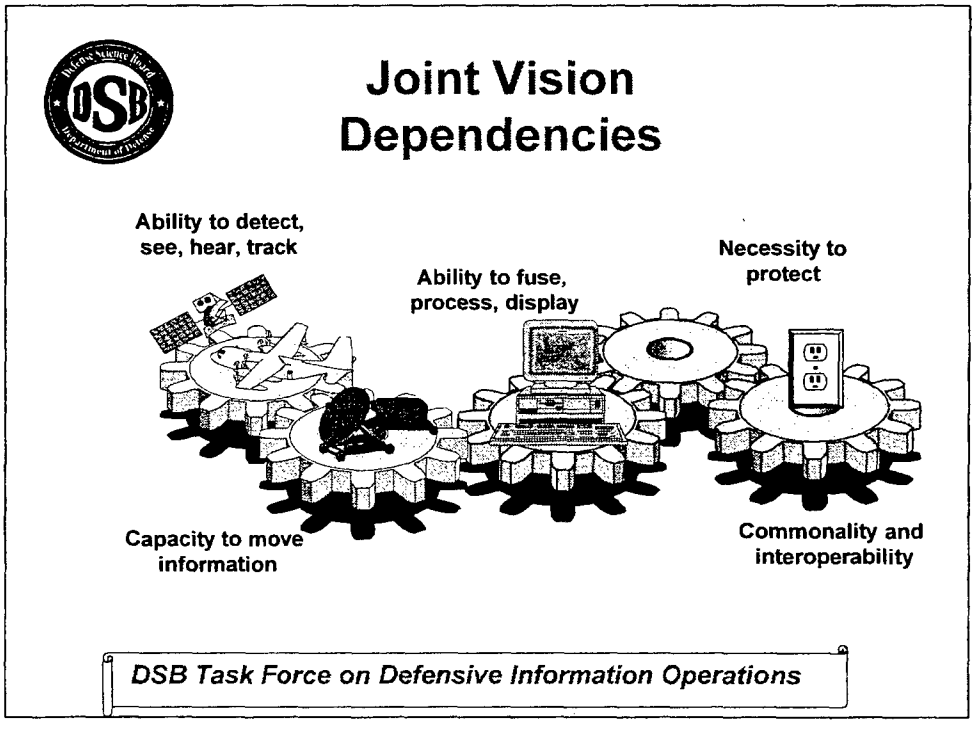


Figure 8. Joint Vision Dependencies

Increasingly, the Armed Forces are shifting to an operational concept wherein surveillance and targeting sensors are separated physically from the command node location, which in turn may be remote from the weapons launch platform. In the case of air platforms, for example, no longer will the sensors, commander (pilot), and weapons necessarily be collocated in a single aircraft. Further, third party targeting data sources and weapons magazines are proliferating. Examples of this evolving trend appear in such concepts as forward pass, cooperative engagement capabilities (CEC), the arsenal ship, and the transfer of tactical situation data derived from a variety of off-board sources directly into cockpits.

This evolution promises major improvements in the tactical flexibility and combat effectiveness of forces. The realization of this promise is not without challenges, however. The operational concept is inhibited by the inadequacy of the traditional military communication and information-services infrastructure as well as continuing interoperability problems between military services and between such systems within a given Service.

Information Superiority has qualitative and quantitative aspects as noted by the United States and North American Treaty Organization (NATO) allies experience in the recent Kosovo engagement. During those operations, the United States maintained a substantial information advantage over Serbia. Yet the successful prosecution of the mission appeared hampered in several respects: the ability of the Serbian forces to operate within NATO's observe, orient, decide, act (OODA) loop and the ability of the Serbian forces to successfully hide and protect their tactical field forces from NATO bombing.

This experience raises the question of whether information superiority as defined relative to the adversary is adequate. Instead, a different threshold of information appears to be needed – one based upon the rules of engagement used and other external constraints such as the unwillingness to accept any U.S. or allied casualties. Additional constraints, such as weapons and tactics, impose a further increase in the required information. Thus the information required for the United States to successfully prosecute a mission can be much greater than the information needed by the adversary. This concept is demonstrated in Figure 9. As illustrated, the United States may have tremendous superiority over the adversary in information, yet still not meet the level required to execute the mission. The adversary operating with a different objective and rules may be able to counter the U.S. initiative with far less information at its disposal.

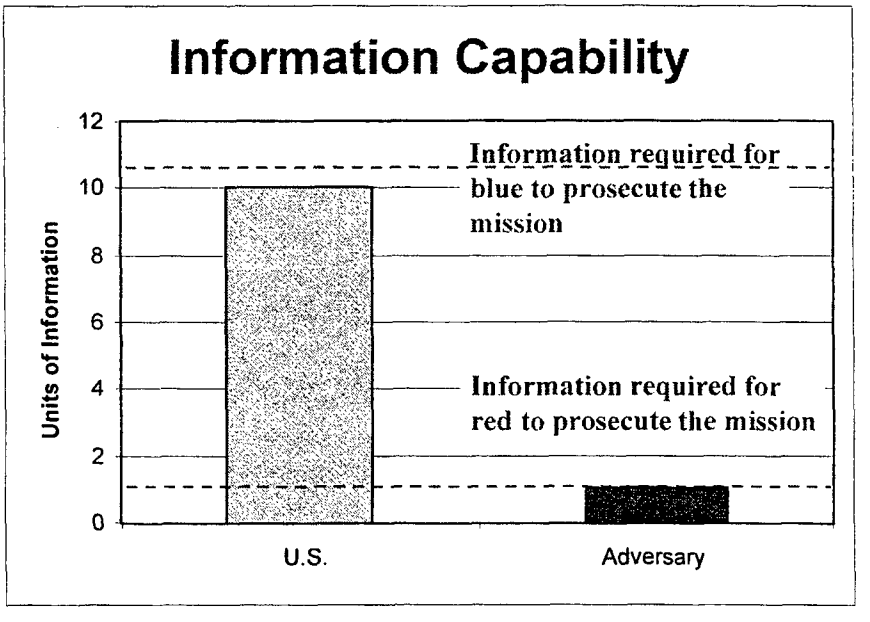


Figure 9. Information Needed to Prosecute the Mission

Since JV2020 is the driver for emerging technologies, capabilities, and operational concepts shaping defense capabilities in the 21st century, this task force raises several overarching questions:

- What is the cost of an Information Infrastructure that must provide information and decision superiority at the time and place of our need, when our adversary is likely to establish the time and place of conflict?
- Will our command, control, communications, computers, intelligence, surveillance and reconnaissance (C4ISR) capabilities provide critical information at precisely the right time to the command element needing it? Our Kosovo experience highlights the daunting nature of such tasks.
- Can we assure both the availability and integrity of critical information in a coalition environment with a high data rate and a dynamic information exchange with our allies of the time: given that such an environment is likely for most future conflict?
- What would be the impact or effect of not having information superiority and decision superiority in a particular circumstance:
  - Might the United States not achieve its objectives?
  - Would there be an unacceptable loss of casualties or resources?
  - Would DoD conclude that its courses of action were constrained?
  - Might our forces be structured for the wrong conflict?

If the nation actually requires DoD to achieve its military objectives at a specific time and place, the cost will be very high to assure success. The Department must design the force structures to include those information systems and networks essential for success, and such information and capabilities must withstand an attack by a creative adversary.

1.5 Progress Since the 1996 DSB Task Force on Information Warfare Defense

1.5.1 Status of the 1996 DSB recommendations

Figure 10 below summarizes the status of implementation by the DoD of the recommendations made by the DSB in its 1996 study. A more detailed portrayal of the current status is found in Appendix D. In most cases, though the understanding of the problem is greater now, the goal post has moved substantially since the 1996 report and there is a need for greater attention and investment. Color Codes are "stop light" assessments:

Green = Substantial progress

Yellow = Some progress – but much remains to be accomplished

Red = Inadequate progress – serious shortfalls

Current Status of 1996 DSB Recommendations

1996 Recommendation	Current Status	Remarks
1. Designate an accountable IW focal point	GREEN	ASD(C3I) designated as focal point (with many other organization s formed since then). Funding has been added, but not at the leve l recommended in the 1996 report (< half).
2. Organize for IW-D	YELLOW	Initial effort was the set -up of NSIRC, JTF -CND, GNOSC, DoD CERT (with minimal/insufficient funding). The recommendation was for plus-ups averaging $50M per year across a range of areas. Actual funding has been in the range of $2M per year across the same areas. CINCSPACE funding for CND mission is lagging two years behind assumption of the mission. DoD Red Team not yet formed or funded.
3. Increase awareness	YELLOW	Former DEPSECDEF was strong proponent / Eligible Receiver raised awareness. Funding is still approximately 1/10th of what was recommended in 1996.
4. Assess infrastructure dependencies and vulnerabilities	RED	CIP analyses and assessments are a beginning. Funding is approximately 1/10th of what was recommended in 1996. JPO funding cuts have resulted in downsizing that activity, directly affecting the study to determine key sites for future assessment . Dependencies and vulnerabilities have grown dramatically
5. Define threat conditions and responses	YELLOW	Definition of INFOCONS provided a good start. Revisions to CJCSM 6510.01 are still pending.
6. Assess IW-D readiness	RED	CJCSI 6510.04 (IA Readiness Metrics) issued 15 May 2000. Not yet enforced or included in monthly readiness reporting. IWD (or DIO now) yet to be operationalized in DoD.
7. Raise the bar with high-payoff, low-cost items	YELLOW	PKI is a very positive step (the PKE bill may hinder actual employment). Detection of insider threat should be a high priority. As much as $500 million above FYDP needed.
8. Establish and maintain a minimum essential information infrastructure	RED	Y2K provided a unique opportunity for assessment and for information sharing, but DoD still does not have a clear picture of what comprises a minimum essential information capability. The restoration process is also an issue -- it is understood by the communications community, but not carried over to the IT community. No significant funding has been applied to this area (1996 report recommended a $100M per year effort).
9. Focus the R&D	YELLOW	Primary efforts are in NSA-IA and DARPA (although the majority of the money goes to pay salaries). Existing R&D is focused on perimeter defense technologies. Substantial additional R&D funds are required.
10. Staff for success	YELLOW	IA Mobile Training Teams, training and certifications are on the rise. Funding remains <1/2 of what was recommended. Retention of trained individuals is also a major issue.
11. Resolve the legal issues	RED	Legal issues remain unresolved and significant.
12. Participate fully in critical infrastructure protection	YELLOW	The understanding of what constitutes CIP is much broader today than it was five years ago. There is still much work to do in identifying key information, the infrastructure that passes it, and the true vulnerabilities that exist.
13. Provide the resources	RED	Bottom line - the money is not there, and asking the Services to take it out of hide will not work.

Figure 10. Current Status of 1996 DSB Recommendations

1.5.2 Findings Regarding Current Capability

Figure 11 shows this task force's assessment of the current capability of the United States and its military in the five critical capabilities needed for effective Defensive Information Operations.

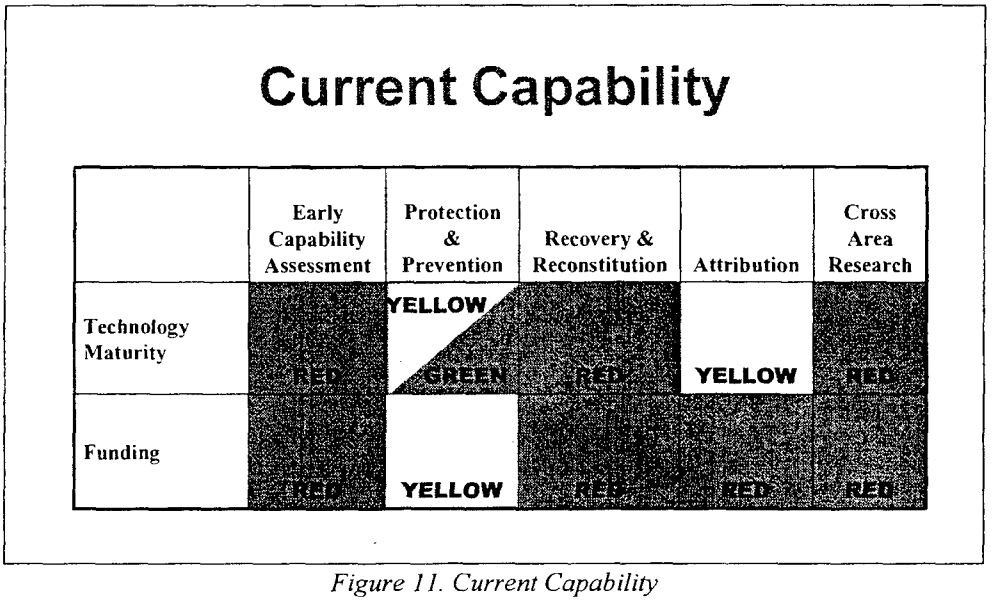


Figure 11. Current Capability

1.6 Current Defensive Information Operations Issues

This figure illustrates that significant research and development remains to be funded and executed to achieve minimal capabilities to detect, protect, respond and reconstitute Department of Defense networked systems.

This DSB task force identified a series of issues, which are crucial to understanding the Department of Defense Posture for Defensive Information Operations. They include:

- JV2020 sets a high standard for achieving Information Superiority,
- Defensive Information Operations (DIO) are critical "go to war" capabilities – DoD must have confidence in its information and the technology that provides it.
- DoD cannot currently measure and assess the readiness of its information infrastructure. DoD also lacks a clear set of definitions, policies, procedures, standards and management structure to implement DIO.
- DoD does not have a viable way to exchange DIO information throughout the U.S. government.
- DoD has no methodology for restoring integrity in its systems.

- DoD cannot currently accomplish the DIO mission.
- JV2020 is unachievable unless DoD builds protection and interoperability into the combat infosphere.

This task force believes the Department and the nation must do more. The discussion that follows outlines specific recommendations in this regard. Chapter Two looks at the needed architecture, while Chapter Three addresses necessary technologies to achieve effective information assurance. Chapters Four and Five focus on issues related to human resources and readiness, as well as the legal and policy roadblocks the Department faces in trying to implement its Defensive Information Operations mission.

CHAPTER 2. BUILDING AN EFFECTIVE SECURITY ARCHITECTURE

"He that will not apply new remedies must expect new evils." -Francis Bacon

2.1 Summary

The Integrated Information Infrastructure (III), a vision developed for the Department of Defense (DoD) by the Defense Science Board (DSB), is now the foundation of many DoD information infrastructure initiatives. The III sets goals and directions for DoD-wide information services that will be developed from private-sector information technologies.

The first phase in the realization of the III will be the implementation of the Global Information Grid (GIG). The GIG will globally interconnect information capabilities, automated processes, and personnel for collecting, storing, processing, managing, and disseminating information on demand to warfighters, policy makers, and supporters.

The GIG will comprise multiple virtual data networks worldwide that use shared, commercial communications media and information technologies. However, the DoD will not own or control the GIG. Furthermore, the GIG will offer virtually no protection against insider threats, especially to tactical networks. No centralized authority over budgets and execution activities exists. A new organizational structure with a centralized, primary point of responsibility is needed.

The DSB task force recommends an information assurance (IA) reference model that assumes the use of internet protocols in a wide range of environments (including tactical and strategic). It parallels the International Organization of Standardization reference model, with the substitution of a middleware layer for the presentation layer, and is consistent with the Transmission Control Protocol/Internet Protocol (TCP/IP) suite. The task force also recommends a series of IA system architecture strategies:

- The use of a consistent architectural framework and metrics across the entire DoD GIG
- Segmentation of the user communities and investment in Public Key Infrastructure (PKI) and Public Key Enabled Applications (PKE) as well as high-speed, in-line encryption
- The establishment of a DoD-wide GIG IA testbed
- More stringent qualification of suppliers of GIG IA technologies
- Investment in a focused R&D program to address the IA needs of the GIG

In particular, the DSB task force recommends the following measures to support IA over the GIG:

- A uniform layered-defense, or defense-in-depth (DID) architecture

- IA functions in the hosts of the GIG, including host-based intrusion detection and response, end-to-end security, domain name system security (DNSSEC), and malicious and mobile code eradication
- Secure network management capabilities
- Adoption of PKI/PKE including deployment of a Level 4
- Link encryption at the physical layer
- An ISO-like reference model with commercial protocols (e.g., Internet Protocol Security (IPsec) for end-to-end protection)
- Fine-grained control of access to computers and communication resources
- Features to counter insider attacks and support survivability
- Features to counter denial of service and enable attribution
- Measures of merit or metrics for IA and survivable architectures, for technical, system, and mission-level evaluation

The GIG will incorporate a number of commercial wireless technologies, which are discussed in detail. The security of wireless networking is essential to the performance of the GIG. Attacks on wireless systems can take the form of interception, denial of access locally and system-wide, and disruption of the entire network.

Although these commercial technologies are attractive and at first glance seem to be infrastructure independent, they are in fact vulnerable extensions of a vulnerable infrastructure. These vulnerabilities must be carefully analyzed and understood, and protection measures must be carefully designed.

Other recommendations include the use of correlated multi-layered Intrusion Detection System (IDS) data as inputs to intelligence-enabled tracing systems and modus operandi detectors.

For the implementation of the above strategies, the task force recommends the formation of a DoD Board of Directors for Information Superiority, and that this Board create an advisory group under Federal Advisory Committee Act Regulations, or as a permanent DSB panel, consisting of senior private-sector IT leaders.

The Board should also create an Executive Office whose director will be responsible for leading the implementation of the DoD-wide common user internetwork on behalf of the Board. The Director's primary responsibility will be to deliver the GIG.

2.2 The Integrated Information Infrastructure

The III vision sets goals and directions for DoD-wide information services that will come about through the exploitation of private sector IT, to include associated IA technologies. The III then sets both a long-term vision and a road map for the evolution of the DoD infrastructure. Figure 12 provides a conceptual view of the III.

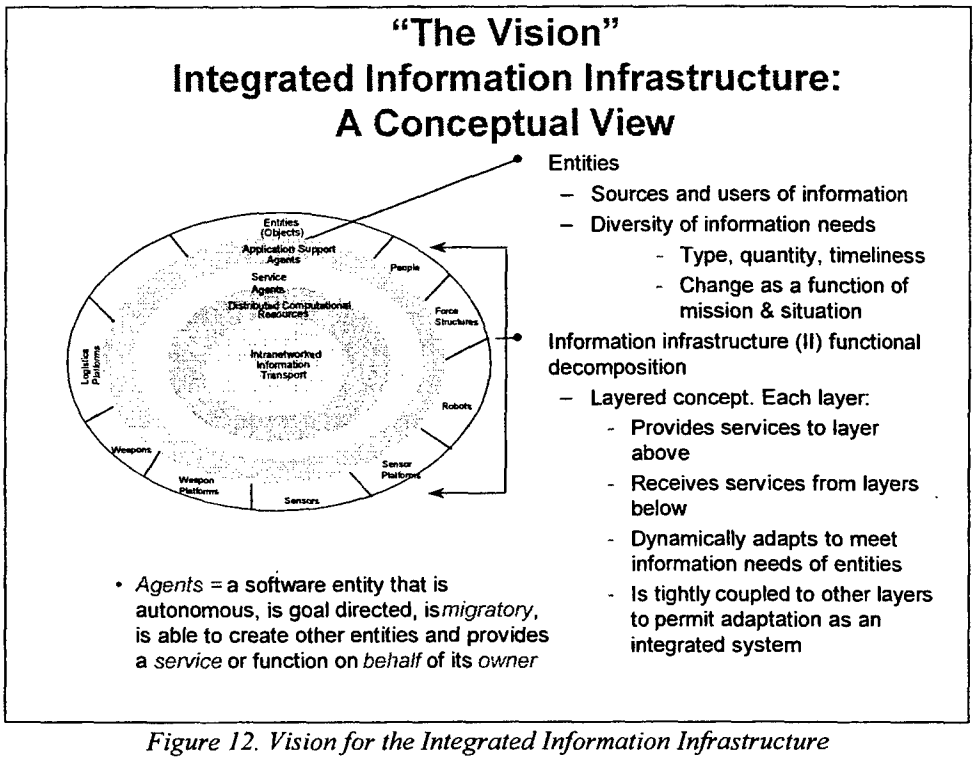


Figure 12. Vision for the Integrated Information Infrastructure

To realize the potential benefit of this new concept, the future information infrastructure must be capable of reliable, secure transmission, storage, retrieval and management of large amounts of data. Today, all systems are segmented into communications links, computers, and sensors that in turn are stovepiped to support specific functions (e.g., intelligence, logistics, or fire control). Furthermore, these component entities are now constrained by a lack of (1) the bandwidth necessary for high-resolution imagery transfer; (2) the processor capacity needed for target recognition and interpretation; (3) memory sufficient to handle massive amounts of archival data; and (4) software to search the many data repositories quickly in order to provide commanders with tactical information in a timely manner. These constraints are magnified by difficulties in integrating a myriad of legacy information systems with newly developed, service-unique stovepipe and joint systems. These limitations can be overcome, and the full capability of joint forces realized, if the goal is to integrate all military command, control, communications, computers, intelligence, surveillance, and reconnaissance (C4ISR) systems into a ubiquitous, flexible, interoperable C4ISR system of systems – the Integrated Information Infrastructure.

The Integrated Information Infrastructure must meet several key requirements if it is to realize its potential to enable future combat operations to support a wide spectrum of missions, threats, and environments. As stated in Joint Vision 2020, a military force must be able to receive or transmit all of the information it needs for the successful and efficient prosecution of its mission, from any point on the globe, in a flexible, adaptive, reconfigurable structure capable of rapidly adapting to changing operational and tactical environments. The information infrastructure must support these needs, while allowing force structures of arbitrary composition to be rapidly formed and fielded. Furthermore, the infrastructure must adapt to unanticipated demands during crises, and to stress imposed by adversaries.

The infrastructure must allow information to be distributed to and from any source or user of information at any time: its architecture must not be constrained to support a force-structure (enterprise) hierarchy conceived *a priori*. Most importantly, the information and services provided to an end user through the infrastructure *must be tailored to the user's needs, and be relevant to the user's mission, without requiring the user to sort through volumes of data or images*.

The information infrastructure must include multimode data transport including land-line, wireless, and space-based elements. All of these media must be integrated into a ubiquitous, store-and-forward data internetwork that dynamically routes information from source(s) to destination(s), transparently to the user. This data transport segment of the infrastructure must be self-managed, be adaptive to node or link failure, and provide services to its users based on quality-of-service (QoS) requests. These services include bandwidths, latency, reliability, security, precedence, distribution mechanisms (point to point, point to multipoint), and the like.

The infrastructure interface will link the user to a distributed processing environment that includes all types of computers situated at locations appropriate given their needs for power, environment, and space. This distributed computing environment will be integrated via the transport component of the infrastructure, thus enabling these processors to exchange data dynamically, share computation loads, and cooperatively process information on behalf of and transparent to the user.

The infrastructure should be an adaptive entity that integrates communication systems, computers and information management resources into an intelligent system of systems. Each component of the III will exchange state information with each other, in order to enable the entire infrastructure to adapt to user requirements and any stresses imposed on the network by an adversary. This adaptability will also enable the infrastructure to change its scale as necessary to support force structure(s) of arbitrary size, or to incorporate new processing, network, and communication technologies as they are developed. Thus, this infrastructure is a scaleable computing environment.

The information infrastructure must provide tailored information services to diverse users ranging from a single person to a collection of people, sensors, and/or weapons by means of intelligent agents – software entities, under the general control of the user, that are goal directed, migratory, and able to create other software entities, and provide services or functions on behalf of the user.

Each user will be served by one or more intelligent software agents that *proactively* provide and disseminate appropriately packaged information. These agents will perform such functions as fusing and filtering of information, and delivering *the right information to the right user at the right time*. They will be proactive in the sense that they are aware of the user's situation and needs, and will provide information relevant to those needs without a specific user request.

These agents will multiply the personnel resources available to combat units by gathering and transforming data into actionable information to support unit operations, just as unit members would have to do were the software agents not provided. Warfighters will therefore be freed of routine chores in favor of actual operations.

To the maximum extent feasible, the infrastructure's transport layer will take advantage of commercial technology and networks, by utilizing open-systems standards and protocols, and will minimize the use of service or function-unique hardware and software. For applications where military-unique capabilities (such as antijam, low probability of intercept, spread-spectrum waveforms and the like are required), military products will be developed or adapted to interface with the overall architecture.

As the Department moves towards the realization of the III vision, it will enable, over time, the following military capabilities:

- Geographic separation and functional integration of command, targeting, weapons delivery, and support functions
- Support for split-base operations, force projection, information reachback, combat, and force protection for units large and small
- Common situational understanding, common operating picture, and informed and rapid decision-making for joint forces
- Enhanced operational flexibility for commanders at all levels
- Reduced logistics footprint in immediate combat area
- Full exploitation of sensor, weapon, platform and processing capabilities
- Real-time or near real-time responsiveness to commanders' requests for information, fire support, and urgent logistics support

2.3 The Global Information Grid

The first phase for realizing the III is the implementation of the Global Information Grid (GIG). The GIG will incorporate near-term information technologies to provide the warfighting capabilities noted above. The GIG will, over time, evolve into the longer-term vision for the III. As the United States proceeds to implement and secure the GIG, it must keep the evolution toward the III in mind. The near-term vision is shown in Figure 13.

Today's communication infrastructure is highly entwined, with many misunderstood capabilities and limitations – *and a false sense of security*.

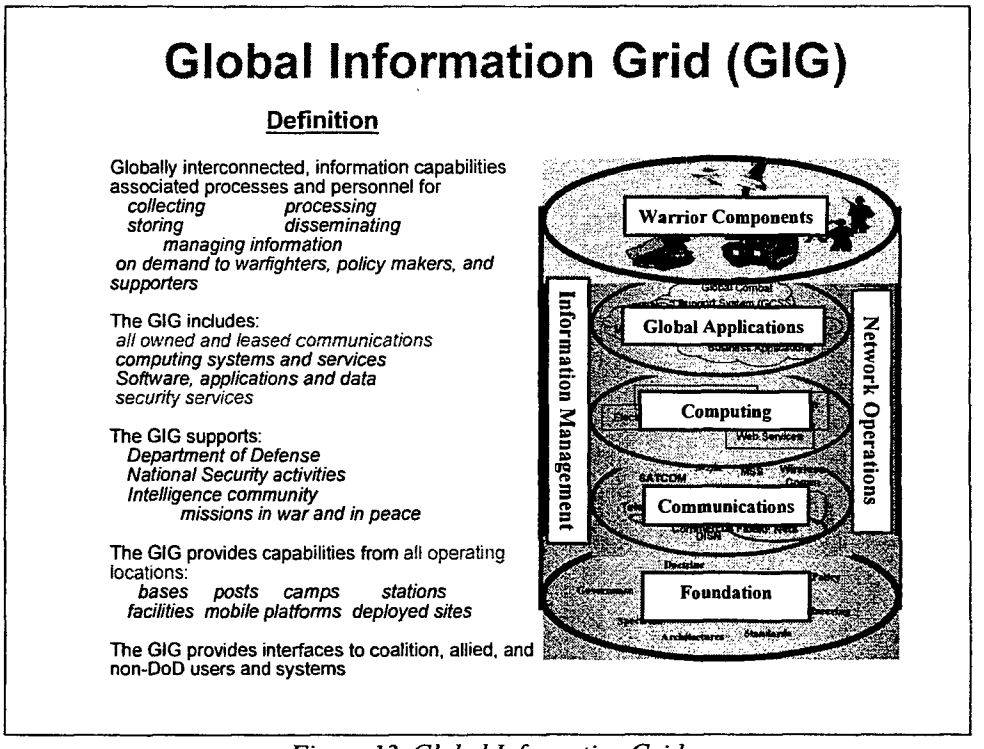


Figure 13. Global Information Grid

Long-haul communications are one clear example. Multiple users may think they have a "unique circuit" when in fact, they are only sharing a fiber or a part of a larger fiber optic cable. Assumptions of privacy, dependability, and assured service are often faulty. In most cases, these long-haul communications merge into a distribution switch that further routes the signal to its destination – making the switch a potential single point of failure. DoD no longer controls many "military only" circuits, but is instead highly dependent on the civilian backbone communications.

2.4 An Effective Information Assurance Architecture

Figure 14 provides a summary of this task force's findings regarding an effective information assurance architecture. The Global Information Grid will comprise multiple virtual worldwide data networks, the Non Secure Internet Protocol Router Network (NIPRNET), Secure Internet Protocol Router Network (SIPRNET), Joint Worldwide Intelligence Communications System (JWICS) and Service tactical Command, Control, Communications and Intelligence (C3I) systems. These networks use shared commercial communications media and commercial information technologies. In addition, all are cryptographically segmented into virtual networks. However, the task force noted that there is virtually no protection against the insider threat, especially for the classified networks. All Services are adopting a defense-in-depth (DiD) strategy, with different implementations. For example, the Air Force is employing a different strategy from the Army: a different protocol translation architecture; a different location for performing enclave level intrusion; and different measures for enclave access control. While there is a general framework for implementing DiD, there is no engineering discipline that allows for design of a DiD solution that provides confidence in security against a variety of attacks.

The current emphasis on information assurance metrics is focused on readiness and is not addressing the metrics needed to assess and measure mission, system or technical level performance. In addition, denial of service measures and attack attribution metrics are not well addressed.

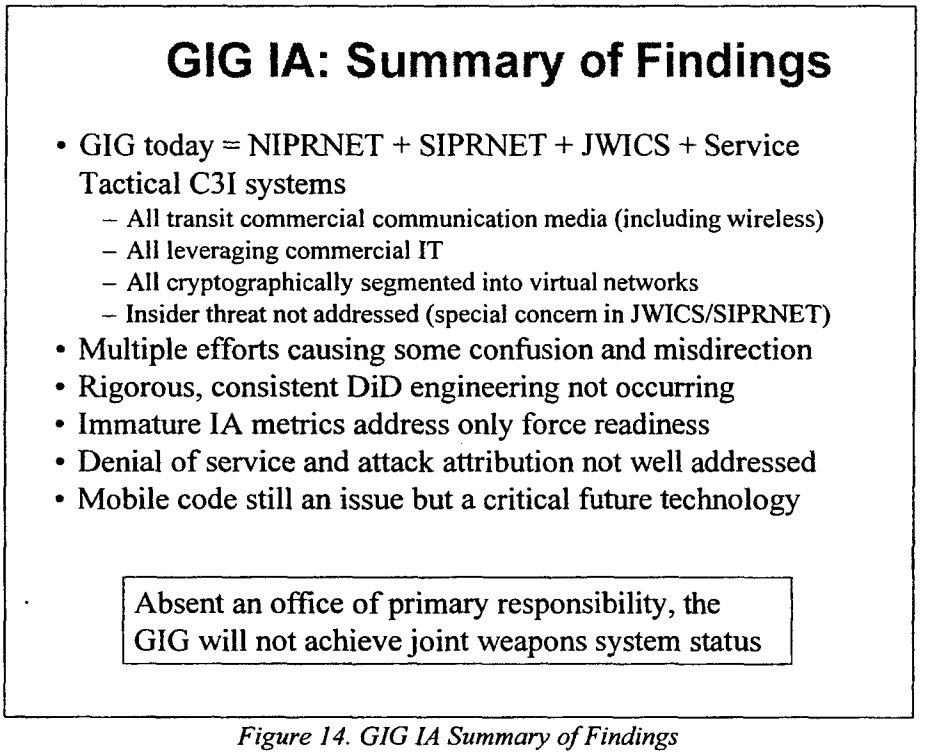


Figure 14. GIG IA Summary of Findings

Finally, the task force believes that today's DoD organizational structure is inadequate to deliver a GIG. Although both the DoD Chief Information Officer (CIO) Executive Panel and the Military Communications and Electronics Board (MCEB) are working on defining and providing guidance for the GIG, the task force believes that a new organizational structure, with a centralized primary point of responsibility, will be required to develop a GIG worthy of weapons system status.

Neither the DoD CIO Executive Board nor the MCEB have the membership or authority over budgets and execution activities that the task force believes is necessary to ensure the GIG is built and managed effectively. Without that level of authority over all elements of the GIG, the architecture is subject to interpretation by each component based on its needs, rather than the needs of the entire DoD enterprise. Additionally, neither of these two boards has a direct oversight responsibility over any specific office or function that carries out its direction. There is also little incentive to address crosscutting issues in a coherent fashion when the funding for these programs is provided via Title 10 channels without some mechanism to encourage cooperation. Because of the Title 10 and DoD versus Intelligence Community issues, the only level of management senior enough to cross this bridge is at the DepSecDef level.

The IA reference model suggested by this task force is shown in Figure 15. This protocol stack assumes the use of internet protocols in a wide range of environments, including both tactical and strategic. It parallels the International Organization of Standardization (ISO) reference model (ISO 7498), with the substitution of a "middleware" layer in lieu of the presentation layer, and is consistent with the TCP/IP suite. (This substitution seems appropriate because modern systems do not make use of separate presentation layer functions; these functions are assumed by applications.)

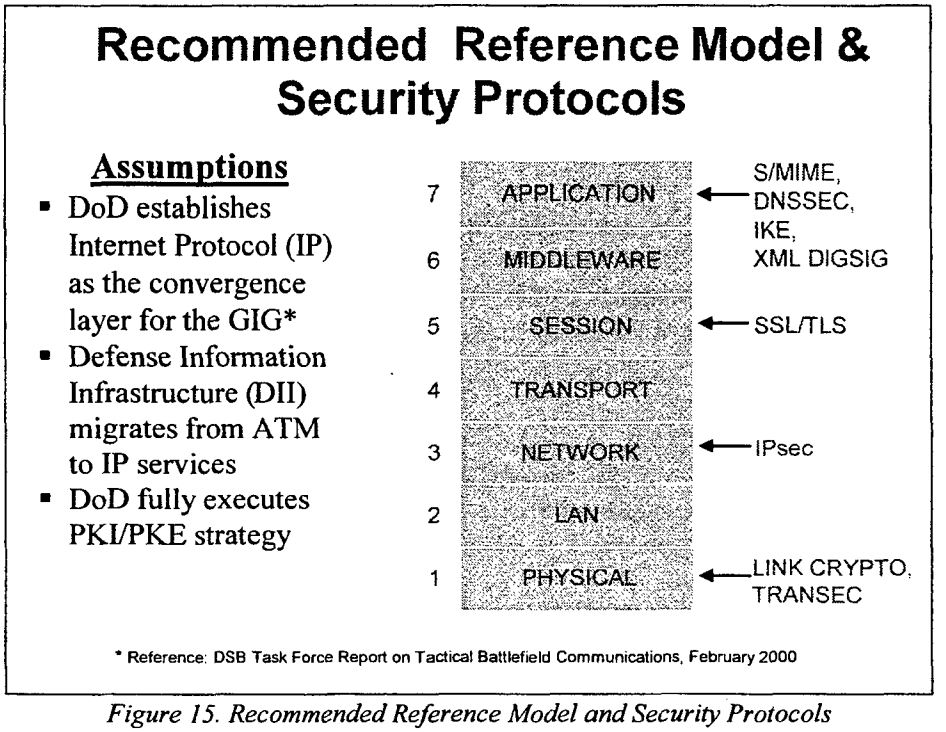


Figure 15. Recommended Reference Model and Security Protocols

In this model, physical layer protection is afforded via link KGs (e.g., KG 84, KG 189, etc.) on a hop-by-hop basis, where warranted by threat concerns. No data link security; e.g., Local Area Networks (LAN) security protocols such as IEEE 802.10, is recommended. This technology has not been adopted by product vendors and is generally not warranted in switched LANs, when higher layer security protocols are employed. Internet Protocol security (IPsec) is recommended for end-to-end, enclave-to-enclave, or end-to-enclave protection. No transport (e.g., TCP) layer security protocol is recommended because there are no widely used standards yet available, and because the services provided at the IP and session layers obviate the need for transport layer security.

Although the Internet protocol stack does not include a session layer per se, the introduction of Secure Socket Layer (SSL), Secure Shell (SSH), and analogous security protocols has created one. SSL is widely deployed and DoD policy calls for its use for secure web access. The task force recommends its use with client (not just server) certificates, for high quality user authentication and access control, with transition to Transport Layer Security (TLS) (the Internet Engineering Task Force (IETF) standard) as it becomes more widely available.

The task force suggests the insertion of a "middleware" layer to accommodate systems such as Common Object Request Broker Architecture (CORBA), distributed computing environment (DCE), or Enterprise Java Beans (EJB). However, such systems are not universally required and there is no clear appropriate choice among these competing middleware technologies at this time. Finally, several critical protocols exist at the application layer, and more may emerge. For secure e-mail, S/MIME (v3 with enhanced security services) is the preferred protocol, and it is widely available in Commercial Off-The-Shelf (COTS) products. Secure domain name system (DNS) is an essential infrastructure security component requiring Defense Information Services Agency (DISA) as well as base-level support. Internet Key Exchange (IKE) is the key management protocol used by IPsec. As Extensible Markup Language (XML) becomes more common, the digital signature standards developed for it will become critical elements of more sophisticated web security designs, supplementing, but not supplanting, SSL/TLS.

Figures 16 and 17 outline recommended GIG IA system architecture strategies.

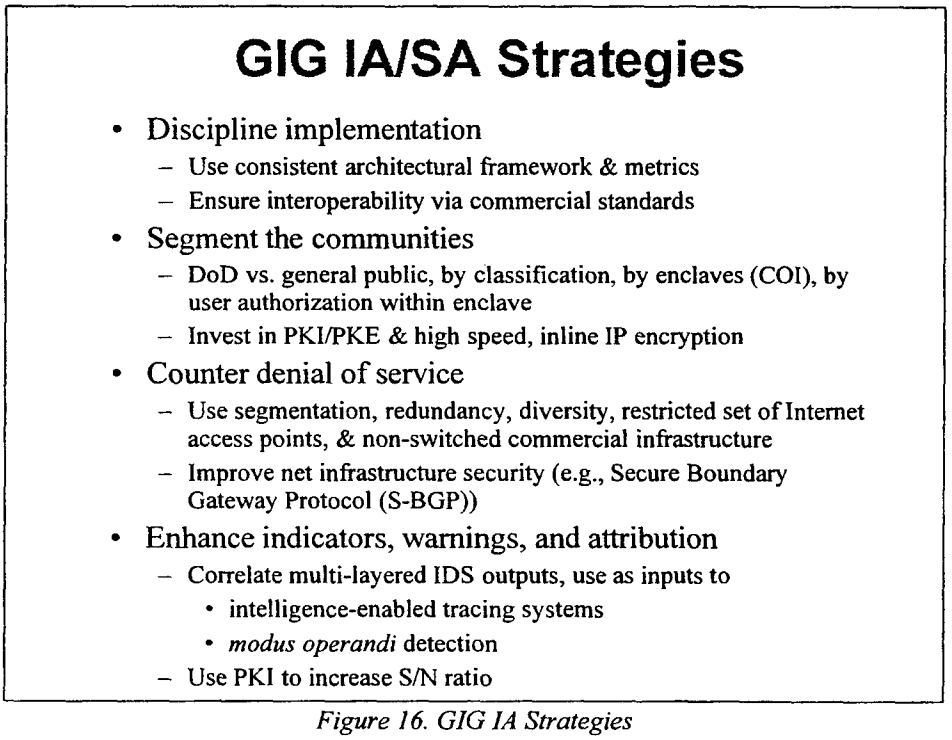


Figure 16. GIG IA Strategies

The first strategy is to use a consistent architectural framework and consistent metrics across the entire DoD GIG. This strategy contrasts the current divergence of approaches the Services. It is important to foster interoperability via commercial standards, so that commercial and government off-the-shelf technology can be employed throughout the system. The defense-in-depth approach leads to the strategy of segmentation. Segmentation is recommended between the DoD and the general public Internet, between levels of classification, by enclave (COI), and by individual user within an enclave. In order to support segmentation, investment will be needed in high-speed in-line IP encryption devices, and in large scale PKI and PKE.

Fine-grained access control (FGAC) is the principle that allows access to computing and communication resources to be shared, in a safe manner, among a large number of users and user communities. Technology is available to enforce FGAC with an acceptable level of computational overhead, but tools must be available to enable local administrators and users to efficiently manage FGAC for Wide Area Networks (WANs), LANs, and individual hosts and servers.

FGAC is supportive of accountability and acts as a deterrent to inside attacks. Fine-grained identification and authentication, e.g., via use of level-4 PKI, provide the inputs needed to make FGAC decisions. Intrusion detection mechanisms help detect attacks that have eluded access controls, or activities that represent inappropriate use of resources by authorized personnel.

The third strategy is intended to counter denial of service. Segmentation, redundancy, diversity, a restricted set of Internet access points, non-switched commercial infrastructure, and improved overall net infrastructure security, such as S-BGP (Secure Boundary Gateway Protocol), used in concert can partially mitigate the denial-of-service threat.

Another important element of the strategy is to enhance indicators and warnings and attack attribution. By correlating multi-layered Intrusion Detection System (IDS) outputs, one can detect patterns of behavior that may indicate a modus operandi. This information can be useful in tracing the sources of unwanted behavior. The correlated outputs of host- and network-based IDS at various levels can also be used to direct attention to potential threats. Resources such as human system administrators and various intelligence assets can be directed in this way. The use of a PKI and PK applications can greatly reduce the noise level of amateur attacks coming into the GIG, and thus increase the signal to noise ratio of the existing indicators and warnings in the GIG.

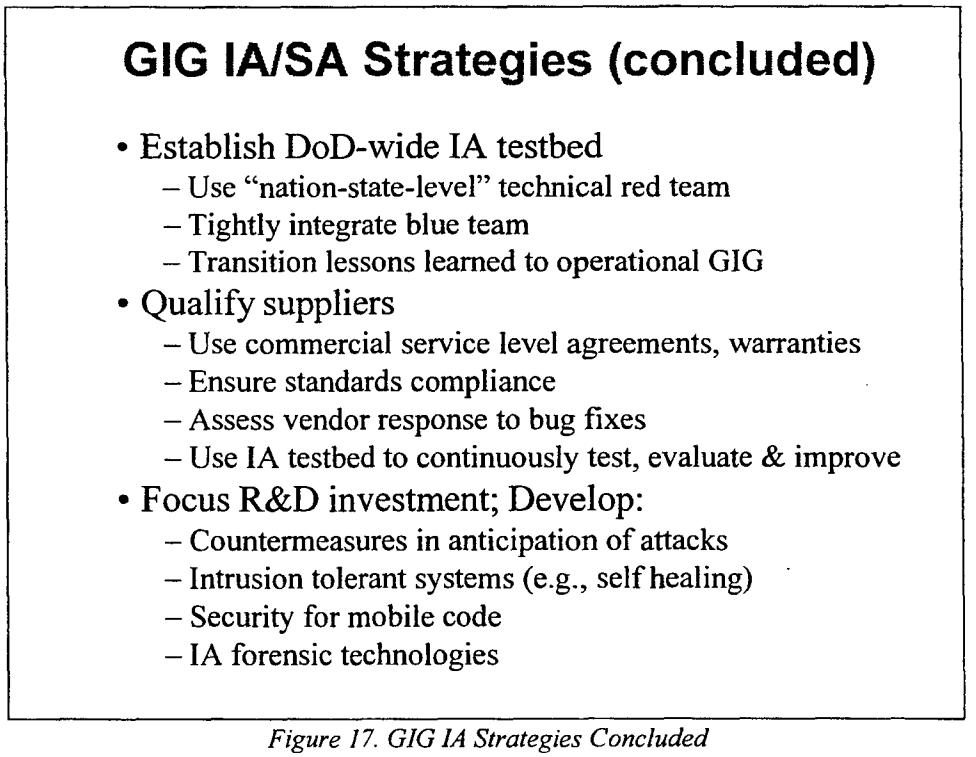


Figure 17. GIG IA Strategies Concluded

The fifth strategy is to establish a DoD-wide GIG IA testbed. This testbed would draw blue team members and current configuration information from GIG operations, and would employ a nation-state-level technical red team. The lessons learned through these exercises should be used to upgrade the IA properties of the testbed, and if successful in defense, should be transitioned to the operational GIG. Building an IA testbed avoids the costs and other issues inherent in red-teaming the live operational GIG.

A sixth strategy is to more stringently qualify suppliers of GIG IA technologies than is current practice in government procurement. It is imperative that the DoD becomes a smart buyer of commercial information and information assurance technology and services. Commercial information services can often be bought with service level agreements (SLAs) and/or warranties. SLAs can cover a variety of service aspects. For example, an SLA for a communications service might cover: 1) communication speed, 2) link availability, and 3) notification of the customer about problems within certain timelines. In the future, we expect that SLAs may also address security issues.

It is also important to assess suppliers' conformance with applicable standards. There are numerous organizations that measure and certify compliance with a wide range of standards, such as Underwriter's Laboratory. In the information security arena, conformance with the Common Criteria, evaluated under the auspices of the National Information Assurance Partnership (NIAP) is particularly important. The NIAP is a collaboration between the National Institute of Standards and Technology (NIST) and the National Security Agency (NSA). The NIAP encourages the development of commercial products with security features as specified in the Common Criteria, and certifies commercial laboratories to evaluate products against the criteria under NIST's National Voluntary Laboratory Accreditation Program (NVLAP). In implementing the GIG, strong preference should be given to products evaluated under the NIAP.

Another way to qualify suppliers is to gauge their commitment to fixing security-related flaws found in their systems. There are numerous organizations that compile information about vulnerabilities in commercial systems, among them the Computer Emergency Response Team (CERT) at Carnegie-Mellon University, the SANS Institute, Security Focus, and NTBugtraq. In implementing the GIG, strong preference should be given to suppliers who have a track record of quickly fixing reported flaws. Furthermore, preference should be given to products that are compatible with the Common Vulnerabilities and Exposures (CVE) list. CVE is a list of information security vulnerabilities and exposures that aims to provide common names for publicly known problems. The goal of CVE is to make it easier to share data across separate vulnerability databases and security tools with a "common enumeration."

Furthermore, while the vulnerabilities of commercial technology need to be understood, the impact on the overall GIG architecture of adding the technology needs to be weighed before employment. The task force recommends that the GIG IA testbed be used to address this issue. As mentioned above, there is a great deal of publicly available information about technology and product vulnerabilities. The testbed should use this information as a starting point for developing a knowledge base of technology and product benefits and vulnerabilities.

- The DoD should develop a deep understanding of how commercial services are provided, so that they can be properly specified when purchased. For example, buying communication lines from multiple suppliers in order to gain redundancy and diversity may not yield the desired results, if each supplier's fiber goes through the same physical switch or runs over the same physical bridge. Instead, when buying a second communication line, DoD should specify that the line share no physical components or transit mechanisms with the first communication line.

The final strategy recommended is to adequately fund a focused GIG IA R&D program. Current DoD IA R&D does not adequately address the IA needs of the GIG. Countermeasures must be developed in anticipation of attacks. The GIG IA testbed recommended by this task force can be used to experiment with potential fixes before any form of specific attacks are found live on the GIG. The development of self-healing systems that are intrusion-tolerant and fault-tolerant is an important step in deploying a reliable GIG infrastructure. Self-healing, recovery, and reconstitution of GIG components could provide continuity of operation throughout and after significant attacks. Clear commercial trends point toward mobile code as an increasingly important software distribution and maintenance mechanism. Current practices in some networks of stripping mobile code out of incoming email and disabling Java and JavaScript are stopgap maneuvers. Significant focused research is called for to contain and verify mobile code, to discover new methods of utilizing mobile code to defend against attacks (e.g., throttling incoming traffic at the routers during a denial-of-service attack), and to automatically install good viruses that upgrade system survivability. R&D focused on forensics, tagging, and traceback could provide GIG administrators with the tools necessary to trace attacks back to their source. Non-repudiable identification of malicious attackers and wayward insiders can provide a level of deterrence not currently in evidence.

2.5 Operating an Effective Information Assurance Architecture

Figure 18 provides an example of layered defense, or defense-in-depth, from a traffic flow perspective. All DoD common user networks, SIPRNET and JWICS as well as NIPRNET, should reflect this architecture. This is a departure from current practice in which the classified networks do not provide significant barriers to attacks launched from sites in the same community, e.g., other subscribers to the same common user network.

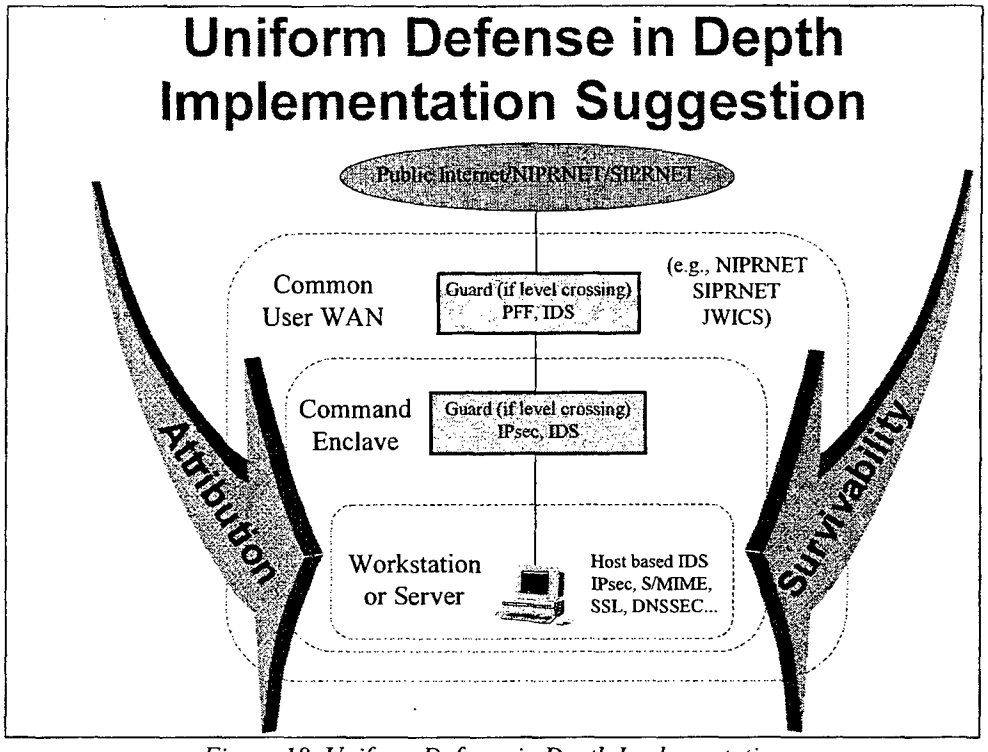


Figure 18. Uniform Defense in Depth Implementation

The outer perimeter represents an interface between a single-level, common user WAN, e.g., NIPRNET, SIPRNET or JWICS, and a less sensitive WAN, e.g., the public Internet. (If a sensitivity level is crossed, e.g., from SIPRNET to NIPRNET, then a guard is employed.) This perimeter is protected by the use of a (stateful) packet filtering firewall (PFF) and an IDS. Non-IPsec- or SSL- protected traffic, e.g., e-mail, DNS, and web traffic, is screened via the PFF and restricted to destinations inside the WAN that are well-defined web servers, e-mail servers etc. The IDS here is used to screen traffic (at very high data rates) to detect patterns of attacks against multiple sites on the WAN, through correlation of analytic data from each of these IDS systems. Virus scanning might even be applied to (non-encrypted) e-mail attachments at this point, via the use of implicit mail relays.

At the enclave boundary, IPsec is the primary defense mechanism, preventing unauthenticated connectivity to external sources. A PFF is used for traffic that would not be afforded IPsec protection, e.g., e-mail and DNS services. (As illustrated later, web data designed to be available for public access will be maintained outside of the enclave boundary.) The enclave IDS has access to some plaintext data (except when IPsec or SSL is used all the way to a workstation or server) and thus can perform more analysis than the WAN IDS. Virus scanning can be applied to (non-encrypted) e-mail attachments at this point, if it is not applied at the WAN boundary.

Each workstation or server is equipped with an IDS, which is monitored by the enclave security administrator. IPsec, SSL and S/MIME are available for end-to-end cryptographic security, including authentication, integrity, confidentiality, and access control. A secure DNS resolver interacts with secure DNS servers.

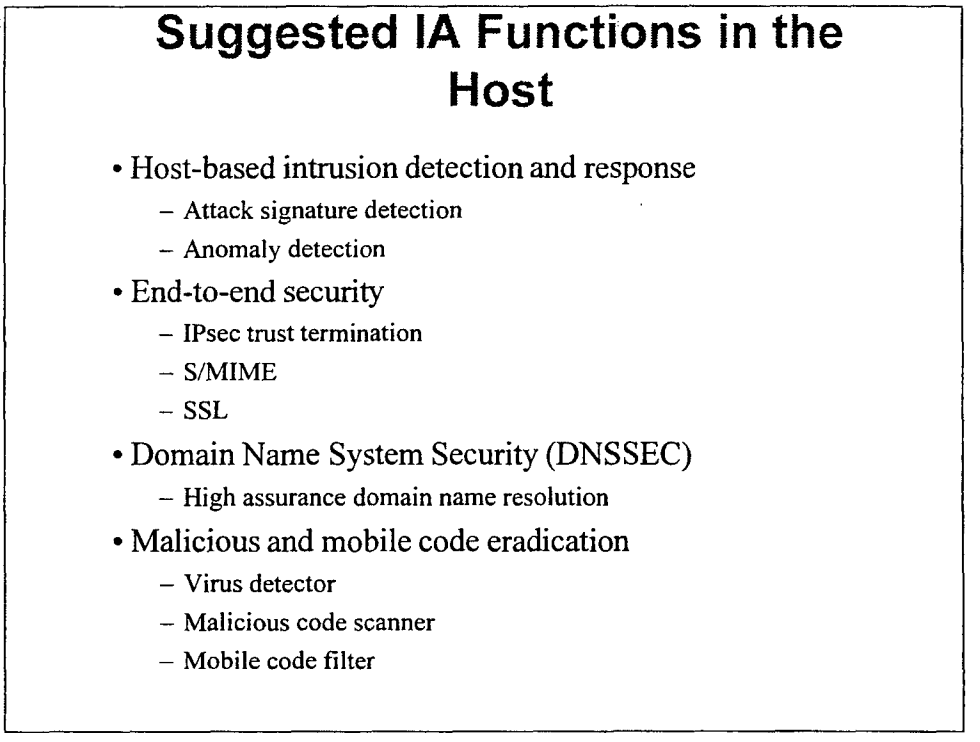


Figure 19. Suggested IA Functions in the Host

In addition to boundary protection provided by the DiD architecture, there are a variety of functions that should be employed to defend the hosts in the GIG. The task force suggests that these be used in all DoD common-user networks, including NIPRNET, SIPRNET, and JWICS.

IPsec, SSL, and S/MIME should be used for end-to-end cryptographic services such as confidentiality, authentication, nonrepudiation, integrity, and access control. A secure DNS resolver should be deployed with secure DNS servers to provide high assurance that a domain name is resolved correctly. A virus scanner, malicious code detector, and mobile code filter should be used to strip any attachments or content violating mobile code policies established within an enclave. In keeping with the defense-in-depth strategy, host-based intrusion detection and anomaly detection tools should also be deployed. When IPsec is used all the way to the host, the host has the only opportunity to apply serious IDS scrutiny to incoming packets. Since the hosts will experience relatively small data rates, the IDS can be tuned to high levels of sensitivity. The host-based IDS should communicate alert information to other enclave IDS services, which can correlate data from network IDS and other host-based IDS deployed in the enclave to obtain a more accurate enclave-wide view of intrusive and other network activity. Signature-based IDS should be kept up-to-date and output monitored by the enclave security administrator.

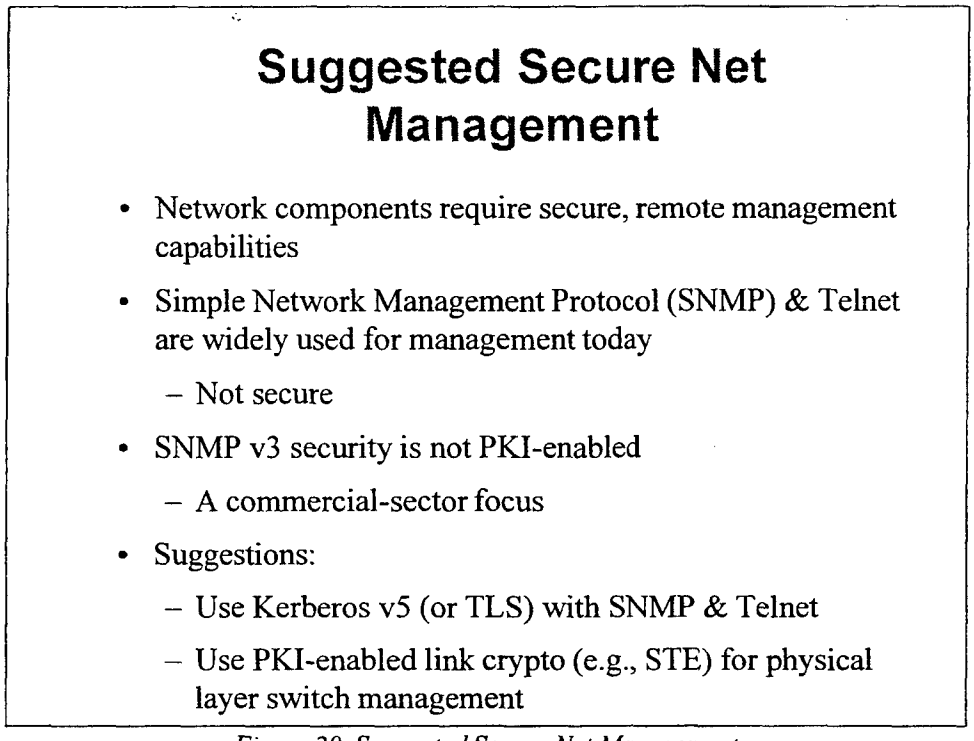


Figure 20. Suggested Secure Net Management

Today, most layer 3 and above network components are managed remotely using a mix of SNMP and Telnet, although some offer web interfaces as well. SNMP v1 offered no security, and so was used only for getting information from managed devices (reading Management Information Bytes (MIB), but not modifying them). Telnet, even if used with plaintext reused passwords, was often employed. SNMP v2 had static, symmetric key cryptographic security added, but was not commercially successful. SNMP v3 has improved security services, but still uses manually distributed, symmetric keys. This is not consistent with our proposed use of PKI for user authentication and authorization everywhere else in the GIG. The use of Kerberos for SNMP v3 security has recently been proposed. Version 5 of Kerberos supports X.509 certificates and thus may provide a means of PKI-enabling SNMP v3.

Telnet, secured by Kerberos, is available and used today in some products for secure Secure Electronic Transactions (SETs), and web interfaces for management can make direct use of SSL/TLS. Telnet also can be secured using SSL/TLS.

For the most part, the GIG will not own or directly manage circuits, but when it does, the circuit switches, SONET switches, and the like often require or offer out-of-band management interfaces, e.g., via the Public Switched Telecommunication Networks (PSTN). These interfaces should be secured via link crypto devices that make use of PKI technology, to provide authenticated, integrity-protected, and confidentiality-secure channels. Some such devices are commercially available, and one can use STU-IIIs (or, preferably, the follow on technology, Secure Telephone Equipment [STEs]) in this fashion as well.

DoD should focus on deployment of level 4 PKI. If this requires delaying Common Access Card (CAC) deployment, the delay should be tolerated. A PKI is a central element of system security and subversion of a PKI can undermine most layers of a defense-in-depth scheme. Thus it is critical that DoD take responsibility for its own PKIs. The DoD should not make use of commercial CAs, although the DoD PKIs must interoperate with commercial PKIs; e.g., to support authentication of DoD contractors.

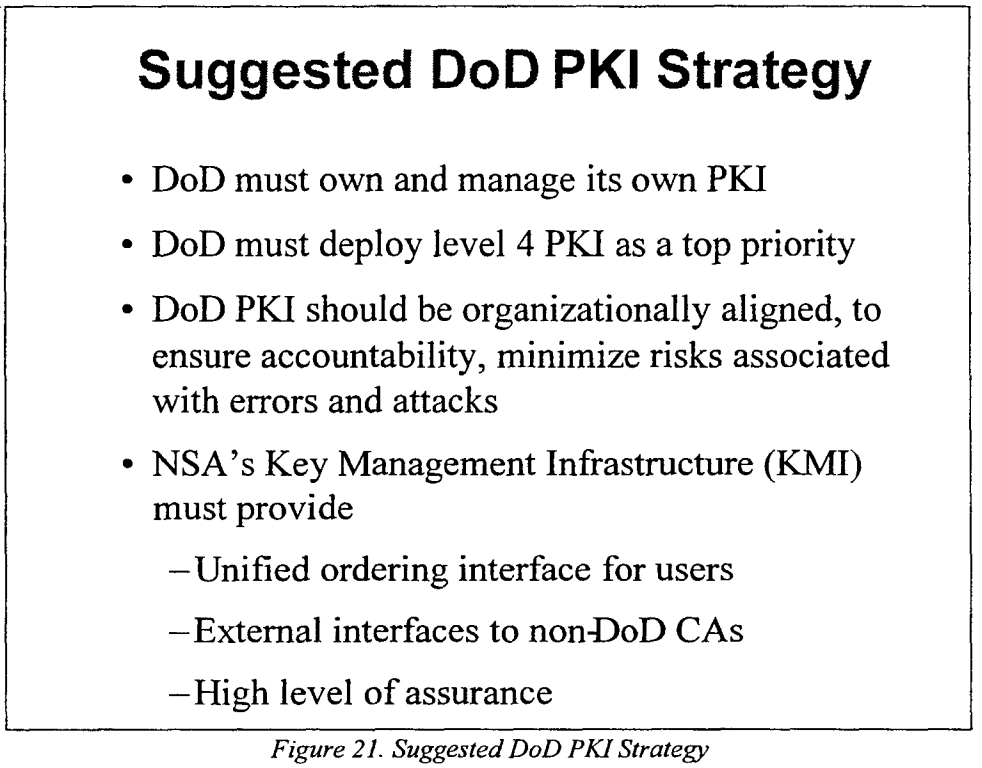


Figure 21. Suggested DoD PKI Strategy

The DoD PKI should be aligned with organizational boundaries, and should use alternate (subject/issuer) name extensions to incorporate DNS names and RFC822 names to facilitate native support of security protocols such as S/MIME, IPsec, and SSL/TLS. The NSA Key Management Infrastructure (KMI) could provide a suitable infrastructure for these requirements. It is critical that certificates be issued along organizational boundaries, to constrain the damage that might result from local security compromises. For example, it must not be possible for an Army Certificate Authority (CA) to issue a certificate that purports to be for an Air Force employee. Current plans for the KMI do not necessarily adhere to this principle and should be modified accordingly. Also troubling is the so-called "bridge CA" concept, developed for inter-organizational cross certification in the federal PKI. Several important PKI security features do not operate properly when a bridge CA is part of a certification path. A bridge CA should be used *only* to facilitate acquisition of public key certificates of other organizations, so that local security administrators can issue cross certificates directly to the other organizations with which they need to interoperate.

Domain Name Systems Security (DNSSEC) is a PKI-like system that provides secure name/address translation support for most Internet protocols. The DNS is global in scope and thus the DoD should encourage widespread adoption of DNSSEC. Within the DoD, high assurance (cryptographic) technology should be employed to protect DoD domains, i.e., the DoD should implement DNSSEC for the .mil and .sml domains and sub-domains.

Directories are essential for widespread deployment of e-mail security (S/MIME), because a sender must retrieve the certificate for a recipient prior to encrypting a message. IPsec and TLS do not rely on directories, except for certificate revocation status information. Lite Directory Access Protocol (LDAP) is the current, commercial directory interface standard; it is a rapidly evolving standard, of growing complexity. Security for directory access, e.g., via TLS, is improving, but implementations will probably remain significantly vulnerable for some time. The DoD must ensure that the directory systems it deploys make use of the best available load sharing, replication, and security.

The suggested system architecture and DiD address the insider threat previously discussed. Intrusion detection systems deployed in enclaves, on user workstations servers and other devices, monitor activity to detect inappropriate (e.g., suspicious) behavior by authorized personnel, as well as attacks by outsiders, which should provide a deterrent to some class of insiders, as well as aid counter-intelligence efforts.

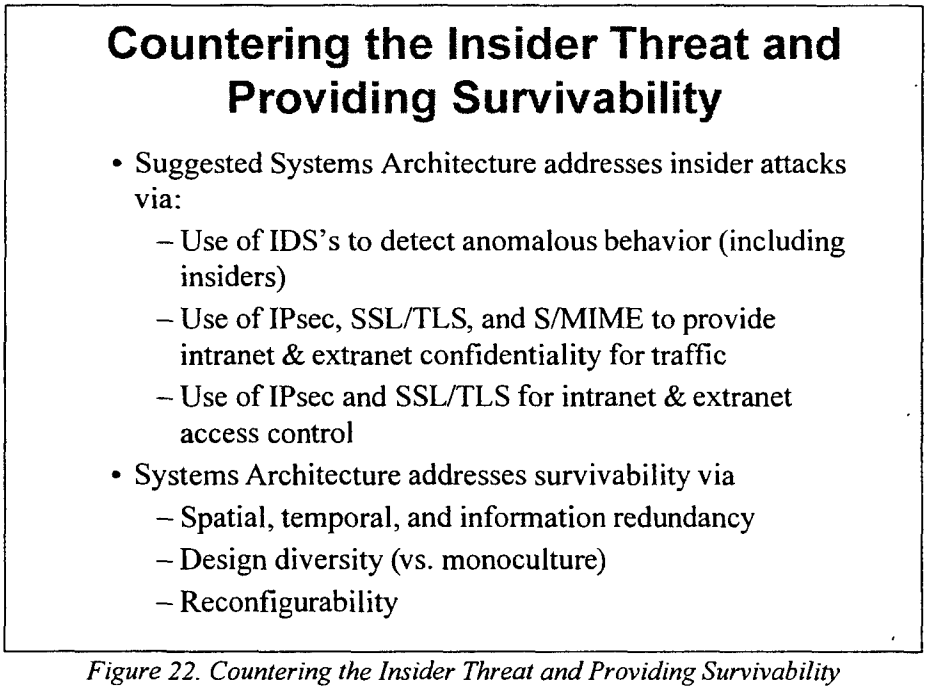


Figure 22. Countering the Insider Threat and Providing Survivability

The security protocols cited above (IPsec, SSL/TLS, and S/MIME), and level-4 PKI support fine-grained access control to information in storage on servers and in transit. This fine grain access control helps prevent a subverted insider from eavesdropping on communications inside enclaves and helps prevent insiders from gaining access to servers or to other enclaves without explicit authorization. Because all of these protocols make use of PKI technology for authentication, the resulting audit trails also help to detect and deter insider misuse.

Survivability is addressed through the use of redundant servers, access lines, and local interfaces (e.g., multi-homing) and via dynamic routing in common user WANs.

The architectural elements that counter denial of service and provide partial ability to attribute attacks back toward their origins are listed in Figure 23. The stateful packet-filtering firewalls installed at the boundaries should be configured to reject Internet Control Message Protocol (ICMP) echo and reply messages, and to throttle synchronization (SYN) messages to limit the number of half-open connections. Smurf attacks depend on ICMP echo reply (as well as other questionable mechanisms) that can easily be stopped at firewalls. SYN floods depend on overflowing the fixed-length queues of TCP, so by throttling the number of SYNs allowed into a network, perhaps contingent on the completion of connections, one can limit the disk operating system (DoS) potential at the firewalls.

Countering Denial of Service and Enabling Attribution

IA Architectural Feature	Benefits
Packet Finding Filters and IPSec	Blocks DoS attack at edge Certificate-based attribution
Nested IPSec	Supports Path tracking Localization of target
Networked IDS visualization	Improves response time
Anomaly detection on military patterns of use	Improves response time
Content distribution	Disperses DoS attacks Geographic attribution
Inline IPSec devices	Fosters commercial robustness to DoS attacks

Figure 23. Countering Denial of Service and Enabling Attribution

There is a potential performance penalty associated with such throttling, but this can be managed. In the February 2000 distributed denial-of-service attacks, approximately 80% of the attacks were Smurf, and 15% were SYN floods. Thus approximately 95% of Feb-2000-style Distributed Denial of Service (DDoS) attacks would be mitigated by present and suggested firewalls at the enclave boundaries.

The task force recommends the use of IPsec, which prevents denial-of-service within the enclaves. Further, future nested-IPsec implementations can counter denial of service and assist attribution by target localization and path tracking. The task force then recommends research and development of networked IDS visualization tools for semi-automated sysadmin response, which would improve the time to respond to a DDoS attack. (It took days for sysadmins to identify the first DDoS attack for what it was.) The task force provides a recommendation to employ anomaly detection configured to exploit known military patterns of use, and to trigger responses

perhaps including dynamic user reauthorization. Content distribution networks, such as those run commercially by Akamai and Digital Island, provide additional mechanisms to counter DoS attacks. The static content of public DoD web sites can be replicated in a similar way. For public DoD web sites using SSL server certificates to prevent web site defacement, the current commercial offerings are inappropriate. Some content-distribution approaches provide a partial geographic attribution. Finally, the task force recommendation to support development of a high-speed inline IP cryptographic device could foster widespread commercial IPsec use, initially in large multinational corporations. Together, the task force recommendations partially address denial-of-service attacks on the GIG, and provide initial attribution capabilities.

Metrics for information assurance and surveillance architectures are an important and inadequately addressed need. Researchers, designers, vendors, and operators of information systems need a broad spectrum of metrics to achieve their respective objectives. From a systems perspective there is a need to develop metrics for technical, system and mission level evaluation. This will require collaboration amongst technical, evaluation, and operator communities. A testbed is required to provide a means for measurement of system performance on scenarios and related information traffic. The defense-in-depth systems architecture and metrics measuring capability facilitate new capabilities for indications and warning. Figures 24 and 25 provide a few examples of how the metrics may be utilized by different communities at different stages of the lifecycle of a system.

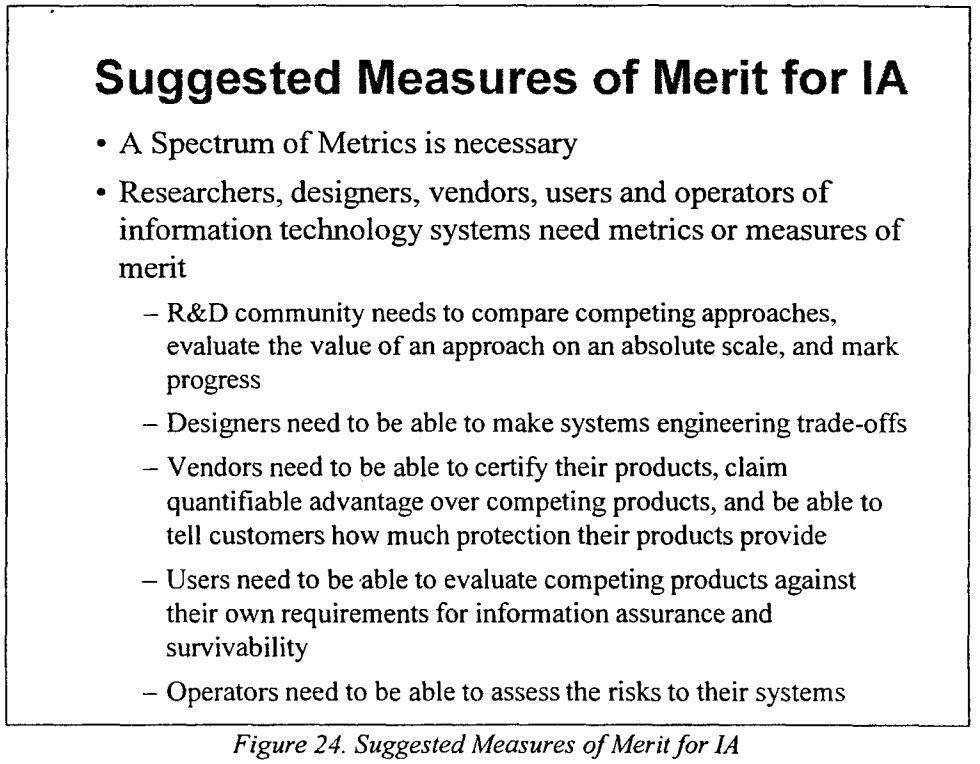


Figure 24. Suggested Measures of Merit for IA

The research and development community must compare competing approaches, evaluate the value of an approach on an absolute scale, and mark progress as a function of time. This paradigm of common metrics, validated training, and test data has proven to be extremely successful in areas such as speech, speaker, and language recognition. Designers need to make systems engineering trade-offs. This is particularly true when attempting to trade complexity for performance.

Vendors need to certify products, claim quantifiable advantage over competing products, and tell customers how much protection their products provide. Metrics provide a means for facilitating an Underwriters Laboratory (UL) approach to evaluating commercial products, i.e., common data, measurements and analysis. There has been progress on this front over the last 17 years, starting with the Trusted Computer System Evaluation Criteria (TCSEC) "Orange Book," progressing to the Information Technology Security Evaluation Criteria (ITSEC), and now the Common Criteria (CC) version 2. However, there are still questions about the viability of such security evaluation criteria, as noted in the recent National Research Council report, "Trust in Cyberspace."[5] Thus one should not expect that component evaluation will, by itself, "solve" the problems we face in engineering secure systems. Thus the approach described below, which emphasizes development of IA metrics for fielded systems, is critical.

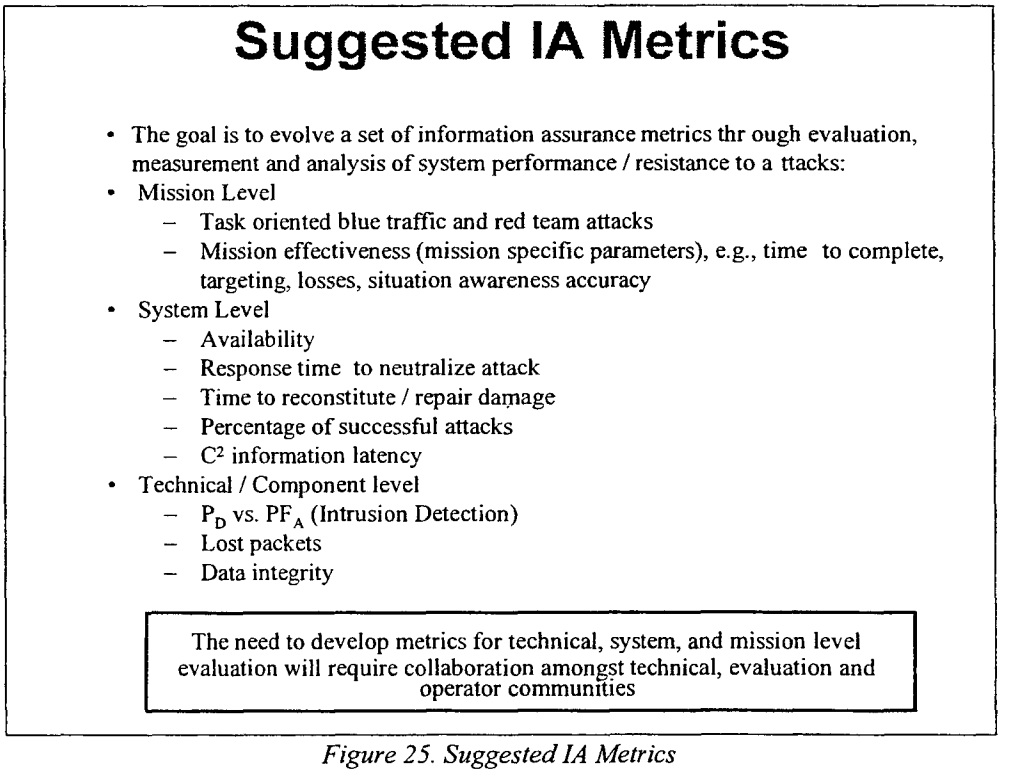


Figure 25. Suggested IA Metrics

[5] Trust in Cyberspace, Committee on Information Systems Trustworthiness, Computer Science and Telecommunications Board, Commission on Physical Sciences, Mathematics, and Applications, National Research Council, National Academy Press, Washington, DC 1999, Fred B. Schneider, Editor

Users need to evaluate competing products against their own requirements for information assurance and survivability. Operators need to assess the risks to their systems. Measures of merit or metrics for information assurance and survivable architectures is an important and inadequately addressed need.

The overall challenge, based on the architectural environment and an evolutionary experiment, evaluation, and analysis process, is to develop a set of information assurance metrics to measure system performance in the face of a wide-ranging set of attacks. At the mission level, the metrics will involve task-oriented blue team operations and traffic and red team attacks to evaluate overall mission effectiveness. Mission-level metrics would cover such topics as time to complete, targeting success, losses, situation awareness, timelines and accuracy, etc. Systems level metrics are related to mission-level metrics but are finer grained and would cover overall system availability; response time to neutralize attacks, reconstitute and repair damage; percentage of successful attacks; and Command and Control (C2) information latency. At the technical and component level, suggested metrics include specific measurements of probability of intrusion detection vs. false alarms, to provide a basis for performance quantification. In addition, measurements of packet loss and data integrity and losses will provide a means for evaluating the overall performance of information systems. The relationship of measurements and performance at all levels will require collaboration amongst the technical, evaluation, and operator communities.

The goal of information assurance metrics is to evaluate the ability of information assurance systems to protect, detect, and react to attacks. To achieve this goal it will be necessary to establish a distributed testbed and processes, as noted in Figure 26, for developing information assurance effectiveness metrics.

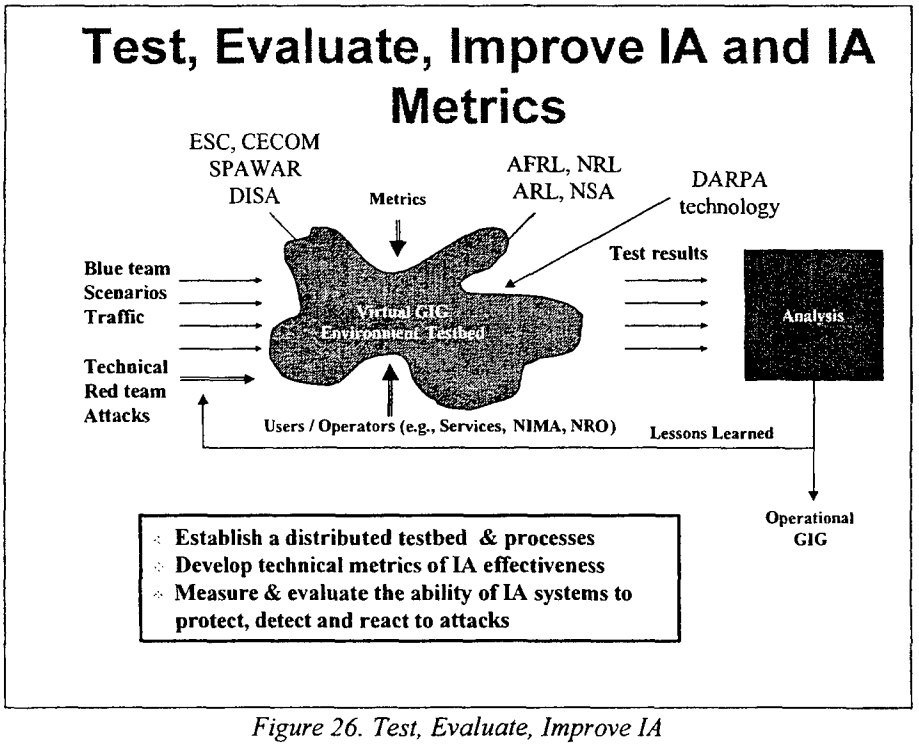


Figure 26. Test, Evaluate, Improve IA

Testbed nodes should be located at Electronic System Command (ESC), U.S. Army Communications Electronics Command (CECOM), Space and Naval Warfare Systems Command (SPAWAR), Air Force Research Laboratory (AFRL), NSA, etc. The participants in the evaluation process will include research and development, evaluation, and operational communities (services and agencies). The testbed will provide a means for measurement of system performance in the face of Red Team attacks on Blue Team scenarios and related information traffic. The testbed will also serve as a primary means for DARPA Information Assurance technology insertion and evaluation. The metrics and measurements will evolve as results are analyzed and lessons learned are derived from the data. Lessons learned will be fed back to red and blue teams to refine and update strategies and will be used by developers to improve system defenses. Lessons learned will also be made available to the GIG architects and system engineers to improve IA.

This evolutionary process is essential to achieving a commonly accepted basis for measuring effectiveness of information assurance systems. The overall process represents a journey rather than a destination. Change is inevitable for offense, defense, infrastructure, and particularly for COTS components. Measurement and evaluation of the ability of information assurance systems to protect, detect, and react to attacks by adversaries must track these changes to achieve continued protection.

As stated earlier, metrics for information assurance and survivable architectures are essential to achieving the broad spectrum of objectives of researchers, designers, vendors and operators of information systems. By implementing the defense-in-depth system architecture previously described, not only is system performance significantly improved, but a new set of system data (metrics) becomes available for indications and warning as noted in Figure 27.

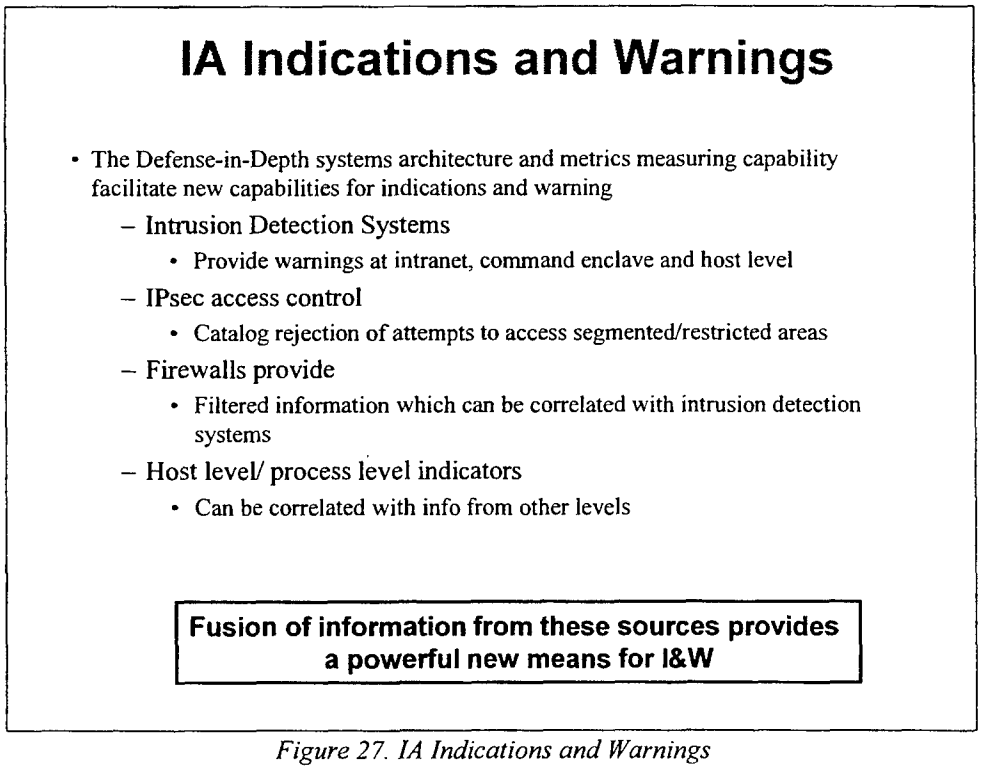


Figure 27. IA Indications and Warnings

The indications and warning data derive from a number of sources: 1) intrusion detection systems provide warnings at intranet, command enclave and host levels; 2) IPsec access controls provide data on illegal attempts to access segmented and restricted areas; 3) firewalls provide filtering information which can be correlated with data from intrusion detection systems; and 4) host-level and process-level indicators can be correlated with data from all of the above sources. The net result is that this multilevel, highly filtered data can be fused together to provide a powerful new means for facilitating indications and warning at multiple levels of the defense in depth architecture.

2.6 The Challenges Associated with Wireless

Since before WWII, wireless facilities have been part of military operations. They have been used in radio trunking throughout the upper echelons of the force and in tactical radio nets in the lower echelons of the force. From an information assurance perspective, wireless links merit special consideration, as noted in Figure 28, because they are not confined to a physical perimeter and can be observed from as far off as space. As a separate issue, it must be noted that frequency availability in foreign locations present an additional challenge to DoD's effective use of wireless technologies.

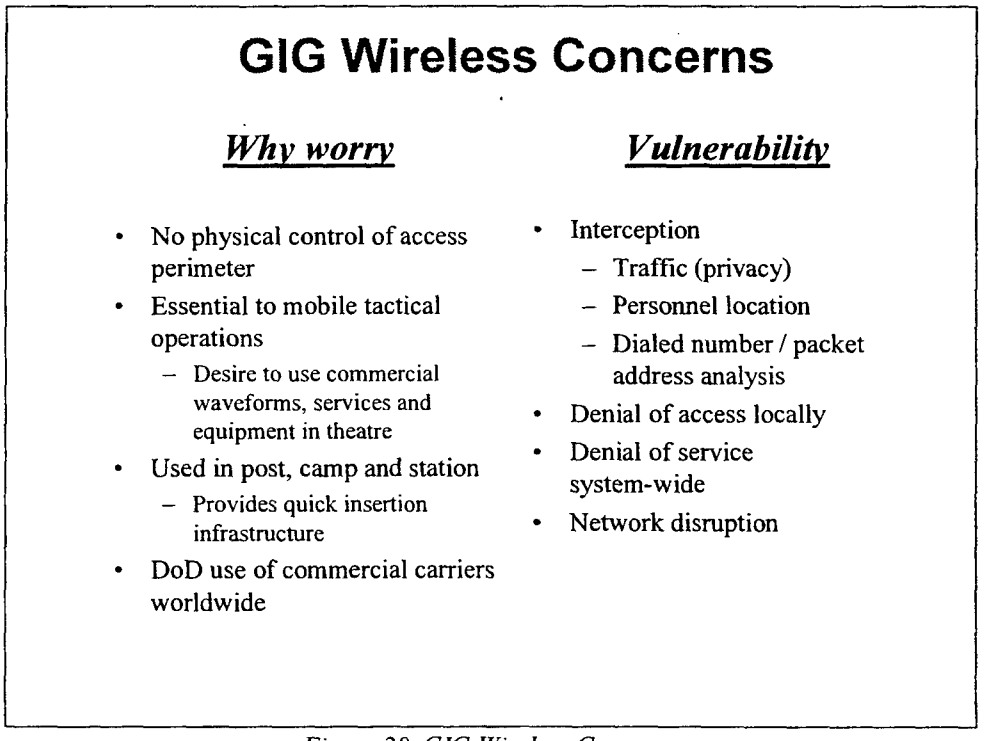


Figure 28. GIG Wireless Concerns

Recognition of wireless observability and the Soviet radio electronic combat doctrine caused these links to be both encrypted and protected against jamming. In the last twenty-five years the tactical forces have procured a wide variety of secure radio systems. Wireless facilities will continue to enable mobile military operations. Recently, efforts to "digitize" the battlespace have demanded an increased bandwidth. Increased bandwidth systems typically will have shorter ranges and thus require "ad hoc" networks to move the data around the battlefield. As a result, networked communications will move further forward in the tactical area.

Projections indicate that data will be an ever-increasing part of mobile military operations, while the level of voice information will be relatively static. Consequently, it can be expected that voice and data services will ultimately be provided above a common wireless/wired tactical Internet (the GIG). Thus, the security of the wireless net is essential to the performance of the system. In the civilian world, the use of wireless has been rapidly exploding. Mobile personal communications systems, such as terrestrial cellular services and satellite-based services, represent large economic investments. They provide ubiquitous, near global access to the Public Switched Telephone network from small, inexpensive user devices.

JV2020 envisions similar universal, on the move, information access for the military. Similarly, there are a number of emerging fixed wireless systems in use for wideband data and video access from the home. These systems are commercially attractive, because they can provide service with a minimal infrastructure. For the military they can also provide "instant infrastructure" in existing and deployed post, camp and station facilities. While the use of these commercial capabilities in the GIG is attractive, these systems will be subjected to attack and, if compromised, could have system-wide impact.

Passive interception and observation of links can provide information on user location, traffic content, called party, and pattern of use. Commercial providers are incorporating some forms of privacy in their systems to prevent well-publicized eavesdropping and fraud. However, network signaling information is generally available and can be used to deduce information or attack the system.

Active intervention in a wireless system, either by jamming or the use of equipment to render a system "busy," can deny access to communications service in a geographic area. More sophisticated attacks can deny particular users, user communities, or use of wireless facilities. All mobile systems depend on some system-level database to allow calls to find a user. Attacks on these databases, either outright or through exploitation of fraud prevention safeguards, can disable use of worldwide wireless facilities.

Finally, as discussed subsequently the exploitation of a network control structure can cause failure of the entire network. There have been examples of such failure in commercial networks due to software defects, and similar scenarios can occur due to either induced misbehavior or the introduction of false control signals into the network using wireless links.

The DoD has led the technology development of a wide range of countermeasures to physical level attack on wireless links. These techniques may be employed individually or in concert. As noted in Figure 29, the standard technique for countering jamming is the use of spread spectrum techniques, which can be carried out with either frequency hopping or direct sequence spreading or a combination of both. The basic strategy common to both is to spread the information across a wide range of frequencies so that the jammer has to dissipate his power over the whole spectrum, while the desired user can exploit his private spectrum access information to reject the

jamming signal. Adaptive antenna arrays have also been used to spatially reject a jammer. On most tactical radio links today the information is protected by Communication Security (COMSEC), typically embedded in the radio.

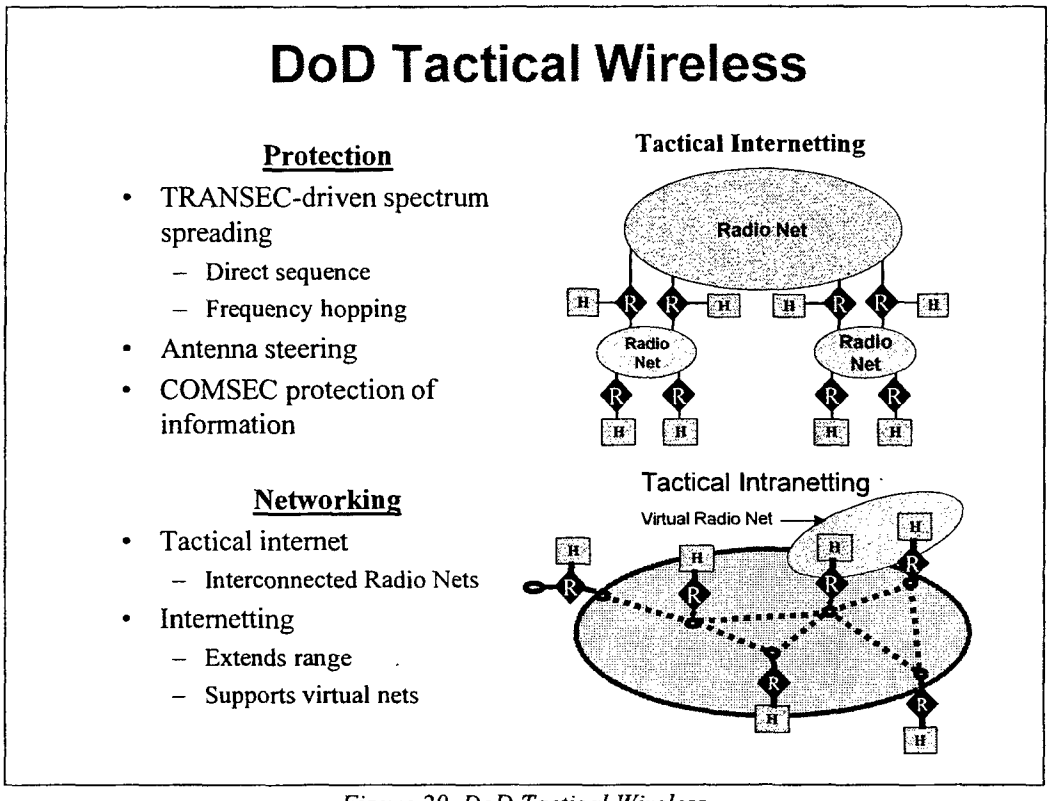


Figure 29. DoD Tactical Wireless

In the forward tactical area, radio nets have traditionally served single organizations. Recently there has been a desire to move digital information across multiple radio networks to achieve wide area connectivity and coordination. Initially this has been accomplished by using routers to interconnect secured radio nets, with the routers operating on decrypted traffic (system high). The Army's interconnected system is referred to as a tactical internet. Various exercises have shown that the routers are vulnerable to intrusion.

With a demand for higher bandwidth and robust connectivity, the emerging system concept is to separate the radio resource from the application. In this model the radios form an intranet where each radio handles all traffic in its area. The organizational communications are then achieved as a "virtual net" above the radio infrastructure.

The GIG will use communications links in the Public Switched Telecommunications Network (PSTN). In the 1980s, telecommunications providers developed and deployed a system architecture termed the "Intelligent Network" (IN) illustrated in Figure 30. This system architecture separated the signaling and control portions of the network from the interconnection process, so that advanced, revenue-producing, call-handling services could be provided. In this system model, a Service Switching Point (SSP) takes a subscriber's request for service and forwards messages through a network of Signal Transfer Points (STPs). STPs are packet switches deployed throughout the telecommunications network. The originating SSP uses these

messages to request information from Service Control Points (SCP) on how to respond to the service requests. SCP contain system level data and processing services. In response to these requests, messages are sent to all switching points required to complete the response to the call request. The suite of protocols used to communicate these control operations has been standardized by the Consultive Committee on International Telegraph and Telephone (CCITT) international standards body and is referred to as Signaling System # 7 (SS7).

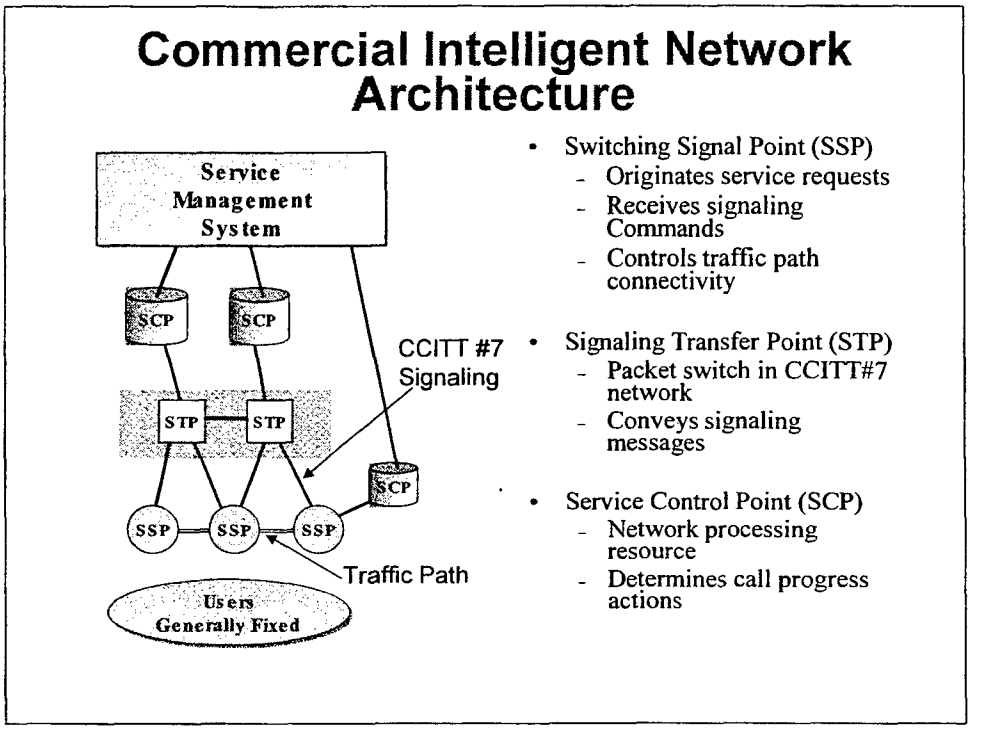


Figure 30. Commercial Intelligent Network Architecture

Access to the Signal Switching point is across an access facility. Traditionally this facility has been twisted pair, and considerable effort has been made to move ever-increasing data rates across this copper plant. In the 1980s, Integrated Service Digital Network (ISDN) was deployed to provide 144 kbps to subscribers. More recently, higher rates have been made available through Digital Subscriber Line (DSL) technology.

The majority of the recent wireless explosion has been in the area of wireless access to fixed infrastructure. Cellular and Personal Communications Systems (PCS) technologies, for example, use wireless access to deliver mobile users both switched voice services and narrowband data services. Low earth orbiting satellite systems are in the early stages of deployment. These systems allow a user access to the fixed infrastructure across a wider roaming area where terrestrial base stations may not be available. In addition, as shown in Figure 31, there are high-speed wireless access technologies, such as Multichannel Multipoint Distribution System (MMDS) and Local Multipoint Distribution System (LMDS), whose services are based on high-bandwidth radio segments in the spectrum at the 20 GHz frequency range. Emerging wireless access methods include Direct Broadcast Satellite (DBS), which employs Ka band satellite technology to distribute entertainment programming. DBS systems also offer asymmetric, two-

way data transmission supporting high-speed data transmission to the user (from the satellite system) and low-speed data reception from the user.

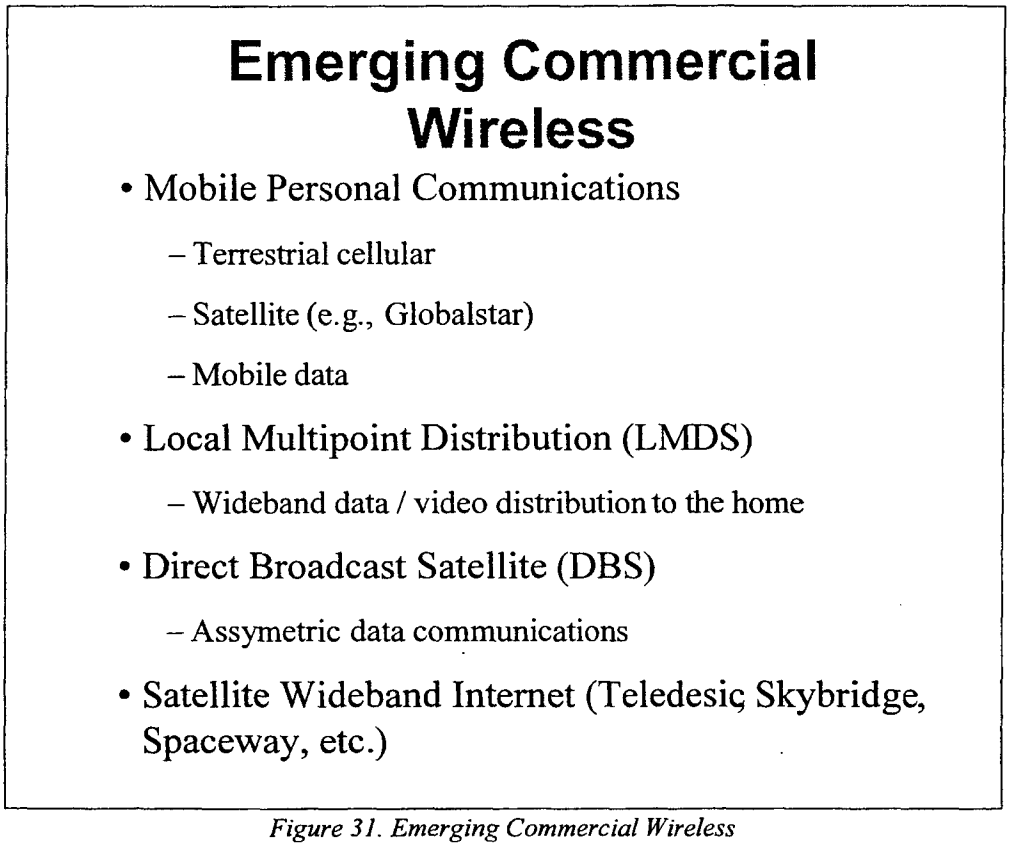


Figure 31. Emerging Commercial Wireless

Wireless wide area transport systems are planned to provide low-cost, high-bandwidth data and voice service to remote areas. These systems operate from either Low Earth Orbit (Teledesic and Skybridge) or Geostationary orbit (Spaceway). Most of these systems use the 20-30 GHz band, where wide bandwidths and small antenna apertures are possible.

The widest deployment of commercial wireless is in the mobile cellular system for which the system model is shown in Figure 32. Commercial mobile wireless services are furnished largely within the context of the Intelligent Network Architecture. The figure shows the standard wireless model. In the case of the cellular wireless application, the Mobile Switching Center serves the role of the Service Switching Point. The Mobile Switching Center and its associated Base Stations receive call requests from the mobile subscriber population. Call handling information is then requested from several key system databases, via the CC7 network. Messages are space-based on the (ANSI)-41 standard protocol suite.

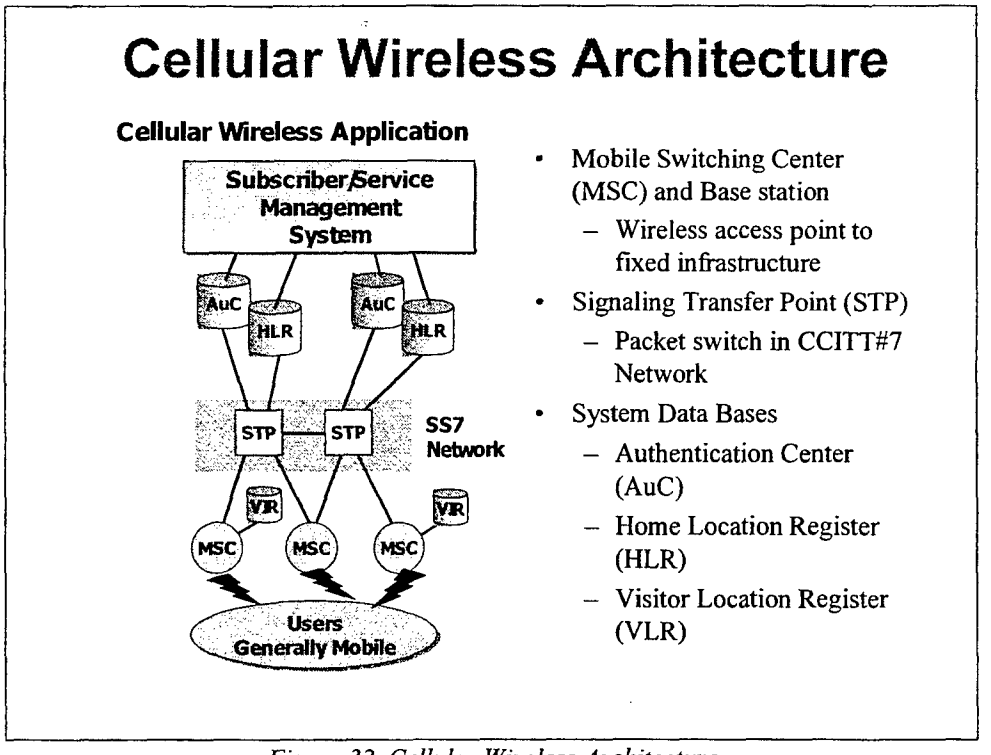


Figure 32. Cellular Wireless Architecture

These databases are: 1) the Home Location Register (HLR), which contains all of the information about the user and his current location within the system; 2) the Visitor Location Register (VLR), which contains information about all subscribers within an area served by a Mobile Switching Center (MSC); and 3) an Authentication Center (AuC), which determines the billing validity of the subscriber and accumulates the billing information. There may also be an Equipment Identity Center that holds information on particular devices in use within the system.

In the future, other processing resources are anticipated for new wireless based services. One is a group of voice-controlled services, e.g., voice-controlled dialing, which allows the wireless user to control features and services through spoken commands. Another is a suite of services offering incoming-call options, where the subscriber can customize call-forwarding or call-blocking instructions for different types of incoming calls or receive caller name identification.

The next level of detail in the cellular communications systems model is presented in the cellular reference model shown in Figure 33. This figure illustrates the Base Station and Mobile Station that provide the subscriber access to the system. Base stations are sometimes split into one or more Base Transmission Systems (BTS) at a cell site and a Base Switching Center (BSC). Multiple BTSs can be served by a single BSC and a single MSC can serve multiple BSCs.

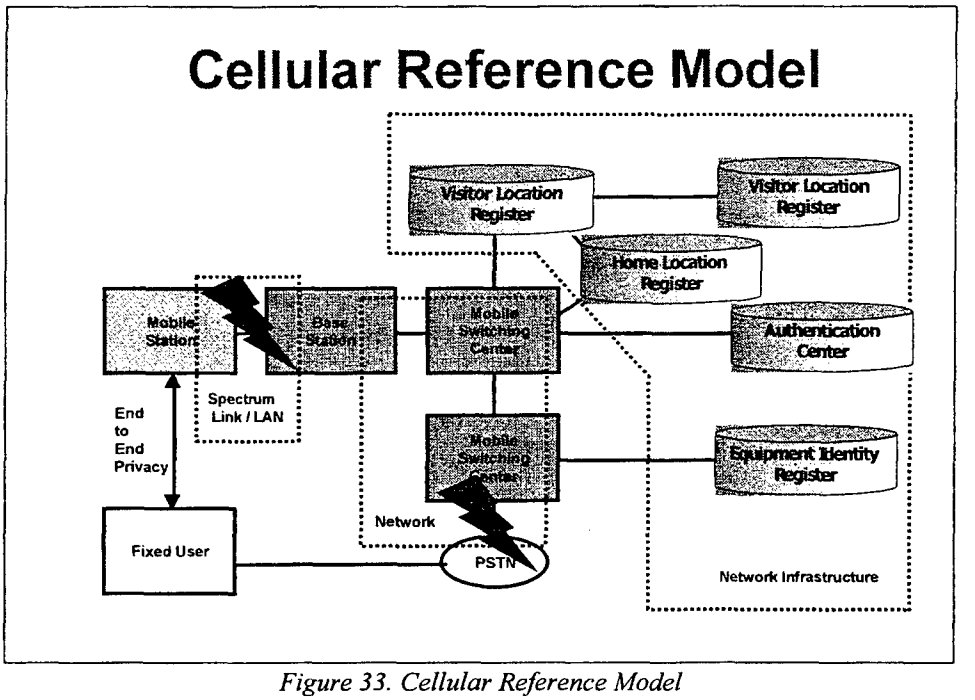


Figure 33. Cellular Reference Model

There are several potential attack points in this system. The first is an attack on the cell spectrum or a wireless point-to-point link between a BTS and a BSC or a BSC and an MSC. The information that is accessible at this point primarily pertains to subscribers currently within the serving area of an MSC and thus has a more localized effect. Wider ranging network attacks can be mounted against wireless point-to-point links that move signaling and traffic information between system nodes, either SS7 messages to system databases or internal information such as cell handoffs. Finally, classical cyber attacks can be mounted against any of the infrastructure databases, which are available through the SS7 network or increasingly through the Internet. While some protection mechanisms are in place, they likely will yield to a determined attack.

The key point to note is that while commercial wireless services may give the appearance of infrastructure independence, they are in truth a vulnerable extension of a vulnerable infrastructure. A number of countermeasures are classically available to defend against attacks mounted at different points in the composite system, as indicated in Figure 34. Attacks in the radio frequency spectrum are the most familiar threat to the military user, and there are a variety of techniques to counter them, such as random waveforms driven by high quality Transmission Security (TRANSEC) and spatial filtering of jammers by adaptive antennas. Although commercial wireless systems employ similar waveforms (Ground station module [GSM] uses Frequency Hopping and IS-95 uses Spread Spectrum), they are designed to combat interference from other users and provide no margin against jamming. Similarly these systems are designed for easy access.

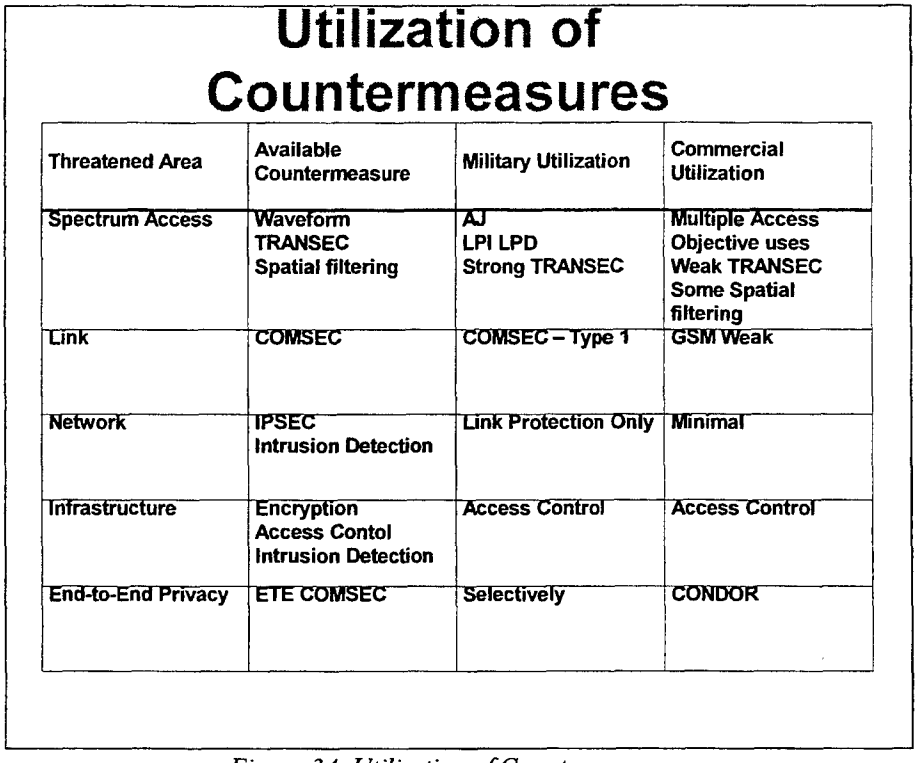


Figure 34. Utilization of Countermeasures

Tactical military systems also typically protect each link with strong encryption, but only some commercial wireless systems employ any encryption, and that encryption is weak. Above the link level, neither system has much protection. The tactical internet operates its routers at system high security level, while commercial systems employ rudimentary protection if any.

End-to-end Type 1 confidentiality is being provided through the NSA CONDOR program that is making commercial wireless available with embedded strong encryption.

2.7 GIG Information Assurance Summary and Recommendations

Figure 35 provides a summary of the panel's suggestions for GIG IA. As noted, the Global Information Grid is the underlying infrastructure to support information superiority for JV2020. The implementation of the GIG is one of the significant events that occurs once every decade or two. The architecture that is designed today will impact the DoD in the next decade or more. To meet this challenge, the task force has identified a layered architectural approach for providing information assurance to the GIG by pursuing a disciplined architectural approach:

- Link encryption at the physical layer
- ISO-like reference model with commercial protocols, e.g., IPsec for end to end protection
- Segmentation of DoD from Internet, and segment by classification and enclaves
- Adopt PKI/PKE
- Use fine grain access control of computers and communication resources.

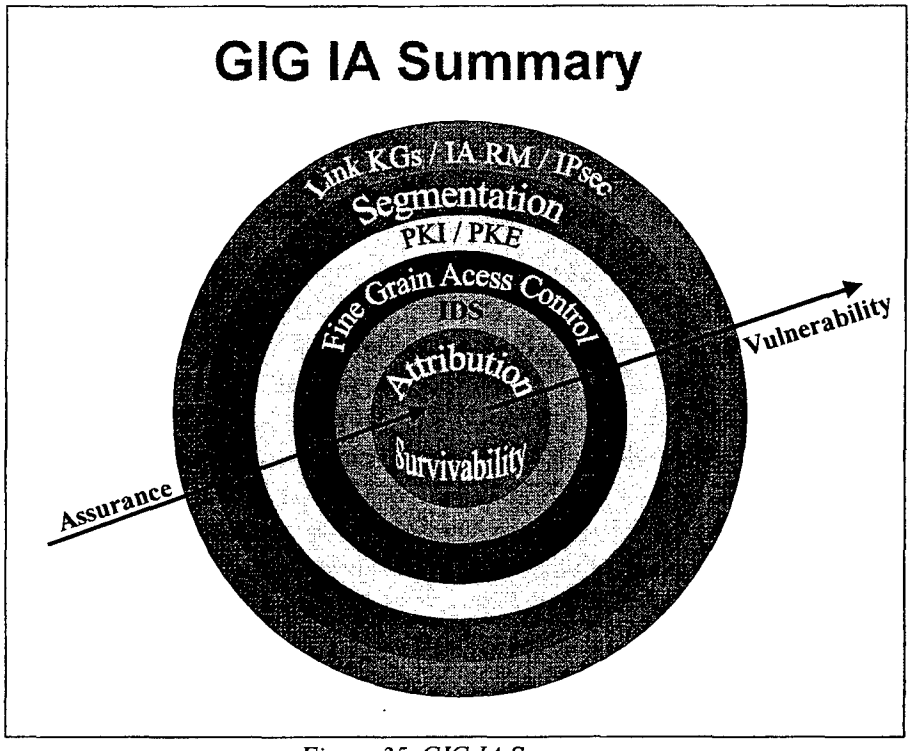


Figure 35. GIG IA Summary

In addition to the architectural layers, the approach also includes use of correlated multi-layered IDS data (e.g., at common user, command and host levels) as inputs to intelligence-enabled tracing systems and modus operandi detectors. Attribution is facilitated by highly filtered data for signal to noise enhancement and IPsec for path tracing and target localization. The approach of the layered defense, combined with measurement, rapid response and attribution, results in significantly reduced vulnerability and dramatically improved GIG information assurance.

In order to provide for implementation of the strategies outlined above, the task force makes the following recommendations:

1. Information Superiority Board

Background: *The task force believes that a new management mechanism is an essential part of implementing an effective information assurance architecture. It does not believe that today's management mechanism will be effective. The CIO Executive Board and the MCEB cannot provide effective oversight and governance for the GIG.*

- ***DoD CIO Executive Board:*** *The DoD CIO Executive Board is the principal forum to advise the DoD CIO on the full range of matters pertaining to the Clinger-Cohen Act (CCA) of 1996 and the Global Information Grid. Additionally, the Board also coordinates implementation of activities under the CCA, and exchanges pertinent information and discusses issues regarding the GIG, including DoD information management (IM) and information technology (IT). These issues include the collaborative development of IT architectures and related compliance reviews; management of the information infrastructure resources as a portfolio of investments;*

collaborative development of planning guidance for the operation and use of the GIG; and identification of opportunities for cross-functional and/or cross-Component cooperation in IM and in using IT. Although the Board has budgetary review authority for IT investments, and can make recommendations, it has no direct budgetary authority. It also has no authority, either review or management oversight, over the warrior components of the GIG.

- ***MCEB:*** *The MCEB considers those military communications-electronic matters, including those associated with National Security Systems, referred to it by the SecDef, CJCS, the DoD CIO, Secretaries of the Military Departments, and heads of DoD components. The MCEB provides guidance and direction to the DoD components and advice and assistance as requested. The MCEB has no budgetary review or execution authority over any component, nor is there any mechanism within the MCEB structure for enforcement of non-compliance with decisions. The relationship between the MCEB and CIO Executive Board is still being discussed, but in effect, the MCEB is a subordinate activity under the direction of the CIO Executive Board, and its recommendations referred to that board for final decision.*

Neither the DoD CIO Executive Board nor the MCEB have the membership or authority over budgets and execution activities necessary to ensure the GIG is built and managed as intended. Without that level of authority over all elements of the GIG, the architecture is subject to interpretation by each component based on their needs, rather than the needs of the entire organization. There is also little incentive to address cross-cutting issues in a coherent fashion when the funding for these programs is provided via Title X channels without some mechanism to insure cooperation. Because of the Title X and DoD versus Intelligence Community issues, the only level of management senior enough to cross this bridge is at the DepSecDef level. Additionally, neither of these two boards has a direct oversight responsibility over any specific office or function which carries out its direction such as the relationship described between the GIG Executive Director's office (a function which does not currently exist) and the DoD "Information Superiority" Board of Directors.

Consistent with its findings that under current organization, methods, and procedures the DoD is unlikely to realize a measured, consistent, and effective approach to creation of a Global Information Grid, the task force recommends the formation of a DoD Board of Directors for Information Superiority.

- *The Secretary of Defense should create the Information Superiority Board, with membership consisting of the Deputy Secretary of Defense (as chair), the Undersecretary of Defense (Acquisition, Technology and Logistics), the Vice-Chair of the Joint Chiefs of Staff (VCJCS), the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and the Director of Central Intelligence.[6] A single member from each service may be important as well.*
- *It is further recommended that the Information Superiority Board create an Advisory Group under Federal Advisory Committee Act regulations (or as a permanent DSB panel) consisting of senior private sector IT leaders.*

---

[6] Reference: DSB Task Force on Tactical Battlefield Communications report

- *The Advisory Group's purpose is to provide the Board with up-to-date knowledge of current and emerging commercial information systems, services, and network technology of potential use to the DoD in the realization of its Global Information Grid.*
- *It is also expected to offer experience-based advice from industry as to the best technical and management methods for creating such an infrastructure.*
- *The Advisory Group should consist of recognized industry experts in inter-networking technologies, commercial information and network security technologies, emerging information transfer technologies and systems, and other commercial activities such as standards development, infrastructure development, and the like.*
- *The Advisory Group charter should also ensure that the group provides independent assessments and counsel to the Information Superiority Board concerning the achievement of the goals and objectives set forth in task force recommendations that follow.*

2. Executive Director and GIG Implementation Process[7]

Placing the proper emphasis on GIG implementation and ensuring adherence to the policies established in accordance with the previous recommendations requires continuous oversight. It is therefore recommended that:

- ***The Board of Directors for Information Superiority create, by 1 June 2001, an Executive Office responsible for leading the implementation of the DoD-wide common user internetwork on behalf of the board. The Executive Director should be responsible for programmatic oversight for all DoD C4ISR systems acquisitions (including those procured by the Services) and through this oversight ensure that all such systems are interoperable within and as part of the GIG. It would be the Executive Director's primary responsibility to deliver the GIG.***
  - *Implementing the GIG*
    - *The Board should establish an Executive Office responsible for leading and implementing the DoD-wide, common-user internetwork (transport component of GIG)*
  - *Executive Director should be a minimum five year appointment*
  - *The Board should provide system engineering resources to the Executive Office through a dedicated system engineering team comprising 20 to 30 outstanding network systems engineers drawn from throughout DoD.*

[7] Reference DSB Task Force on Tactical Battlefield Communications

Time:

- *Office and Leadership Position Established by 1 June 2001*
- *Systems Engineering Office and Billets set up by 1 June 2001*

Cost: $10M per year

3. GIG Implementation Plan

A well-defined, measurable, and clearly understood GIG implementation plan is an essential step in ensuring a functional and secure infrastructure.

- *The Executive Director should be tasked to develop a GIG implementation plan, to include technical milestones, measurable interim goals, and an estimate of the resources necessary to complete transition and realization of the GIG by 30 September 2003.*
  - *The Board of Directors should provide manpower billets for a system engineering team to support the Executive Director. A cadre of 20 to 30 outstanding system engineers with backgrounds in Internet telecommunications and security technologies should be selected from throughout DoD. These individuals must be exceptionally proficient technically and visionary in their system engineering skills. This system engineering team would provide independent technical inputs to the Executive Director regarding the many responsibilities this individual will be given as noted in the next paragraph.*
- *The Executive Director should immediately establish a process to transform DoD information infrastructure systems from their present stovepipe configurations into a global DoD-wide common-user virtual intranet, the GIG. This transformation must embody the current and evolving commercial IT standards, protocols, and technology, with the goal of reducing inefficiency in spectrum usage and the costs of information transport, storage, retrieval and management. Most important, this transition should enable new operational flexibility that can be leveraged by warfighters.*

4. GIG Policy and Guidance

Existing policy and guidance is insufficient to meet the needs of GIG implementation. A solid and easily understood framework of policy and guidance is essential.

- *The GIG Executive Director should immediately set policy and guidance for GIG IAA. Specifically, ambiguities regarding an IA reference model, system architecture and technical architecture (as noted in the body of the IAA report) should be clarified. The Executive Director should establish this unified strategy and framework by October 2001.*
  - Executive director should establish a consistent IA strategy for all GIG networks
    - *Select reference model*
    - *Define a single system architecture*

- *Address tactical & strategic systems integration issues*
- *Utilize Joint Technical Architecture (JTA) security chapter as single source IA standards*

Time: by 1 October 2001

Cost: already included in recommendation II

5. GIG System Architecture

Implementation of a functional GIG system architecture requires detailed coordination and buy-in from key players.

- *Finally, the GIG Executive Director should work through the CIO Executive Panel and the MCEB to implement the GIG system architecture. Specific system architecture and implementation issues that need immediate attention include:*
  - *Continuing to aggressively deploy PKI, and addressing scalability issues*
  - *Aggressively pursuing NSA KMI initiative, addressing scalability issues*
  - *Deploying PKI-enabled subscriber security protocols: IPsec, SSL/TLS, S/MIME*
  - *Developing Type 1, high speed (multi-gigabit) IPsec devices*
  - *Constraining SIPRNET and JWICS network connectivity security policies*
  - *Deploying network infrastructure security technology: DNSSEC and Secure Boundary Gateway Protocol (S-BGP) (under development now)*
  - *Deploying diverse intrusion detection systems at WAN and enclave boundaries and in hosts*
  - *Moving all public DoD web sites of NIPRNET*
  - *Directing Defense Information Service Agency (DISA) to transition subscriber interfaces to IP (consistent with availability of suitable Type 1 crypto)*
  - *Employing spatial redundancy and design diversity for critical servers*

6. Budget to Support the GIG

In order to effectively implement the various aspects of planning, coordination and policy, adequate funding must be placed against this task. Otherwise, the effort will become a hollow attempt at cutting corners, with high likelihood of increased vulnerability and limited operability.

- *To support GIG implementation and to accelerate the DoD PKI/PKE strategy, the Panel recommends an increase in budget of 50% over what is presently planned. This increase should not only accelerate the strategy, but also fund the development of Type 1 high-speed IPsec devices. This funding increase should be complemented and supported by the IA S&T investments discussed in Chapter Three.*

7. GIG IA Testbed

Due to the ever-changing nature of today's technology it is essential to be able to test and evaluate emerging technologies before they are embedded into critical systems, without degrading ongoing operations.

- *The task force recommends that the Executive Director's system engineering office establish a GIG IA research and development testbed. The testbed nodes should be located at ESC, CECOM, SPAWAR, AFRL, NSA, etc. The participants in the evaluation process will include research and development, evaluation and operational communities (services and agencies). The testbed will provide a means for measurement of system performance in the face of Red Team attacks on Blue Team scenarios and related information traffic. The testbed will also serve as a primary means for DARPA Information Assurance technology insertion and evaluation. The metrics and measurements will evolve as results are analyzed and lessons learned are derived from the data. Lessons learned will be fed back to red and blue teams to refine and update strategies and will be used by developers to improve system defenses. Lessons learned will also be made available to the GIG architects and system engineers to improve IA for the deployed system.*
- *The testbed should be used to engineer, evaluate and update defense-in-depth (DID) strategies and technologies. The testbed will provide the means to understand residual DiD (and GIG) vulnerabilities and thus facilitate cost/benefit analysis for GIG IA investments. As noted in the task force's findings, no rigorous means for evaluating DiD systems, architectures, or technologies exist today.*
- *The testbed should be implemented no later than July 2001, and augmented to support GIG IA technology, architecture and metric evaluation over a five-year period.*
- *Additional tasks for the GIG IA R&D testbed include:*
  - *Develop metrics for protect, detect, and react (consistent with JV2020)*
  - *Combine real networks with simulation to achieve sufficient scale*
  - *Relate testbed experiments to real world via selected exercises and experiments*
  - *Test, evaluate and determine vulnerabilities, including wireless*
  - *Transfer results to GIG as P3I*
  - *Provide feedback to industrial base*

Time:

- *Establish version 1 testbed by 1 July 2001; Support test, evaluation and analysis efforts and testbed upgrades through 06*

Cost = $200M over five years

8. Public Key Infrastructure

- *The task force recommends that the DoD begin the process of incorporating IA, and specifically PKI/PKE, into the DII COE. In discussing alternatives with representatives from DISA, it was noted that the Common Operating Picture (COP) application is critical to CINC and Services Joint-Task-Force-mission success. For a modest investment focused on PKE of this application, an acceleration of PKI into the COE – as generic, run-time utilities – can be accomplished. In addition to gaining important experience with PKE in battlefield applications, PKI could be integrated into the COE setting software standards and infrastructure for use in other Service and CINC C4ISR systems.*
- *Although IA infrastructure is planned to be incorporated into the COE "sometime in the future", the task force believes that accelerating this process is critical to ensure consistent PKE with tactical C4ISR systems. Experience gained sooner rather than later is key to effectively deploying an IA-enabled COE for the GIG.*
  - *Director DII COE office should develop IA infrastructure consistent with GIG system architecture*
    - *Select operational application and integrate PKI with Services (e.g., COP)*
    - *Establish Common Operating Environment (COE) generic IA services using NSA Key Management Infrastructure (KMI)*
    - *Provide generic services as COE infrastructure and DoD PKI as available*

Time:

- *Develop and deploy PKE COP by 1 September 2002*

Cost = $10M over two years

CHAPTER 3. TECHNOLOGY

"Science and technology multiply around us. To an increasing extent they dictate the languages in which we speak and think. Either we use those languages, or we remain mute." ~ J. G. Ballard

3.1 Technology Drivers

In order to assure the availability and integrity of critical DoD computer networks, the Department must develop a long-term strategy that couples a desired end-state for information assurance that is consistent with JV2020 with a roadmap for achieving that end-state. While many areas need to be included in an overall roadmap, the information assurance R&D roadmap is fundamental. An information assurance R&D program supporting the protection needs of the Global Information Grid is essential for DoD to be prepared on the scale required.

The information volume that JV2020 will need to handle and protect will be vast. It is already possible to project data rates in the range of multiple terabits per second that will require protection. While secure remote access to data will somewhat reduce the requirement for data rates and bandwidth that increase in proportion to the size of databases, it is still obvious that protecting information in the volumes required for successful execution of JV2020 will be a daunting task.

In addition to defending DoD computer networks, we must be able to rehabilitate them. It has recently been understood that no matter how effective the defense of computer networks is, there will always be vulnerabilities that a determined adversary or disgruntled employee will discover and exploit. Experience shows that as America's defensive capabilities increase, so too will the adversary's offenses. U.S. adversaries over the next 20 years will be developing a range of attack capabilities that will likely cover every possible node and path of DoD networks.

There will certainly be attacks against DoD networks. Many will be ineffective, but more importantly some attacks will succeed. The results of a successful attack will range from an irritation or embarrassment all the way to serious disruption of critical DoD networks or information. The severity will depend on the attacker's skill level and resources and on the defenses DoD has in place. These attacks could result in serious damage to a critical DoD network, but could also compromise a warfighter's confidence in the information system he or she has to rely on, no matter what the attack actually accomplished.

Today, DoD has no methodology for dealing with the consequences of a successful attack and restoring integrity in its systems. And so, with the ever-increasing reliance of DoD on computer networks as an integral component of warfighting, this task force finds that it is now necessary to develop technologies to help recover and restore DoD networks and the data they contain. One of the key tasks in this area will be to restore the integrity of networked computer systems that have been attacked, or are thought to have been attacked, and restore confidence that they remain ready for their intended purpose. Warfighters must have confidence in their information and the technology that provides it. The technologies that will deliver effective defense-in-depth of DoD,

recover and reconstitute those networks after an attack, and restore their integrity, need considerable emphasis.

It should be noted that any list of research areas compiled today would certainly not be a complete list for tomorrow. Part of the Information Assurance R&D management challenge in the rapidly evolving world of Information Technology is the frequent examination of those research areas most needed to provide defense of and integrity restoration to the latest computer network developments and deployments. Against the tide of technological advances and determined adversaries, considerable R&D will be required just to maintain the level of security DoD has today. Much of the R&D required by the DoD will not come from the private sector. To achieve and maintain the higher levels of protection required by JV2020, it will be necessary for DoD R&D investment to keep pace.

The DoD must provide the support for an aggressive R&D program that has the breadth and depth to deal with the entire spectrum of information assurance issues. These range from near-term needs to thwart the latest threats that pop up, to long-term basic research. The latter must be coupled with an examination of the R&D strategies necessary to satisfy the full range of JV2020 requirements. Further, the R&D program must result in products that are unique to DoD requirements and which complement and enhance commercial systems. Many of these research programs will necessarily be long-term – and thus not suited to short-term evaluations.

What the funding levels should be is likely to be a matter of debate, but the general level needed is at least a factor of two over the DoD Information Assurance R&D spending of today. There are many areas that are minimally funded, which this report highlights. There are certainly many more areas that time did not allow the task force to pursue, or that have simply not yet been articulated.

What is clear, however, is that the preponderance of R&D expenditures have been on technologies principally related to perimeter defense of our systems and networks. Encryption, firewalls, intrusion detection devices and visualization tools have all focused on protecting the perimeters – in the same way we lock doors and place fences around sensitive or important installations. Now however, we must add significant technology developments oriented to insider threats, successful intruders and restoring integrity of our systems.

Defense-in-depth. The Department of Defense must continue existing work to provide and improve the defense of network and systems boundaries, or perimeters. In addition to those perimeter defense activities, the DoD must now develop extensive defense-in-depth capabilities as well. Thus substantial new R&D funding is required.

3.2 Promising Technology Areas for Investment

What follows is a general description of some representative technologies that this task force believes currently need increased attention.

Early Capability Assessment. Computer Network Defense, like any defense, is most effective if the intentions and capabilities of an identified adversary are understood, and when it is known that offensive operations have, in fact, begun. The technology for this entire area , including intelligence, indications and warning, intention, and identity determination, is complicated by legal and policy issues, which are discussed in Chapter 5 of this report. Examples exist today of attacks which have gone unnoticed, of intrusions with unknown purpose, and of

network disruptions that have remained un-diagnosed. This is a technology area that must mature as JV2020 develops. Some necessary research topics include the following:

Cyber Intelligence Tools. Advanced active agents using secure mobile code should be developed that could gather information without taking any hostile actions. "Picket" or "sentinel" agents could provide early warning of hostile action or intent. This program will ideally result in an array of tools that will provide a much greater understanding of hostile IO capabilities against the United States and its allies and better warning of incipient attacks.

Attack Pattern Discovery. No methods exist for automated or assisted discovery of existing or novel attack patterns or signatures, particularly for those attacks, which are distributed across many computers or networks.

Prevention and Protection. Much of the progress within DoD since the 1996 DSB report has been in the area of protection of DoD networks and prevention of unauthorized access. These are very important and sensible places to begin the defense process. However, as DoD becomes more and more dependent on networks, and as the complexity of these networks increases, the opportunities for disruption will also increase. R&D is required that is specifically designed to prevent problems caused by both insiders and outsiders, to prevent unknown attacks, and to guard against commercial systems with unknown flaws. The science of network security is currently immature, but with proper R&D infusion, the foundation for the protection required by JV2020 can be put in place. Representative areas of research to enhance protection of DoD networks and prevention of unauthorized access would include the following:

Scalable Global Access Control. Current DoD network architecture calls for a secure network with authorized access via tokens – a public key infrastructure (PKI). The scope of this security apparatus is enormous. It will involve distribution of secure capability to multiple locations in many countries. It will require limited access for foreign coalition partners. It will necessitate the distribution of millions of tokens. For example, the 2 million system users in DoD will each require one token for NIPRNET, another for SIPRNET, yet another for JWICS, and possibly another for e-mail. Thus it is estimated that the DoD Public Key Infrastructure will manage in excess of 4-6 million tokens, thousands of which will be issued or revoked each day. It will require rapid implementation and expansion during a period of crisis. It cannot burden the user. It must withstand insider attacks. These are severe requirements. PKI has not been modeled and tested under extremes of this type anywhere in the world. It is the security backbone of the future, and must be supported by a vigorous R&D program, which will test features including its scalability, its extremes, and any vulnerabilities. It requires the same attention to detail that continuous testing of high-grade cryptographic systems has received over the past several decades.

Malicious Code Detection and Mitigation. The need to nullify malicious code is acute for both the Defense Information Infrastructure and the National Information Infrastructure because of increased connectivity and reliance on the Internet, increasing prevalence of mobile code, and the likely development, access, and remediation of code by disgruntled insiders and outsiders. The DoD is unable to determine how many "low and slow" attacks (like Moonlight Maze) have occurred, nor what malicious codes have been left behind.

Mobile Code Security. Mobile Code Security decomposes into three challenges: to protect hosts from malicious inbound code; to protect code from malicious hosts; and construct survivable distributed systems capable of tolerating compromised elements. Consider how much commercial code is added to DoD systems each month around the world, all without testing for malicious code.

Anomalous Behavior Detection. The technologies for detecting anomalous behavior are too brittle to produce robust and useable results. Outcomes are laden with false alarms and missed events, both of which increase human and system workload, while reducing confidence in results. These technologies are badly needed for mitigation of the insider threat, as well as for underpinning downstream technologies for detection of related threats.

Fault Tolerance. Fault tolerance technologies have been successfully used to construct highly available and reliable systems for transportation and financial sectors as well as real-time control of plants, vehicles, and command-and-control systems. Such fault tolerant systems have been designed to cope with naturally occurring faults and failures such as hardware component faults, design errors in software, and environmentally induced faults such as transients caused by lightning. Advanced research is needed to adapt these technologies for intentional faults and attacks mounted by a human adversary. Research is also needed in creating fundamentally new intrusion-and-attack tolerant systems that use and exploit design diversity, stealth, randomness, and uncertainty as built-in system attributes.

High-Speed Encryption. Over-the-network access, both to classified and unclassified-but-sensitive information, is of critical importance as the Global Information Grid becomes reality. The near-instantaneous global access available once one is "inside" the protected network raises the issue of how to recover quickly from problems such as the loss of an encryption device. There is also the necessity to rapidly add or remove coalition partners from a network during international operations.

For the DoD to conduct operations using the GIG, it must have the ability to almost instantaneously remove selected (compromised) users from the grid, while at the same time, permitting the remaining users to continue to conduct their operations. Important pieces of this complex problem are being solved. The STU-3 model was a start, but the supporting infrastructure does not scale to required levels. There are upgrades underway, but they are not of the scope necessary to address JV2020 requirements.

At least three major technical challenges exist. First is the development of a high-speed encryption device that can scale to the 10 Gbps rate and beyond for both Asynchronous Transfer Mode (ATM) and Internet Protocol (IP). A second challenge is to build an encryption device that is protocol, algorithm, and key agile. This class of device is required if the GIG is to be interoperable with legacy devices and with coalition partners. The third challenge is to reduce the cost and to integrate all the security functions into embedded capabilities that are transparent to the users. The more transparent the security functions are, the more they will be used and not bypassed in time of crisis. The DoD needs to work with the vendors in the earliest stages of developments to integrate highly scaleable security into their products.

Advanced Intrusion Detection/Monitoring. Intrusion-detection technologies currently produce only moderately reliable results in simple environments, and even less-reliable results in complex environments. In terms of correlating and fusing information from distributed sensors in distributed attacks, what little technology exists is too immature to be useful. Intrusion-detection

technologies are critically dependent on monitored sensory data. However, with respect to what is monitored and the places from which the monitoring data are taken, little to nothing is known about either how to decide what should be measured, or how to determine the most effective placement of sensors in an operational environment.

Consequence Management. Some network attacks will be successful and DoD does not have adequate technology in place to address the consequences of the successful attacks. Research is needed to improve our ability to address these consequences. Some of the areas that should be included in a research program are self-healing networks and systems, network isolation, integrity restoration, and recovery and reconstruction.

Integrity Restoration. DoD does not have a methodology for restoring integrity in its systems. If a user loses trust in a system, because of an attack (internal or external), or because of a perceived problem, there is a need to validate that the system is performing all functions accurately. Trust in a system can be lost as a result of bad data, natural events, degraded performance, fear of tampering, inconsistent data or decisions, or anything that causes the user to question the usefulness of the system. Tools and methodologies are needed to address system user questions such as: Was something done to the system? What was done to the system? Is the system OK? Is the data reliable?

Recovery and Reconstitution. When a network or system is successfully attacked, there is a need to return it to a useable level of service and ensure that the same attack will not produce the same negative result. Recovery is the process of taking a system from an unacceptable level of performance to a minimum level. Reconstitution is the process of taking a system from the unacceptable or minimum level of performance and returning it to full performance. In addition, the reconstituted system should not be susceptible to fail in the same way from the same attack. The ability to recover and reconstitute a system will increase trust, improve protection against future attacks, and provide systems that have increased availability.

Attribution. Once it is determined that a network has been attacked, automated tools are necessary to understand exactly who initiated the attack. Attribution is essential to establish the attacker's motive and to determine an appropriate response. An extensive R&D program focused on attribution needs to be developed. This is an area where extensive civil, law enforcement, and DoD interaction is essential. Some suggested areas of research include the following:

Message Signature Processing. Advanced research is needed to develop algorithms that transform extremely high bandwidth Internet traffic channels into near-real-time searchable signature spaces such that an attack can be quickly correlated against the passively collected signature stores at multiple nodes. Near-real-time correlation capabilities could narrow the potential set of attributable source points and facilitate rapid engagement of appropriate traps and traces.

Active Code Beacons. Attacks that rely on covert target responses could theoretically be co-opted by the infusion of active code beacons in the return traffic – beacons that would provide attribution information. Research is needed to develop this and other active attribution concepts.

Identification Friend or Foe (IFF) tools. Research in this area would determine if the Identification Friend or Foe concept could be extended to cyberspace to support authentication functions with minimal resource requirements.

Cross-Area Research. There is a broad category of needed R&D that does not fit within the attack phases described earlier, but rather is common to most or all of them. Precisely because of this somewhat non-specific nature, there is much less research being conducted than necessary for the long-term health of the GIG, and DoD's overall information infrastructure. In most cases, this R&D lacks a logical "ownership" – it often does not fall clearly within the responsibility of an organization or an industry, and as a result is insufficiently funded. The most important areas of research that cut across the attack timelines are Modeling and Simulation, Theory of Vulnerabilities, Broad Based Fundamental Research and GIG Research Coordination. To date there has been very little research into the interdependent effects that can accompany the interconnection of multiple infrastructures, both of the same general type and completely different ones, e.g., the interdependencies between information networks and the electric power grid. The possibility of cascading and nonlinear effects from such interdependent systems is rhetorically acknowledged but little understood or studied. While responsibility for networks or other infrastructures is often easily identifiable, no organization has an institutional responsibility for interdependent effects. As networks and infrastructures become ever more tightly interconnected, the likelihood and magnitude of such effects will become greater.

This research would seek to understand the nature and origin of interdependent effects and how they propagate among infrastructures of varying degrees of complexity. Feedback control theory, network analysis, advanced modeling techniques, and other disciplines would be used in conducting this research, which would seek to assess both intentional (hostile) attacks and naturally occurring instabilities (such as network "storms"). As research progressed, infrastructures with increasing numbers of nodes and interconnections would be studied. At some point, an IA test bed would become an invaluable tool for such analysis.

3.3 Recommendations

The GIG is an evolving weapon system and the United States is in an arms race. Experience suggests that as the U.S. defensive capabilities increase, so will the adversary's offense. To stay ahead of the adversary the task force recommends that the Department:

- *Task and resource the GIG Executive Director to create a vigorous sustained and balanced IA R&D program to maintain GIG security. Promising areas for investment include:*
  - *Scaleable network sensing, anomaly detection, diagnosis*
  - *Malicious code detection and high-speed network IA*
  - *Self-healing, recovery, and reconstitution*
  - *Traceback, forensics, tagging*
  - *IA modeling and simulation*

Time: *1 October 2001*

Cost: *Add $40M in first year; add $350M over 5 years*

- *Promising tools and techniques should be tested on the R&D test bed outline above.*

CHAPTER 4. READINESS

"Know your enemy and know yourself and your victory will always be assured."
Sun-tzu

4.0 Introduction

Of the many issues facing the Department of Defense in carrying out the DIO mission, the issues regarding organization and personnel readiness are among the most critical and most difficult to address. Without organizations that are appropriately structured and staffed with qualified people who understand what they are supposed to do and when, the most sophisticated and capable technology is not fully effective.

The Department has created organizations and realigned responsibilities to address the DIO area, such as creating the Defense-wide Information Assurance Program (DIAP), the JTF-CND (Joint Task Force for Computer Network Defense) and assigning the Computer Network Defense mission to USSPACECOM. The DIAP's role is to provide for improved coordination of the DoD IA efforts, maximizing the Department's return on its IA investments. It accomplishes this by continuous oversight and integration of all DoD IA-related activities. The JTF-CND was created to coordinate and direct the defense of DoD computer systems and computer networks. The UCP (Unified Command Plan) 99 assigned the mission of CND to USSPACECOM, effective October 1999, changing reporting assignment of the JTF-CND to USSPACECOM on that date. All of these organizations have made significant progress in accomplishing their tasks, but the roles, missions, and responsibilities, as well as personnel and funding resources, have been slow to catch up with the requirements. A number of recommendations made in the 1996 DSB report relate to these areas and, although progress has been made since then, much remains to be done.

The lack of clarity in roles, missions, and responsibilities has also affected those organizations responsible for carrying out Critical Infrastructure Protection (CIP) activities, or Homeland Defense activities, and their relationship to the DIO organizations. Two examples illustrate the problem: (1) the existence of the CIP and DIAP as separate entities within ASD(C3I) and (2) the responsibility of USSPACECOM for Computer Network Defense (CND) and coincident responsibility of the United States Joint Forces Command (USJFCOM) for Homeland Defense, where there may appear to be a conflict of responsibilities if there were a computer network attack against the homeland.

Four major categories of issues relate to how DoD is executing the DIO mission areas:

- Operational Readiness
- Organization
- Human Resources
- Resources

4.1 Operational Readiness

Embed DIO into Military Planning and Execution

DIO is not adequately integrated into mission planning and execution:

- Control conflicts exist between operational and support equities when services are disrupted
- Network discipline and CND compliance are issues of concern (training, SOPs, command emphasis)
- Issue of what Components should support the U.S. Space Command's CND mission is still under discussion
- CINCSPACE should develop Continuity of Operations Plan (COOP) should JTF-CND lose capabilities
- It has not yet been determined what CND information should be posted on DoD Global Command and Control System's (GCCS) Common Operational Picture (COP)
- It is not clear what the U.S. Space Command should protect as part of its CND mission beyond the SIPRNET and NIPRNET.

Integrating DIO into all phases of operational exercises, testing and evaluation, and operational assessments will better insure that network systems fully consider DIO from design through acquisition and integration and employment. Implementing DIO into training and plans will insure that operational plans consider the assuredness of the information they are depending on and that networks and network personnel are exercised and stressed to better respond when failures and attacks do occur. Planning and exercising for network attacks better prepares the on-scene commanders and operators to respond to the attacks or failures in a measured and appropriate manner. Accordingly, as part of exercises and operational plans, developing a set of responses, or delineating the rules of engagement for responding, will ensure that any response is appropriate, measured, and authorized.

Readiness Assessments, Reporting, and Metrics

There is neither a consistent nor an adequate system for assessing DIO readiness across DoD:

- Readiness assessment mechanisms are incomplete and fragmented,
- Numerous efforts are ongoing to measure IA/CND/DIO readiness of DoD activities (e.g., Chairman, Joint Chiefs of Staff Instruction (CJCSI) 6510.04 and DIAP IA metrics efforts),
- CJCSI 6510.04 does not address or apply to all DoD agencies, and is neither obligatory nor mandatory. It is intended to be used as a guide to develop Readiness criteria.

- DoD IA readiness includes measuring and assessing, evaluating, and improving and enhancing the readiness posture of DoD IA capabilities.

The success of operational missions is now, more than ever, dependent on the assured and timely delivery of information from operational commanders to operating forces. Planning for, testing, exercising, protecting, and resourcing the assuredness of those systems that deliver that vital information has not kept pace with the emphasis placed on using the information in some operational manner. Yet, assuring the security and availability of information is critical to DoD's success in peace and war, and is a key element of achieving information superiority. DIO readiness must be measured, assessed, evaluated, and understood for operational commanders to understand and achieve information superiority.

The DoD's information systems have been, and will continue to be, under attack. When disruptions occur to the flow of information, either through attack or system failure, operations suffer.

- System failures are often unpredictable and unavoidable. Network operations reconstitution after a system failure depends on the skill, experience, training, and ability of network technicians.
- System attacks are also often unpredictable and unavoidable. Responses and network reconstitution to network attacks also vary depending on system administrator skill, experience, training, and ability.
- Disabling a network as a response to the threat of attack has the same effect as a successful attack.
- The ability of any given command to better face the challenge of a system failure or attack is improved through planning, training, assessment, and practice.
- Some attacks might not disable or disrupt networks, but might corrupt information on the network in a subtle way. Readiness assessment must include integrity restoration capabilities.

Policy needs to be established which will lead to a structured, mandated, and recurring DIO assessment capability, across all elements of the Global Information Grid. An effective DIO readiness reporting mechanism, accompanied by a viable response mechanism to provide proactive and responsive solutions, is as important as anticipating ammunition shortfalls and assessing more traditional critical warfighting systems, and will in the end save money and conserve other resources. Many different organizations, elements, and activities must be brought together within the DIO readiness system construct to achieve synergy, efficiency, and effectiveness throughout all facets of the system.

Critical success indicators for the readiness system include the people, operations, training, equipment, infrastructure, and processes that characterize the DIO readiness posture of the DoD.

- *People*: The ability to attract and retain qualified, cleared, available, accountable, and motivated personnel to sufficiently staff DIO-related mission requirements.

- *Operations*: The ability of CINCs/Services/Agencies to ensure organizations, procedures, and tools are effectively synchronized to execute DIO actions in order to defend information capabilities – thus providing timely, reliable, integrated, and secure information to achieve mission objectives.
- *Training*: The ability to specify and then satisfy DIO training requirements across the DoD through external and internal education, training, and awareness programs which meet nationally and/or internationally recognized quality and curriculum criteria, which generate qualified and certified DoD DIO work force and users.
- *Equipment and Infrastructure*: The ability of the DoD's defense-in-depth architecture to ensure authenticated and authorized access to information across service and mission boundaries, throughout all applicable equipment and infrastructures (cyber and physical), and with adequate levels of confidence in information availability, confidentiality, and integrity while being processed, stored, or in transit.
- *Processes*: The ability of the DoD to institutionalize across the Department measurable, repeatable, reliable, valid, cost-effective, streamlined, consistently applied, and well-documented DIO processes.

Operationally Test Against a World-Class Threat

Due to lack of clear policy and resources, aggressive, comprehensive, effective operational Red Team activities are lacking across DoD:

- Operational Readiness Assessment involves the Cyber Operations Readiness Triad (CORT): vulnerability assessments, vulnerability evaluations, and red teaming,
- Vulnerability assessments, vulnerability evaluations, and an aggressive, no-notice red-teaming program are lacking across DoD,
- Red-teaming that is being done is inadequately funded, insufficiently staffed, poorly coordinated and hampered by lack of clear policy, and
- Formal Computer Network Attack (CNA) red-teaming efforts/definition/authorities have yet to be defined.

The purpose of an operational readiness assessment is to examine and test an information system or product to determine the adequacy of security measures; identify security deficiencies; provide data from which to predict the effectiveness of proposed security measures; and confirm the adequacy of such measures after implementation.

An intrinsic part of information superiority is the ability of a network system to survive a focused attack and continue to provide the information needed by operational commanders in a timely manner. The ability of any particular system to survive an attack can be attributed to the technical health of the system and to the skill, experience, training, and ability of the system technicians. Due to the networked nature of the Global Information Grid (GIG), a weakness within any particular system may cause vulnerability within the network as a whole.

Evaluating network technical health through testing for system upgrades and patches, proper password management procedures, and firewall standards, just to name a few procedures, is necessary to ensure that administrators have maintained their systems according to manufacturer updates and established procedures. Similarly, system administrators must be trained and exercised in recognizing and responding to unauthorized attacks and intrusions, from sources both external and internal to the system. Training and assistance teams provide vulnerability assessments of networks and help provide the local system administrators with the skills they need to maintain system operations.

The different equipment and software that make up information systems intrinsically have known and unknown vulnerabilities associated with them. Timely installation and maintenance of manufacturer upgrades and patches for known vulnerabilities help maintain a higher level of security and assuredness, but often comes after vulnerabilities become widely known and exploited. Thus, operations may be put at risk if the military community does not aggressively test, appraise, and evaluate the hardware and software that make up the information systems. Evaluations of hardware and software also identify vulnerabilities not widely known within the public domain and permit the military to work with developers to correct the vulnerability before hackers can exploit it. This level of evaluation, however, is best done during R&D and operations, test and evaluation (OT&E) so that network systems can be acquired that best meet the overall DoD information superiority objectives.

Actual readiness of in-place information systems can be measured only through the aggressive testing of a system by an independent (red) team. Red team assessments are conducted periodically within the DoD, but often with inadequate resources and limitations placed on their ability to conduct an aggressive assessment. The red teams are being used unevenly throughout DoD, which results in some commands being highly effective in thwarting network attacks while others may have minimal capability or skill in doing so. Also, different red teams evaluate systems using different standards and measures of effectiveness, which may lead to a false sense of security within certain commands. Since a potential aggressor seeks out the most vulnerable system to penetrate or attack to achieve his ends, this uneven approach to red teams may lead to an unrealistic sense of security when in fact, little exists.

Doctrine needs to be developed to guide the CORT process to ensure all of DoD is at the same level of DIO readiness. Specifically, red-team structures, authorities, responsibilities, and functions should be specified for all DoD activities, and organized in a manner to make maximum synergistic use of the teams and in-place assets. Accordingly, Operational Readiness Assessment Teams should be aligned for each of the military departments; Defense Threat Reduction Agency (DTRA) for Weapons of Mass Destruction (WMD) purposes; NSA for DoD and national requirements; and Joint Forces Command to organize reserve forces for appropriate missions.

Operational readiness assessments should be conducted often and randomly because any introduction of a new equipment or software upgrade changes the design, and hence the vulnerabilities, of the system. Highest priority should be given to upper echelon command and control systems, highly classified systems, and the systems of those forces preparing for operational deployment. However, each system within DoD should receive complete CORT assistance not less than every five years.

Because of the nature of networked systems, and DoD's reliance on contractors and vendors, policy should be extended to subject those contractors and vendors who are involved in applicable DoD activities to the same red-teaming standards as DoD.

Improve Emergency Response and Consequence Management

DoD Computer Emergency Response Team (CERT)/Computer Incident Response Team (CIRT) activities vary in their execution and are not inclusive of all DoD CINCs/Services/Agencies (C/S/A):

- Not all Defense agencies have or have access to CERT/CIRT-like services for their enterprises,
- Overall DIO readiness posture cannot be clearly understood today,
- Tools, response procedures, and reports differ among CERT/CIRTs, and
- Doctrine is inconsistent.

CERT/CIRTs provide analysis of external attacks against DoD network systems through reports from automated monitoring tools as well as manual reports from systems administrators to determine when unauthorized probes, scans, intrusions, and service denials occur. The information provided by the CERT/CIRTs permits a clearer understanding of the level, severity, and scope of network attack. This information is also used to alert other DoD network users of attack, and to permit counter measures to be implemented to mitigate the attack. The sum of all this information is a significant indicator of the readiness and ability of information systems to achieve information superiority.

Today, DoD activities use different tools to monitor network activity and, when suspicious activity is noted, report the information using differing methods and procedures, most of them manual. Further, the majority of these tools are based on identifying recognizable and known network security vulnerabilities, and are not easily configured to protect against emerging or changing technological threats. These differences and shortcomings mean inequities exist when NOCs (Network Operations Centers) measure and assess network health; these inequities can lead to inefficiencies throughout the system or a false sense of assuredness. For the reports to be valuable, it is important that they be derived from measurements that are accurate and timely, and be able to be dynamically updated to identify and warn against the most up-to-date threats as well as to distinguish other non-malicious activity. Additionally, to be easily accessed and understood throughout DoD, the assessments need to have a common format and reporting guidelines.

Due to the nature of their mission, technicians at CERT/CIRTs are significantly more adept than most systems administrators at understanding and mitigating network vulnerabilities. Therefore, CERT/CIRT technicians provide a critical technical capability and expertise for commands to draw from when needed, especially in preparation for or during operational employment. However, the current number of CERT/CIRTs and the number of technicians within the CERT/CIRTs, do not adequately meet the assessment and on-site assistance needs of CINCs/Services/Agencies.

4.2 Organizational

Organizational Roles, Missions, and Responsibilities

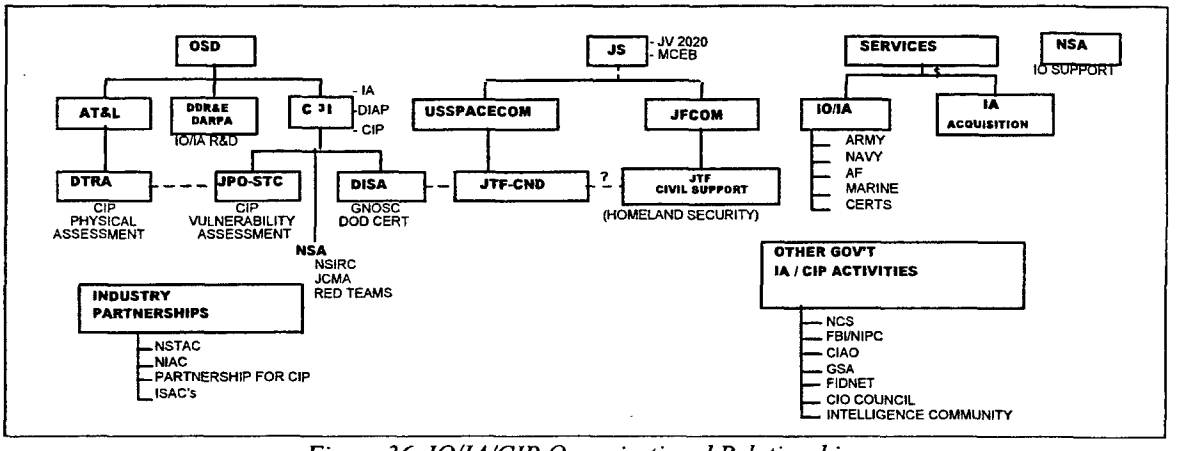


Figure 36. IO/IA/CIP Organizational Relationships

The DoD established the Defense-wide Information Assurance Program (DIAP) and the Joint Task Force for Computer Network Defense (JTF-CND) and its component activities as steps to coordinate and integrate IS activities. However, existing policy inadequately describes the responsibilities and authorities of these activities and extrapolation of existing policy has resulted in inconsistent interpretations of roles, missions and responsibilities across the DoD, as illustrated in Figure 36, above. The Department has conducted a number of studies, assessments and working groups to clarify the issue, but guidance to date in this area is incomplete. Additionally, where new missions have been identified, funding and manpower have been taken out of existing programs (if any were provided at all) and are inadequate to accomplish the DoD's objectives. As an example, the DIAP was created to provide oversight and integration of all DoD IA activities, but staffing problems have severely hampered its ability to meet either its assigned mission or expectations of leadership. An additional example is the assignment of the CND mission to USSPACECOM prior to funding and staffing decisions necessary to carry out that mission.

Other issues arise from the unclear roles, missions and responsibilities such as the distinction between the entirety of DIO, IA and CND. DIO, as defined in DoD Directives and Joint Publications, includes all activities within IA and some additional activities. CND is an activity within DIO, but is not all of IA. Different offices and activities within DoD are responsible for various areas of IO, but the relationships and boundaries among the activities and areas are unclear. A way of illustrating the relationships among these activities is provided in Figure 37, below.

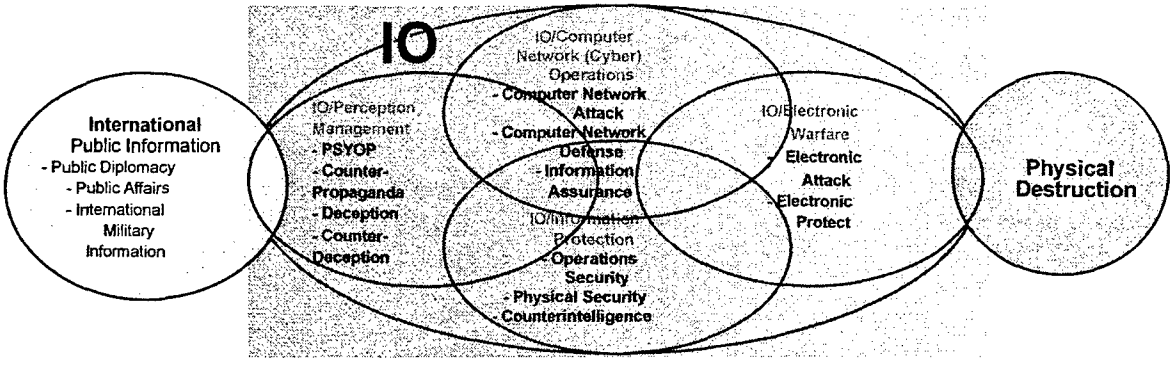


Figure 37. Information Operations Problems Space

The overlapping definitions and areas of interest cause confusion and conflict among a variety of DoD entities. For example, DoD's Critical Infrastructure Protection (CIP) programs are largely unfunded, in part because the responsibility for the actual protection of DoD's infrastructures is bifurcated and unclear. The sector leaders have little authority over the actual funding needed to support the programs and the beneficiaries of the results (the CINCs) have little say in the establishment of priorities. There is also considerable difficulty in determining actual expenditures in IO (offensive), DIO (defensive), IA, CIP, CND, etc; because of changing definitions and a wide variety of program elements associated with them. Additionally, some funding programs benefit more than one area, so the "binning" (assigning for accountability purposes) in one category or another is subject to interpretation by a number of different entities, generating additional confusion and reducing accountability. Another example of potential confusion is the scope of responsibility of the JTF-CND. Its mission is specifically CND, yet it is not clear what other IA responsibilities may or not be included in that mission, as there is an undefined distinction between "defense" and "protection" roles. This issue has resulted in significant difficulty in executing a number of processes (Information Conditions [INFOCONS] and Information Assurance Vulnerability Alerts [IAVAs]) where operational imperatives are dependent upon Title 10 funding of day-to-day operations and maintenance activities.

As the concept of DIO has evolved and matured, concerns have been raised about the appropriate roles, missions and responsibilities of the CINCs/Services/Agencies in this area. Recent real-world events and exercises have indicated that clarification of roles and responsibilities are absolutely essential. Additionally, the reality is that many of the activities being targeted and those, which support the infrastructure, are not under the control of the DoD, i.e. the commercial infrastructure. This situation has required the Department to establish strategic partnerships in those instances where they do not exist and reinforce those that do with industry and other Federal and State government activities. These strategic partnerships lay the foundation for appropriate policy and response. For example, the NSTAC (National Security Telecommunications Advisory Committee) is an existing partnership between government and leading telecommunications industry companies, which provides industry views and expertise on the commercial telecommunications and information systems, networks and infrastructures. It has been in existence for eighteen years, providing advice on complex information technology policy issues. Members of NSTAC companies also participate in the National Communications System (NCS) National Coordinating Center (NCC) for telecommunications involved in commercial network operations.

4.3 Human Resources

Find and Keep IT Talent

Maintaining a cadre of DoD personnel with critical IT skills is essential for successful implementation and execution of the GIG; and yet, the shortage of IT professionals within DoD is serious and growing. The complexities of solving the DoD shortage of IT professionals, when viewed in the larger context of the private sector are serious. Shortages in the supply of IT professionals are not confined to the DoD – they exist for other federal agencies, nationally and globally. More than 1 million information technology jobs are vacant around the world and the number is likely to increase. By 2002, there will be 850,000 vacancies in the United States and more than 1 million in Europe.

Recruiting is difficult when colleges and universities are only producing enough IT graduates to fill half of the growing annual requirement. Several U.S. companies have begun recruiting foreign nationals to fill their IT jobs. Under the H-1B non-immigrant category of U.S. immigration law, U.S. employers may sponsor 65,000 professional foreign nationals each year. This was just one congressional effort to try to narrow the gap. The turnover rate among IT professionals in the private sector is 30%, five times the rate for other skills in the private sector as a whole. The private sector is, therefore, providing a number of incentives to combat these shortages.

The Department's ability to compete with the private sector in the area of compensation is limited by personnel practices and guidelines, and by law, in the case of military personnel. The private sector is able to react quickly to any substantive change in market values for IT skills – something the government has difficulty accomplishing. However, there are some government authorities that offer limited relief.

The Office of Personnel Management (OPM) authorized specific flexibility for civilian personnel to help address the government-wide recruiting and retention problems facing managers.[8] A recent Integrated Process Team (IPT) within DoD revealed that little flexibility is being used within the Department.[9] Many reasons can be given for this situation, including an unwillingness to differentiate between civilian employees on different types of pay scales, but the most significant reason is lack of funding. As the DoD has sought to reduce its size, the number of and funding for personnel and personnel incentives has also suffered. Instead of targeting reductions to functions that are no longer needed, most activities have taken percentage reductions across the board, exacerbating shortages for key skills. A recent OPM announcement authorizing higher pay for IT workers, as well as release of the Parenthetical Classification Titles and Competency-Based Job Profile (Qualification Standard) for the Computer Specialist Series GS-0334 and the Telecommunications Series GS-0391 will dramatically improve the ability to manage the civilian IT workforce.[10]

---

8 "Recruiting and Retaining Information technology Professionals," Office Personnel Management, November 1998.

9 Information Assurance and Information Technology Human Resources Integrated Process Team, ***Information Assurance and Information technology: Training, Certification and Personnel Management in the Department of Defense***

10 "Higher Pay for Information Technology Worker," Office of Personnel Management, CPM 2000-13, 3 November 2000; "Special Salary Rates for IT Workers," Office of Personnel Management, CPM 200-14, 3 November 2000; Parenthetical Classification Titles and Competency-Based Job Profile (Qualification Standard) for the Computer Specialist Series GS-0334 and the Telecommunications Series GS-0391, OPM (draft)

On the military side, the Services have recognized the need for key IT skills and have begun targeting recruiting and retention bonuses to encourage individuals to remain on active duty. Although government bonuses cannot compare with what is offered by the civilian community, they are a tacit recognition of the pay discrepancies. Additionally, other incentives, such as choice of duty assignments and schools are used to entice military personnel to remain.

Even with adequate incentives, there will be insufficient personnel with specific technical skills available for DoD. This means that a realistic approach to solving the problem must consider outsourcing as an alternative. This approach was explored in some detail by a separate Defense Science Board Task Force on Human Resources Strategy, which recommended assigning military and DoD civilian personnel to those tasks essential to the business of governing and those, which only the military can do. All others should be addressed by the private sector for those functions it does best.[11] This alternative, however, should not be seen as a way to save money, but instead as a method to augment and acquire key IT skills. Unfortunately, in the rush to outsource, little thought has been given to careful planning of what should and should not be outsourced. This planning requires a clear statement of "Inherently Governmental" that is understood and executed in a consistent way. Unfortunately, no such clear definition exists. Although there is a policy document, which describes "Inherently Governmental", the applicability to the IT arena is not clear.[12] There is a current effort to provide this clarification with an Integrated Process Team consisting of Undersecretary of Defense for Personnel and Readiness (USD(P&R), Undersecretary of Defense for Acquisition, Technology and Logistics (USD(AT&L) and Assistant Secretary of Defense for Command, Control, Communications and Intelligence (ASD(C3I) membership. With this clarification, DoD should develop an outsourcing strategy for key IT skill sets that complement those available from DoD civilian and military personnel.

Other, more creative alternatives should also be considered. It is well established that IT personnel move more frequently between jobs than those in other skill areas. This makes it difficult to encourage individuals to enter government service if the potential job candidates expect that the choice is, in fact, a long-term career choice. The DoD should acknowledge the fluidity in the information technology profession by creating alternatives to attract needed resources in these critical areas. One alternative may be an "Education and Training for Service" (ETS) model which requires a minimum payback of employment for education. This program could provide dual benefits in encouraging more students to consider an IT career, as well as providing education incentives with a promise of employment. It could also provide constant refreshment of talent in a constantly changing IT environment. For example, DoD could establish a program in which talented high school graduates could enter Service or join the government, and be trained to be "world-class" systems administrators. In exchange for this training and experience, the U.S. government could require payback for example of five years service. Of course, the DoD would encourage participants to stay longer through career programs and continued professional development. Additionally, enhanced retention pay could be offered such that IT professionals could accumulate some amount of money for each year of service, say $5,000 per year: they can collect after the 15th year.

---

[11] Defense Science Board, ***Report of the Defense Science Board Task Force on Human Resources Strategy***, February 2000, p. vii.

[12] OFPP Policy letter 92-1, "Inherently Governmental Functions," 23 September 2000.

Sensitize and Train Users

The DoD workforce at all levels is ill prepared to execute the DIO mission because current training efforts are fragmented, inadequately scoped, and poorly documented. The attacks against the DoD's information infrastructure have heightened awareness of the importance of training as a critical component of protecting the Department's information resources against attacks. Because of the shared risk environment created by highly connected and interdependent information systems, all individuals using, administering, maintaining, and managing systems and networks must understand the threats and the policies, procedures and equipment designed to mitigate these threats. This training continuum (from cradle to grave, from the lowest civilian and military to the highest) will ensure that all personnel understand the threat and their role in protecting DoD's networks. An analogous program that can provide insight into how training affects successful mission performance is the safety program, particularly in the area of aviation safety.

Training for all users of DoD computer systems is mandated by statute,[13] with additional guidance provided by Office of Personnel Management (OPM) regulation,[14] Office of Management and Budget (OMB) Circular,[15] and DoD Directive.[16] In spite of this direction, user training has been implemented unevenly, requiring issuance of additional guidance by ASD(C3I) and USD(P&R) in 1998.[17] This policy memo also levied an initial requirement for system administrator and maintainer training and certification. Outside of user training, the level and content of training in the Department varies. In some areas there are comprehensive training programs available for all DoD personnel. Unfortunately, the Department does not take full advantage of these programs. In other cases, training has been either unavailable or too expensive for the IA workforce. As a result, the level of training for the DoD IT/IA workforce is uneven at best. The training content also varies across the Department, which is a potentially serious threat to the Department's joint warfighting capability. The previously mentioned policy did not address this issue, nor did it address training for personnel performing other IA functions, or establish a permanent, recurring requirement for those identified functions. That task was taken on by an Integrated Process Team (IPT) established in September 1998 by ASD(C3I) and USD(P&R).[18] This IPT produced a report that made a series of recommendations to begin establishing permanent training and certification requirements for critical IA functions.[19] The report resulted in a recently signed DepSecDef policy memo.[20]

The Department has made great strides in developing and implementing a DIO training continuum, but much work remains to be done. As the training requirements are developed, they need to not only incorporate the emerging OPM civilian personnel standards, and be validated against commercial sector standards (where those exist), but must also be included in the formal training mechanisms of the Department. Without this formalizing of the requirements into the normal training mechanisms, they will not become institutionalized into the way the Department

---

13 Public Law 100-235, ***Computer Security Act of 1987***.

14 OPM Regulation 5CFR930. 301-305, 3 Jan 1992.

15 OMB Circular A-130, 8 Feb 1996.

16 DoDIR 5200.28, ***Security Requirements for Automated Information Systems (AIS)***

17 OSD Memo, Subj: ***Information Assurance (IA) Training and Certification***, 29 June 1998.

18 DepSecDef Memo, ***Implementation of the Recommendations of the Information Assurance and Information Technology Integrated Process Team on Training, Certification and Personnel Management in the Department of Defense,*** 14 July 2000.

19 ***Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense,*** Information Assurance and Information Technology Human Resources Integrated process team, 27 August 1999.

20 DepSecDef Memo, Subj: ***Implementation of the Recommendations of the Information Assurance and Information Technology Integrated Process Team on Training, Certification and Personnel Management in the Department of Defense,*** 14 July 2000.

does business. Additionally, it makes little sense to require military and DoD civilians to be trained to a standardized requirement if contractors performing the same functions are not held to those same standards. The recent DoD Chief Information Officer Global Information Grid Guidance and Policy Memorandum (G&PM) establishes the initial requirement for such standards.[21] Realizing that this may require modification to existing contracts, contracting officers need to ensure that any contracts, or modifications to existing contracts contain standardized requirements and performance metrics to hold contractors accountable for meeting these requirements.

Reserve Component

The DoD increasingly relies on its reserve component to fulfill its mission, both from a resources and skills available standpoint. The Reserve Component Study, Feb2000, was chartered to provide recommendations to the ASD(C3I) on the subject of expanding the role of the Reserve Component (RC) in domestic preparedness in two specific areas of defensive information operations: information assurance and computer network defense. The study made two recommendations: 1) bolster RC support for USSPACECOM and JTF-CND, and to the Services by strengthening the RC support to the Service component commands (Land Information Warfare Activity [LIWA], Fleet Information Warfare Center [FIWC] and Air Force Information Warfare Center [AFIWC]) and 2) establish Service Joint Reserve Component (RC) Virtual IA/CND units.[22]

Virtual RC support to LIWA, FIWC and AFIWC can provide several advantages. The increase in virtual manning could result in improved mission accomplishment and extended "normal business hours" coverage (the United States' Reserve Components in States encompass six time zones from the East Coast to Hawaii); an increase in Service component commands' talent pool (RC members with high technology skills can be reassigned or recruited to perform inactive duty training near home); development of a skilled pool to man the Service component commands during annual training periods of the virtual Joint Web Risk Assessment Cell (JWRAC) for Reservists and Guardsmen; and an increase in Service component commands' mobilization base. Using the RC in these ways would require little or no addition of on-site staff or facilities. Issues that must be addressed include how to identify Reservists with the right skills; the management challenge of virtual drilling; and possible Service reluctance to depend on the RC for fulltime support.

Increased RC Support to the Service component commands would leverage the expertise of skilled Reservists with civilian acquired skills, capable of conducting virtual operations in support of Service missions. The virtual augmentation could objectively perform portions of the Service missions that are not completed due to real-world mission pressure or could augment staff during weekends and during summer months.

In addition to the Reserve Component Study, there were recommendations made in the Defense Science Board Task Force on Human Resources Strategy published in February of 2000.23 The task force identified a number of priority areas for shaping both the civilian and military workforce, including the Reserve Component. Its recommendations included the

---

[21] DepSecDef memo subj: ***Department of Defense Chief Information Officer Guidance and Policy Memorandum No 6-8510, "Department of Defense Global Information Grid Information Assurance,"*** 16 June 2000.

[22] ASD(RA) Study, ***Reserve Component Information Assurance Study***, February 2000

[23] DSB Task Force on Human Resources Strategy, February 2000

following: 1) moving to a seamless integration of active and reserve components with a single, integrated personnel and logistics system, and 2) constituting a task force to study and develop a plan that will merge, over time, the Army and Air Force reserve units with their respective National Guards.

The DIO task force notes that on December 6, 2000, the Deputy Secretary of Defense announced a plan to establish five joint reserve virtual information operations (JRVIO) and information assurance organizations. These JRVIOs will directly support DoD's five key information operations agencies and joint commands. The task force sees the establishment of these bodies as an important first step to more effectively use reserve components in this key national security area.

Know Your Insiders

The insider threat has long been recognized as one with the potential to cause a great deal of damage – both inside the government and in the private sector. An insider is identified as anyone who "is or has been authorized access to a DoD information system, whether a military member, a DoD civilian employee, or employee of another Federal agency or the private sector."[24] An insider has the capability to disrupt interconnected DoD information systems, to deny the use of information systems and data to other insiders, and to remove, alter or destroy information. Recognition of this problem exists in many DoD documents that discuss the issue and make recommendations on how to mitigate the risk of the insider. The most comprehensive of these is a recently released report listing the recommendations of the Insider Threat Integrated Process Team, chartered by ASD(C3I).[25] This report identifies the basic sources of insider security problems as (1) maliciousness, (2) disdain of security practices, (3) carelessness, and (4) ignorance of security policy, security practices and proper information system use. The key elements of a strategy to minimize the impact of the insider threat are to:

- Establish system criticality
- Establish trustworthiness of personnel
- Strengthen personnel security and management practices
- Protect information assets
- Detect problems
- React/respond

The report makes a total of 59 recommendations in 7 areas that, if adopted, will significantly improve the ability of DoD to mitigate the insider threat risk. A separate report addressing training and certification issues for personnel performing for critical IA functions also makes recommendations to mitigate the insider threat.[26] This report specifies that personnel performing critical IA functions – defined as those that require the individual to have privileged access to networks and operating systems – require special attention to ensure that they can be trusted. These critical IA personnel include systems administrators who have the most ability and access to both protect and damage DoD networks. A third report, issued by the National Security

---

[24] OASD(C3I) Insider Threat Integrated Process Team, ***"DoD Insider Threat Mitigation,"*** Department of Defense

[25] ***DoD Insider Threat Mitigation: Final Report of the Insider Threat Integrated Process Team***

[26] ***Information Assurance and Information Technology: Training, Certification, and Personnel Management in the Department of Defense,*** Information Assurance and Information Technology Human Resources Integrated Process Team, 27 August 1999.

Telecommunications and Information Systems Security Committee (NSTISSC), also addresses the insider threat,[27] as does a DoD Inspector General report.

There are many ways to address the problem, but all require knowledge of who the critical personnel are, and what the critical processes and systems are. The Y2K effort provides a model of how to distinguish between critical and non-critical systems and processes. The results of this discrimination process can provide a mechanism to focus attention on constrained resources for systems and processes that are most critical to the Department. However, there is, as of yet, no mechanism to identify critical personnel, although the recommendations by the IT/IA Human Resources Management (HRM) IPT previously referenced, begin to accomplish that objective. These recommendations, recently approved by DepSecDef, will take several years just to identify all of the DoD's systems administrators.[28] This step is absolutely essential because systems administrators are the most critical of all those who perform IA functions. Systems administrators can be military personnel who are performing this function in a full-time or part-time capacity, DoD civilian personnel (full-time or part-time) or contractor personnel performing functions that have been outsourced. Regardless of their status, all individuals performing these functions must be held to a consistent – and high standard.

It is not enough, however, to screen those performing critical functions for trustworthiness, because the most rigorous screening may not identify a potential problem insider, or someone who may be susceptible to blackmail. Screening also does not prevent someone who had no intention of misusing the system initially from doing so at a later date. Therefore, monitoring of both personnel and systems must be done to detect those who are not using the system as intended. This surveillance requires establishment of a clear, legal and enforceable monitoring policy so that all personnel using the systems are aware that their activities can be monitored. This policy can also act as a deterrent to anyone who may contemplate unauthorized activity, as well as aid in holding those accountable who violate the policy. The Department has a monitoring policy, but it needs revision to accomplish the objectives stated. The technical means to monitor are available, but require proper configuration and deployment within the network architecture.

Access control processes and mechanisms are also required to prevent individuals from unauthorized access to information and processes. Passwords can provide some measure of control, but require a management process to ensure they are regularly changed. Additionally, the files need to be protected from disclosure, and users need to be aware of their responsibility in protecting passwords. Passwords also have flaws, and other access control mechanisms should be employed, such as Public Key Infrastructure (PKI) and biometrics. The DoD PKI program will address many access control issues and the DSB DIO task force acknowledges this effort.[29] However, insufficient funding and lack of follow-up in the enabling of applications for PKI could jeopardize the deployment program.[30] The biometrics program, with the Department of the Army as the executive agent,[31] also shows promise in issues of access, but inadequate funding could also jeopardize this program.

---

27 ***Ninth Assessment of the Status of National Security Telecommunications and Information Systems Security within the United States Government,*** National Security Telecommunications and Information Systems Security Committee, 21 June 2000 (draft).

28 DepSecDef Memo, Subj: ***Implementation of the Recommendations of the Information Assurance and Information Technology Integrated Process Team on Training, Certification and Personnel Management in the Department of Defense,*** 14 July 2000.

29 ASD(C3I) Memo, Subj: ***Department of Defense (DoD) Public Key Infrastructure (PKI),*** 12 August 2000.

30 OASD(C3I) DIAP Report, April 2000.

31 National Security Act, 1947.

The insider threat is, therefore, well documented, and numerous recommendations exist that, if implemented, would significantly reduce the impact of this threat. However, a number of the recommendations have yet to be implemented. The reasons for this situation vary, but lack of resources and difficulty in developing appropriate policy appear to be the primary factors. This DSB recognizes that the Department has acknowledged the problem, but the lack of policy and resources to address a very real and growing problem is of concern.

4.4 Resources

The last five years have seen three trends that, taken together, threaten DoD's information infrastructure. They are:

- An exploding military network dependence, increasingly vulnerable to denial, disruption or degradation.
- A concomitant spread of tools, technology and interests in exploiting or threatening DoD information systems by potential adversaries –specifically including persons operating in the United States.
- The adoption of Joint Vision 2010 and 2020 that predicate U.S. Military objectives, in part, on information superiority and decision superiority.

Funding throughout the DoD to provide information assurance has been and continues to be inadequate. Unfortunately, DoD must apply substantial additional funds if information assurance is to be achieved or sustained to support JV2020. It is noteworthy that:

- Exploding sensitive but unclassified (SBU) network infrastructures are at risk while pressure increases for more interconnectivity between various security domains and public domains
- Network interconnectivity in and of itself is causing DoD to invest in non-traditional security initiatives to provide information integrity, electronic identification and authentication, non-repudiation, and availability over and above traditionally funded legacy confidentiality (Communication Security [COMSEC]) programs.
- Insider threat is largely ignored, raising trust issues with classified networks as well
- Looming COMSEC Modernization bill to replace aging infrastructure will further strain commitment to SBU problem

The DSB in 1996 recommended funding levels to address deficiencies identified in the Department's DIO budget. Since that time, the funding levels for DIO have increased only slightly in relative dollars, but the requirements and the situation regarding DIO have changed significantly.[32] In 1996, the primary focus of funding was for classified systems. Subsequently, the Department has realized that its unclassified systems and networks that process sensitive and mission critical information require protection, but the requirements in this arena have far outstripped the funding available and allocated to address the problem. Although it may look to the uninformed observer as if funding has increased, slightly, the reality is that the problem has

[32] DIAP PDIT Brief of 14 July 2000

grown much more comprehensive in scope, and therefore, funding has failed to keep up with requirements. The results are "unfunded mandates" and robbing of critical long-term programs to pay for immediate short-term concerns.

Exacerbating the situation, the DoD has yet to articulate a clear strategy for funding and implementing DIO. Some documents describe some pieces of a strategy (CIO ITM Strategy[33] and the Global Information Grid), but they are incomplete or immature and insufficiently detailed to provide a clear picture are the DoD's priorities in this arena. The result of this lack of strategy has been an inconsistent DIO funding profile across the Department – with components making internal decisions about what they can afford regardless the impact on the overall needs of the DoD. In a shared risk environment, this inconsistent implementation of DIO requirements results in uneven levels of assurance, increasing the risk to all. The lack of an overall strategy, coupled with outdated, incomplete policy, also makes it difficult for the components, and therefore the DoD as an organization, to justify the increased funding levels that it needs to address the requirements.

4.5 Recommendations

1. Integration of DIO into mission planning and execution

DIO is not adequately integrated into mission planning and execution nor is there an adequate system for assessing DIO readiness across DoD. To facilitate the integration into all phases of operational exercises, testing and evaluation, and operational assessments, the task force recommends that the Secretary of Defense, and Chairman, Joint Chiefs of Staff should:

- *Issue guidance to make DIO a key element of all military planning and operations, to include promulgating Rules of Engagement (ROE), continuity of operations plans, and conducting unit training exercises,*
- *Promulgate guidance in the Joint Military Readiness Review (JMRR) and other appropriate Service readiness reporting systems,*
- *Measure and assess IA readiness, and specify policies to hold commanders accountable for aspects of DIO readiness within their control.*

Time:. Initial actions by October 2001, with completion no later than October 2002

Estimated cost of implementation: Approximately $500K for initial actions. Budget requirements for completion will need to be developed and submitted for the PPBS process.

2. Red Team Activities

The purpose of an Operational Readiness Assessment is to examine and test an information system or product to determine the adequacy of security measures, identifying security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation. However, due to a lack of clear policy and resources, aggressive, comprehensive, effective operational Red Team activities are lacking across DoD. To redress this, the task force recommends that the Secretary of Defense should:

[33] DoD DIO ITM Strategy, Oct 1999)

Formalize and empower DIO Red Teaming throughout the DoD by:

- *Developing a three level assessment capability:*
  - *Level I: Vulnerability Assessment*
  - *Level II: Vulnerability Evaluation*
  - *Level III: IO Red Team*
- *Establishing policy that defines authorities and responsibilities,*
- *Expanding the number, scope and frequency, and*
- *Providing adequate staffing and resources to accomplish expanded mission (technology, tools, manning).*

Time: Begin actions as detailed by October 2001

Estimated cost of implementation: $30M per year

3. Assessment of Civil Sector Dependencies

There is no formal program or priority for assessing critical civil sector dependencies. Yet the success of operational missions is now, more than ever, dependent on the assured and timely delivery of information from operational commanders to operating forces and reliance on the private sector infrastructure to do so. To redress this shortfall, the task force recommends that the Joint Project Office- Special Technology Countermeasures (JPO-STC in Dahlgren, VA) should be:

- *Chartered to assist local commanders in identifying and assessing key infrastructure dependencies and vulnerabilities of DoD Elements,*
- *Designated as a critical element in the DoD DIO readiness system,*
- *Subordinated to Joint Forces Command with a military O-6 in charge, and*
- *Manned, equipped and resourced to do the job.*

Time: Begin actions as detailed by October 2001

Estimated cost of implementation: $25M per year

4. CERT/CIRT Activities and Coordination

CERT/CIRTs provide initial indication of external attack against DoD network systems. Yet, DoD CERT/CIRT activities vary in their execution and are not inclusive of all DoD CINCs/Services/Agencies (C/S/A). In order to improve the DoD CERT Structure and Scope, the task force recommends the following actions:

The United States Space Command, supported by Office of the Secretary of Defense/Joint Chiefs of Staff Policy should:

- *Develop doctrine/TTPs (tactics, techniques and procedures) on emergency response, including deployment when necessary,*
- *Implement CERT clearinghouse capabilities,*

- *Provide access to standardized & advanced tools and methodologies,*
- *Establish common reporting formats and a shared common database,*
- *Develop a standardized alerting process, and*
- *Establish additional CERTs where needed at C/S/A.*

Time: To be implemented by October 2001

Estimated cost of implementation: $50-70M over the FYDP

5. Roles, Missions and Responsibilities

To ensure that roles, missions and responsibilities of organizations tasked with DIO functions are clearly understood and executed appropriately, the task force recommends the following action be taken by the Department:

- *SECDEF and CJCS should clearly define roles, missions and responsibilities of organizations tasked with DIO functions, including clarifying chains of command and relationships with other organizations.*
- *When tasking organizations to perform these additional functions, resources should be provided, along with priorities of execution of missions.*

Time: To be implemented by October 2001

Estimated cost of implementation: Minimal for definitions. Resources for tasking addressed in separate recommendation.

6. The IT Workforce

To find and keep the IT talent necessary for successful implementation and execution of the GIG, the task force recommends the following actions be taken by the Department:

- *The Secretary of Defense should direct more aggressive recruitment and retention efforts. The SecDef should also direct a proficiency pay for critical DIO skills. The authorities to accomplish this already exist.*
- *ASD/C3I in coordination with USD/P&R, should develop formal career paths for DIO officer, enlisted, civilian personnel.*
- *DoD needs to develop an outsource strategy to complement DoD key DIO resource needs and develop an "Education and Training for Service" program, for example, of 5 years tenure.*

Time: To be implemented by October 2001

Estimated cost of implementation: $25M per year

7. DIO Training and Awareness

DoD workforce at all levels is ill prepared to execute the DIO mission because current training efforts are fragmented, inadequately scoped, and poorly documented. Awareness to the full dimension of cyber risk is very limited. Therefore, the task force makes the following recommendations:

- *SecDef, ASD(C3I), USD(P&R), USD(AT&L) and Military Departments should establish policy to develop and implement formal Education, Training, and Awareness (ETA) programs for DIO throughout DoD. These programs should:*
  - Codify the DIO training program within the formal DoD Joint Training System (JTS)
  - Ensure DIO programs are consistent with commercial and DoD certification standards
  - Require contractor personnel performing outsourced DIO functions to meet ETA criteria required for government employees.

Time: Establish the recommended program by 1 October 2001

Estimated cost of implementation: $150M over the FYDP

8. Personnel Shortfalls and Reserve Component Configurations

Significant personnel shortfalls will impact the execution of the DIO mission at all levels in DoD. The DoD increasingly relies on its Reserve component to fulfill its mission both from a resource and a skills available standpoint. However, because the two systems are separate, DoD must relearn how to manage the joint configuration each time the reserve component deploys. To facilitate a more seamless integration, the task force recommends the following:

- *The Deputy Secretary of Defense should direct USD(P&R) and ASD(C3I) to implement the recommendations from both the Reserve Component Study and the Defense Science Board task force on Human Resources Strategy.*

Time: To be implemented by October 2001

Estimated cost of implementation:

- *For Human Resource Management DSB: as determined by the study, applicable to IT workforce*
- *For Reserve Component Study: $10.5M over the FYDP*

9. IT Personnel Security

Insiders are both DoD's first line of defense and the most dangerous cyber threat. Systems Administrators have the "Keys to the Kingdom" yet often require no special "reliability" investigations, such as those in the Personnel Reliability Program. To redress this crucial inadequacy, the task force recommends the following actions be taken by the Deputy Secretary of Defense:

- *Mandate an innovative and effective security program for critical IT professionals, which might include:*
  - *System Administrator auditing software,*
  - *Open source commercial style background investigations,*
  - *Peer accountability,*
  - *Pre-employment agreements,*
  - *Credit Checks, and*
  - *Two-person integrity for certain functions.*

Time: To be implemented immediately

Estimated cost of implementation: $5M per year

11. DIO Funding Strategy

Adequate resourcing and a clear strategy for DIO throughout the Department are critical to ensuring a consistent implementation of DIO requirements. To ensure adequate funding of the DoD DIO requirements, the task force recommends the Secretary of Defense should:

- *Develop a DIO funding strategy and profile, establishing priorities where sufficient funding does not exist and provide implementation guidance on this strategy to DoD components.*
- *Where funding is insufficient to meet requirements, reallocate, and reprioritize existing programs and support justification in the budget process for necessary across- the- board increases in budget allocations.*

Time: To be implemented by October 2001

Estimated cost of implementation: Total IA Budget for DoD should be around $3B/year, an increase of about $1.4B over current documented funding.

CHAPTER 5. POLICY AND LEGAL

"In times of change, learners shall inherit the earth, while the learned are beautifully equipped for a world that no longer exists." James Thurbur

5.1 Introduction

What country, suffering under U.S. imposed sanctions and a hail of cruise missiles, has not dreamed of bringing that same disruption and fear to Cleveland or Omaha? That dream is the reason that Information Operations is an almost inevitable part of the American future. State-sponsored attacks on our computer networks are much safer than other ways of going to war against this country. Network attacks can be anonymous – or at least deniable. And they are asymmetric. They will allow hostile nations to attack on a battlefield that avoids American strengths, such as conventional and nuclear forces. Indeed, it allows them to turn our strength into weakness by exploiting our unique dependence on computer networks for more and more of the necessities of life.

The next Saddam Hussein, or the current one, for that matter, could win a symbolic victory just by tying up Manhattan's traffic control network for a day. But information warriors aspire to much more. Some believe network attacks will soon be able to cause death and chaos across the country, especially if offensive capabilities continue to outpace the defenses we are erecting, or thinking about erecting. By and large, thinking about erecting defenses is all that the United States is doing. The Defense Department is spending money on computer network defenses, as are a handful of other agencies. But many of the high level targets are not in the government's hands. And for most in the private sector, computer defense means little more than updating virus software and changing passwords frequently.

The vast expanse of networks that run our lives and have propelled our economy to new heights lie exposed to devastating and imaginative attacks. In practice, information operations is nowhere to be seen. Information vandalism is around; hacking and virus writing have become annoyances, but until the "ILOVEYOU" virus, even highly wired civilians were far more likely to encounter such problems in the news media than in real life. We will only get truly serious about information operations when we experience it.

However, the United States can do more to harden networks in the government's hands, especially those on which the armed forces rely. And it can offer incentives to the private sector to beef up their security. It can tinker with policies and laws as new computer crimes emerge. But more serious changes will have to wait until the threat is more obvious. Which suggests one more thing that the United States should do – immediately. It should gather as much information as possible about network intrusions and security breaches that are occurring right now. Information operations cannot be launched from the blue. Like any weapon, it must be tested. Indeed, to be truly effective, information operations should be planned, and preliminary intrusions should be launched years before an overt and coordinated attack.

How will the United States defend itself against such sophisticated attacks? Very likely, it will reproduce in cyberspace all of the defensive techniques of war – intelligence-gathering, defensive perimeters, counterattacks, and the like. Because the targets of information operations

will be civilian as well as military, defending against such attacks will require close cooperation between the public and private sectors. Such cooperation is mildly controversial today, but a sophisticated attack on public and private networks will likely make cooperation not just politically acceptable but politically necessary. When that happens, the legal regime needed to respond to the attack will likely be put in place quickly by politicians anxious to be seen as part of the solution.

Today, however, there is no consensus among Americans that strenuous efforts are necessary to prepare for or defend against information attacks. A healthy skepticism exists toward government alarms, particularly when the government's solution is to grant itself more power. In this climate, private industry and government bodies alike are reluctant to change their behavior in fundamental ways. In particular, there is little appetite for large expenditures on network security and little enthusiasm for significant changes in the law.

This task force's recommendations for policy and legal reforms are made in that context. The task force did not recommend a sweeping change in existing legal structures. Instead, a somewhat less ambitious goal has been set: to examine the policy and legal concerns that currently prevent the government from adopting otherwise sensible defensive policies, and where those policy and legal concerns are not fully justified, to recommend reforms. While the task force has not tried to fully imagine or recommend the national security, policy and legal structure that will be needed to respond to the information operations techniques the country will face in 2020, it believes that its recommendations take several steps toward a structure that will still be workable 10-20 years from now. The recommendations take the form of four sets of issues: Common DIO Terminology, Government-Wide Coordination, Law Enforcement Information-Sharing Roadblocks, and Critical Infrastructure Protection. Actions taken in the near-term to implement these recommendations would materially benefit the effective execution of DIO within the Department.

5.2 Toward a Common Terminology

New technologies and new concepts inevitably require new terminology. Unfortunately, terminology and definitions related to DIO vary widely throughout government and the private sector. DoD has expended considerable effort to standardize Information Operations (IO)-related definitions, but differences and controversy remain. The Intelligence Community (IC) and DoD, in spite of a great incentive to share definitions, have managed to formally agree on only about a dozen. Industry and the private sector use a wide variety of definitions depending on convenience and circumstance.

How one defines a concept or an action has a direct bearing on which laws may be applicable to a situation and which authorities may hold sway. It may also affect how actions are funded. Consequently, definitional issues often masquerade as surrogates for deeper struggles over turf and resources.

The situation is made more complicated by the fact that some terms arrive on the scene laden with semiotic baggage. For example, "monitoring," means one thing to the National Security Agency (NSA) in a foreign intelligence context, another to the FBI in its law enforcement role, and something quite different to the American Civil Liberties Union (ACLU) when discussing the Fourth Amendment. Likewise, the term "attack" may mean to destroy, to penetrate for

purposes of monitoring, to trace back for purposes of defense, or to temporarily disable, depending on who is conducting the "attack" and the intent of those actions.

Fortunately, the law does not need to be changed to create a common lexicon and direct its use throughout government. Most, if not all, of the problems associated with definitions can be solved using existing processes and organizations. However, a necessary precondition of such a lexicon would be an improved consensus on authorities, roles, and responsibilities to perform DIO. The process of building a common lexicon would force many issues into the open for discussion and resolution. Finally, if such a lexicon were developed with utility to the civil sector in mind, it might have the added benefit of helping industry consolidate its efforts to defend critical infrastructures.

A Presidential Review Directive (PRD) has recently been signed, which calls for an Interagency Working Group (IWG) to reach consensus on several matters important to IO in general and DIO in particular. Doing so will do much to clarify roles and responsibilities. The subject of definitions is among the matters to be discussed, but the PRD stops short of calling for a comprehensive common lexicon to be used throughout government.

5.3 Requirement for Government-Wide Coordination

Prior to the Information Age, protecting the nation from external attack was clearly the province of the DoD, supported by the IC. Law enforcement agencies assisted with counter-intelligence efforts and other domestic responsibilities. The situation is more complex today. An attacker in cyberspace may do harm to our critical infrastructures without our knowing his identity or location. The infrastructures he is attacking may be private property and not clearly under the purview of the national security apparatus. Similarly, uncertainty about the origin, severity, and target of an attack may lead to confusion over whose authorities are preeminent in responding to it. Obviously, coordination becomes critical in such circumstances.

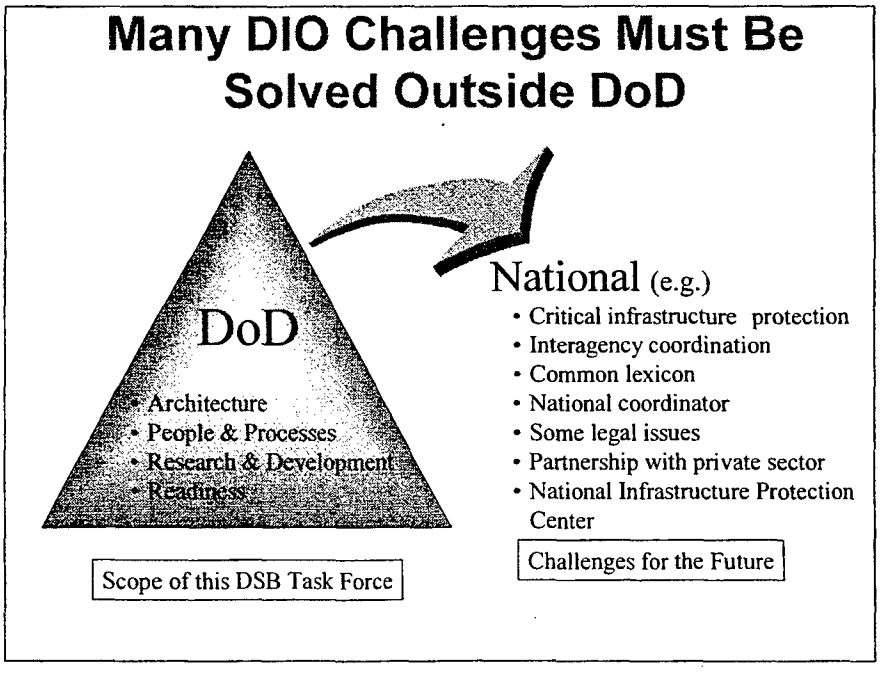


Figure 38. Solving DIO Challenges

Warning is another issue that will be seen through different lenses in the Information Age. Traditional intelligence collection and analysis methods might provide some measure of *strategic* warning of an IO attack, but the nation currently has no means of providing *tactical* Indications and Warning (I&W) in cyberspace. In fact, there is no reliable means to even detect a widespread, subtle, "slow and low" attack, let alone to warn of it. Some would argue that such an attack is already ongoing. Even if an attack were detected, there is no consistent, widely understood process for reacting to it or recovering from its effects. Furthermore, there are no formal mechanisms for balancing equities between law enforcement and national security when reacting to it.

Any cyber I&W effort will require visibility into a large number of domestic networks, if not for content, at least to characterize the health of their operations. Obviously, the IC is limited in its ability to perform such a function. Likewise, law enforcement is proscribed from monitoring actions in the absence of compelling legal grounds. Nevertheless, there is much that can be done within existing law, policy, and regulation. (For a more complete discussion of this subject, see the legal section in Volume II of the report.)

A few systems in government and industry (e.g., monitored command networks and Telecommunications Service Providers) have limited capabilities to detect an attack within their own "stovepipes," but reaction options are limited and local. Coordination and "spreading the word" generally falls to Computer Emergency Response Teams (CERTs) and individual initiative. In no case is there a robust means of characterizing diverse attacks occurring in separate segments of government and industry or of rationalizing large-scale reaction and recovery. The National Infrastructure Protection Center (NIPC) was originally created to help coordinate information on such attacks, but has devolved primarily into a cyber-crime investigation body. In fact, the predominant FBI (law enforcement) culture of the NIPC has made information sharing difficult in a practical sense, within government or with industry. As always, well-meaning individuals with initiative have built informal coordination mechanisms, but these are personality dependent.

Since the NIPC, by default, considers a cyber intrusion to be a crime, rules of evidence and strict investigative procedures are applied and information sharing is restricted. This practice, which appears to have little justification in law, biases reactions in favor of law enforcement and stands in the way of really effective information sharing and the coordination that would be necessary to mount an effective national defense. Finally, no one is assigned the responsibility or the authority (other than through Cabinet level cooperation) to make the decision that an ongoing attack has progressed from a law enforcement case to a national security matter.

A similar vacuum is seen when one looks for someone in authority to coordinate a recovery from a nationwide or large-scale cyber attack. Obviously, some activities would be covered under standing contingency plans for disaster recovery or continuity of government. Likewise, many segments of industry, (e.g., banking and the stock markets) have elaborate backup and recovery plans. On the other hand, if an attacker were to mount a carefully coordinated assault on several segments of our infrastructure simultaneously, it would be difficult to recover without massive dislocation. For example, if phone service and the power grid were lost at the same time that gas lines were disrupted during winter, the combined effect could be very severe. Even worse would be a scenario combining such cyber attacks with traditional bomb blasts or the

release of a biological agent. It does not take much imagination to see that coordinating a recovery would require difficult decisions about whose infrastructure should be recovered first. Questions of liability aside, these hard choices must be made by someone with visibility across infrastructure stovepipes and the authority to compel actions that will affect lives and finances.

As matters stand today, a declaration of martial law or use of the National Guard might be required to answer the demands of the wide-spread situation described above. However, a more palatable, more effective, and less costly recovery could be made using the offices of a standing official charged with the responsibility for national critical infrastructure protection. It is true that there is a coordinator for counterterrorism, security, and critical infrastructure protection, but realistically his authorities are constrained to his powers of persuasion. Likewise, CINC, Joint Forces Command is charged with homeland national defense, but confusion may arise from the fact that CINCSPACE is responsible for Computer Network Defense. Realistically, neither CINC can do much to prepare for homeland cyber defense without asking hard questions about *posse commitatus*, the legal aspects of dealing with private industry, and public perceptions of the military taking on such a role in peacetime.

Finally, there is the question of international allies and corporations with close ties to U.S. firms. Geographic boundaries mean little in cyberspace. Effective reaction to and recovery from a serious cyber attack almost certainly will require coordination with allies and foreign partners. Consequently, the State Department (DOS) must engage on these issues in the immediate future. In fact, the State Department is already involved in several DIO-related matters, such as a Russian proposal to limit national programs on Information operations. As matters progress, DOS will have to join more fully with the DoD, the IC, and Law Enforcement communities in coordinating responses to cyber issues.

In sum, the nation needs a well-staffed, designated official with direct access to the principals of the National Security Council (NSC) who is charged to plan for and respond to the type of crisis described above. Perhaps the growing discussion about creating a Federal Chief Information Officer (CIO) within the Executive Office of the President will answer these concerns, provided that the position is given the required authorities and that national security matters are coordinated through the NSC. Such an official will require explicit authorities that can only be granted in law by Congress. Consequently, anyone appointed to fulfill these duties will require Congressional confirmation.

5.4 Resolve Law Enforcement Information Sharing Roadblocks

The task force examined in detail how the United States government currently gathers information about network attacks, and how well it shares that information among the agencies that need to analyze it. This examination raised a number of pertinent issues and several problems for which there are no easy answers. The task force, however, does make some important recommendations that will accelerate the pace of information exchange. There are three important points on which these recommendations are based:

National Security and Law Enforcement Missions Overlap

Why have Justice Department entities like the FBI assumed such a large role in defending against network attacks? In a word, because attacks on American networks have traditionally been the work of hackers, not foreign states. They are crimes, nothing more.

That may change quickly however, as hacker tools become weapons in the hands of hostile nations, because our information systems are a tempting target, especially for countries that cannot confront our armed forces directly. Network attacks are anonymous – or at least deniable. Furthermore, some knowledgeable people believe network attacks will soon be able to cause deaths and chaos across the country – especially if offensive capabilities continue to outpace our defenses.

In short, network attacks have a national security as well as a law enforcement dimension. DoD must be involved, both because it has a responsibility to defend the country and because it depends so heavily on a civilian infrastructure that is particularly vulnerable to network attacks. But DoD cannot act alone; it may not be possible to tell at the start of an attack whether the matter can be treated as a crime or an act of war or something in between. This means that the defense, intelligence, and law enforcement communities must be prepared to work together in a smooth and coordinated way.

Based on what we have seen, that day is a long way off. While they have been quick to take the lead in protecting information networks, the Justice Department and the FBI have been slower to recognize the need for cooperation with the Defense Department and other national security agencies.

Information-Sharing Is Critically Important

This tendency toward limited information sharing has harmed the country's preparations for attacks on our critical information infrastructure. The first order of business in preparing for network attacks is to gather information about the attacks now being mounted against U.S. information systems. The more we know about today's attacks, the better prepared we will be to deal with tomorrow's. Information operations cannot be launched blindly. Like any weapon, it must be tested. Indeed, to be most effective, Information operations should be planned, and preliminary intrusions should be launched years before an overt attack – defenses must be probed, vulnerable systems reconnoitered, logic bombs planted. To judge the extent of our danger, we should be watching intently for just such activities – sifting those patterns from the noise of "script kiddy" hackers. We should be alert for the subtle signals that governments and terrorists are in fact beginning to turn the theory of Information operations into practice.

Thus, gathering information about the kinds of attacks now being launched is the crucial first step of any defensive effort. But the effort to begin this task has become the subject not of effective initiative, but of continuing political and bureaucratic conflict. Although it has responsibility for national defense, the Defense Department must rely on law enforcement agencies such as the FBI and the Justice Department to gather information about attacks and then decide what DoD needs to know.

Information-Sharing Is So Hard

The FBI is the principal "intake point" for information about network attacks, in large part because it is easy to use the tools of criminal investigation to gather information about an attack, especially in its early stages. That is why the National Infrastructure Protection Center (NIPC) was housed within the FBI. Although staffed by defense and intelligence personnel as well as FBI agents, it relies heavily on criminal investigative tools that could not easily be deployed by other agencies.

But the effectiveness of the NIPC in protecting national security depends on sharing information about attacks, and the FBI does not have a strong reputation on that score. A wide range of different communities – local police, intelligence analysts, civilian agencies and business executives – all complain with regularity that however much information they share with the Bureau, the Bureau does not reciprocate effectively.

The NIPC has struggled to avoid the same reputation, but the culture of reticence cannot be turned on and off, particularly when the Justice Department, for its own reasons, has raised additional barriers to information sharing with defense and intelligence agencies.

As things now stand, DoD cannot count on NIPC, Justice, or the FBI for a free flow of information about network attacks. On the contrary, the task force identified policies and legal interpretations at NIPC, the FBI, and the Justice Department that have prevented effective information sharing about potential national security risks. The task force concludes that these barriers should be removed, and soon, if DoD is to continue to support and rely upon NIPC. Unless NIPC, FBI, and Justice overcome their narrow crime fighting perspectives – in a formal high-level agreement with the Defense Department – then DoD and the intelligence community should consider pulling out of NIPC to create an independent center for gathering and sharing information about the most serious network attacks. But this should only be a measure of last resort. Rather than splinter the government's limited resources further, we make several specific recommendations in paragraph 5.6 for changes in policies and legal interpretations that have prevented the NIPC from achieving its full potential as an information sharing center. It is the view of this task force, however, that these changes will not happen without leadership from the very top of both departments and the issues raised in paragraph 5.6 should form the agenda for a series of discussions that will culminate in a new agreement over information sharing between the law enforcement and national security communities.

5.5 Critical Infrastructure Protection

The Defense Department is increasingly reliant on a broad range of vital infrastructure services provided by the private sector, municipal utilities, and other non-DoD sources. Over recent decades, DoD's communications, energy, transportation, logistics and supporting requirements grew significantly, making the DoD far more dependent on non-DoD owned and operated systems and networks. The underlying private sector infrastructures have undergone an explosion in technical capability, complexity, and integration, adopting new technologies and processes, particularly evident in communications and energy infrastructures. This revolution in technology and system interoperability has empowered infrastructure owners and operators to better serve their customers while expanding capabilities and building corporate strength. Technological interoperability, a feature inherent in these infrastructures, was market-economy-driven and thus the infrastructures are exceedingly interdependent. As the infrastructures advanced in capability, capacity, and complexity, DoD took advantage of their availability.

Private sector dependencies have direct implications on the availability and reliability of DoD's Global Information Grid (GIG); leased private sector systems incorporating our nation's fiber optic network, twisted wire, and wireless systems provide the GIG's backbone outside DoD's information infrastructure gateways. The dependencies go much further than this vital information backbone; the breadth of defense operations requires much more energy, logistics, and other vital services than ever before. For DoD to fully understand its private sector

dependencies, it must analyze and assess those dependencies, a process that cannot be undertaken without dialogue and partnering with the private sector or municipal owners and operators of those infrastructures.

DoD's expanded use of private sector infrastructures should logically require a more detailed assessment of potential risks inherent in the interdependent, underlying infrastructure. The private sector built and operated these infrastructures while using a very different risk model than those used within DoD. Private sector risk analyses are based on economically driven models, focusing on profitability and customer service, with modernization reliant on anticipated returns on investment. Threats and risks are plausible in peacetime scenarios, where threats may be seen as backhoes and risks are seen as natural disasters or competitive business practices. DoD risk models focus on more sinister threats – where a bad actor or nation state could purposefully deny infrastructure to degrade our global projection of force or otherwise undermine the national security of the United States.

The Presidential Decision Directive on Critical Infrastructure Protection (PDD-63, 1998) focused national efforts to implement critical infrastructure solutions, including expanded partnership between government and the private sector. Many national initiatives began, including establishment of the National Infrastructure Protection Center at the FBI and the initiation of Information Sharing and Analysis Center (ISACs), attempting to expand partnership between government and the private sector within individual infrastructure sectors. Arguably, though much has been done to advance national CIP efforts, the broad ranging initiatives have not seemed to gel into the desired partnerships, including interagency coordination and partnerships between government and the private sector. Similarly, many agencies and departments have not funded CIP efforts consistently across government. DoD began recognizing its need to consider critical infrastructure issues and proceeded somewhat independently and separately from other government agencies to focus on vital aspects central to DoD.

In 1997, DoD accelerated its exploration of dependencies on non-DoD infrastructures, standing up individual infrastructure sector teams and coordinating them through organizational processes such as the Critical Infrastructure Protection Integration Staff (CIPIS). Administrative and organizational efforts within the Office of the Secretary of Defense (OSD) and the services were supplemented by operational initiatives, such as Joint Service Integrated Vulnerability Assessment (JSIVA) efforts, accelerated Red Teaming, DoD readiness exercises such as Eligible Receiver, and expanded infrastructure initiatives at the Joint Program Office for Special Technology Countermeasures (JPO-STC) and the Defense Threat Reduction Agency. Most infrastructure vulnerability assessments focused on our key defense sites and facilities.

The risk environment, especially as it pertains to the critical infrastructures on which DoD relies, has changed. Threats to the U.S. homeland are becoming far more real, leading to important explorations of new risks: information operations, biological and chemical warfare, and unconventional nuclear risks. While the risk environment has evolved, the infrastructures on which the United States relies, both domestically and in forward-deployed areas, have become more technologically advanced, concentrated in increasingly critical nodes, with complex distribution that DoD may not fully understand. Further, these infrastructures are less within the government's and DoD's control. Market pressures drive technological advancement within these networks, with fiscal realities no longer shaped by government needs.

The potential for a smart adversary to undermine the reliability or availability of our critical infrastructures is increasingly real. In the context of DoD's evolving GIG backbone, protecting information architectures and their content does not necessarily protect the underlying cyber and physical infrastructures. Similarly, protecting DoD's GIG within the gateways that connect it to private sector-owned and -operated information infrastructures does not guarantee GIG availability should the leased connectivity outside those gateways be denied.

DoD should accelerate its efforts to identify its private sector dependencies and vulnerabilities, for DoD's information backbone as well as for other infrastructure dependencies that support energy requirements, logistics and transportation, water, and other critical infrastructure reliance. Without broad-based consideration of the full scope of critical infrastructure dependencies, mission constraints are unknown, but potentially significant.

Relationship building and the resultant trust takes time. It is likely that both the government and private sector leaders at a localized level have multiple overlapping requirements and interests that contribute to both national security and the corporate prosperity of the infrastructure provider. For the purposes of critical infrastructure protection, it is important that these relationships advance toward the mutual benefits of government interests, including those of national security, and those of the critical infrastructure providers. As such, it is important that efforts taking place at the local DoD installation level to define local dependencies on private infrastructures be explored and assessed in depth. More work needs to be done to identify vulnerabilities outside the lifelines of DoD, yet within the infrastructures on which DoD is very reliant.

One important area for DoD to explore is the pursuit of local contracts between the base or installation level commander and their key private sector infrastructure providers to attain contractual agreement on expectations and requirements for continuity of services, including redundancy options for vital functions. Resultant guarantees in service availability and reliability would likely require some reimbursement to the infrastructure provider for such guarantees. They could also include provisions for proprietarily protected, mutual explorations of infrastructure service reliability, allowing a partnered analysis to identify and mitigate potential single point failures outside DoD gateways. Such an initiative across DoD facilities would go a long way toward expanding infrastructure partnerships with the private sector. Further, critical infrastructure protection assessments would help build a common understanding of vital national security needs for the government customer. It would clarify the differences in risk analysis approaches, and the needs both, the private sector infrastructure provider and the national security focused customer.

Partnership between government and the private sector remains a vitally important yet elusive goal. Efforts to expand partnership with the private sector are hampered in many ways. The private sector sees a lot of the government wrangling and interagency squabbles (some of these indicate the shortfalls in PDD-63 implementation), confusing the infrastructure owners and operators and making it easier to question the government's seriousness in partnering. Further, especially in the context of information sharing between government and the private sector, the owners and operators need relief from the Freedom of Information Act (FOIA) to protect their proprietary data and interests and their competitive position.

Industry has indicated a willingness to help, but will not necessarily be motivated by the same things that motivate government. Industry fears regulation and unfunded mandates and will

not go beyond what makes financial sense in the market economy. The private sector level of trust in government is low. In particular, the public is least trusting of three specific government sectors. They are law enforcement in particular, and to a lesser degree, the intelligence community and DoD. Government must be willing to openly respond to industry concerns if it hopes to overcome the hurdles in achieving partnership. While the government and the public perceive that industry has the answers, true partnering with industry remains the prime challenge. Best practices within the private sector and within government should be shared, not only as an element of trust and partnering, but to enhance the security and economic implications of infrastructure operability and assurance issues. Partnership challenges will become even more constrained in the future, as companies became even more global.

5.6 Recommendations

1. Terminology and Definitions

The terminology and definitions related to DIO vary widely throughout government and the private sector, leading to numerous difficulties and controversy. To facilitate the standardization of DIO-related definitions, the task force recommends the following actions:

- *The Secretary of Defense and the Director of the CIAO should jointly sponsor an effort to produce an authoritative document (perhaps an Executive Order) containing DIO-related terms which would be useful in both the national security and civil sectors of government. This effort should draw upon the work of the IWG established by the PRD on IO.*

To assist this effort, the following Office of the Secretary of Defense (OSD) actions should be undertaken:

- *DoD & IC General Counsels (GCs) should work with the DOJ to develop a common concept for and set of terms to be used when conducting "investigations" in cyberspace.*
- *The Bilateral IO Steering Group (BIOSG) should create a joint DoD/IC working group to produce the largest possible set of common IO-related definitions. The term DIO should be included.*
- *USD(P) should initiate a dialogue with the State Department regarding common DIO definitions. The goal of these talks would be to encourage the use of common DIO-related terms throughout State and the DoD.*

The challenge will be to reach out beyond DoD and the IC to include the private sector, the law enforcement community, and the rest of government in the process. For this reason, the effort requires sponsorship at the National Security Council (NSC) or Executive Office of the President (EOP) level.

2. DIO Responsibilities and Coordination

Due to the complexities associated with a cyber attack, it is not clear whether it is the DoD's purview to respond or that of law enforcement agencies. Coordination becomes critical in such circumstances. To foster an environment where effective and timely decision-making can occur, the task force makes the following recommendations:

- *The Secretary of Defense should propose the creation of a national DIO coordinator. Prior to congressional action, the Coordinator's authorities will be limited. In the interim, he could serve as the focal point for of DIO policy development. Eventually, this individual should sponsor the development of national-level, coordinated DoD/IC/Law Enforcement mechanisms to provide I&W of a cyber-attack, respond to it, and recover from its effects.*

To support this effort the SecDef and DCI should:

- *Create a joint DoD/IC panel to work with the DOJ and NSC staffs to draft a DIO Executive Order (EO). The EO should clearly establish the preeminence of the national security response over the law enforcement response in cases having a national security impact.*
- *Create a panel to examine relevant law, policy, and regulations in light of emerging DIO realities (to include EO 12333.)*
- *Create a standing GC's working group to monitor legal precedents for decisions useful and inimical to DIO efforts and to explore the latitude available for DIO under existing law.*
- *Task the BIOSG to propose mechanisms for the military services and the IC to resolve conflicts relating to DIO (especially related to Computer Network Operations.)*
- *Declare the Information Operations threat a "Hard Intelligence Problem" and initiate the following steps:*
  - *The SecDef should request that the Director of Central Intelligence critically evaluate the Intelligence Community's ability to collect, analyze, and report intelligence that would allow more confident national estimates of the foreign IO threat.*
  - *The SecDef should establish a viable Research and Development program to develop new tactical- and operational-level ISR systems to provide warning of IO attacks to operational commanders.*

3. Information Sharing and the NIPC

The NIPC, which was created to foster coordination between the DoD and the FBI has not fulfilled its potential. As it currently stands, DoD cannot count on the NIPC for a free flow of information regarding network attacks. To encourage information sharing and cooperation in response to a cyber attack the task force makes the following recommendations:

- *First, all information available to NIPC should also be available to defense and intelligence analysts (who are already trusted with rather more sensitive information) unless there is an express legal bar on sharing or an interagency consensus that sharing the information is imprudent. The task force found that there may be*

misperceptions about the "law enforcement sensitive" label which is placed on much information flowing from the NIPC to the Department. The DOJ should clarify for recipients that the label is attached to alert its readers to the sensitive nature of the information rather than to prevent its flow to those requiring the information within DoD. Likewise, this task force also believes that DoD agencies (including the National Security Agency) should share all available information on events with the NIPC.

- *Second, the Justice Department has blocked NIPC from easy and natural communication with the National Security Council about infrastructure attacks, despite the NSC's central role in national security decision making generally and infrastructure protection in particular. Justice is plainly reluctant to share information about criminal investigations with White House personnel, but Justice's general policy should not be applied to information about network attacks.*

- *Third, DoD should have access to information about network attacks gathered under Title III (the wiretap statute). The Justice Department opinion refusing to provide this access shows little appreciation of the need for interagency cooperation on national security matters and should be reconsidered.*

- *Fourth, concerns about grand jury secrecy have made it difficult to know what material in the criminal investigative file may be shared with DoD and what may not. These concerns are mostly derived from very conservative readings of the rules on grand jury secrecy (readings adopted in part to serve the prosecutors' interest in avoiding public disclosures of their investigative priorities). They are also derived in part from the Justice Department's failure to train investigators of infrastructure attacks; these investigators could gather information without using grand jury subpoenas and thereby avoid later information sharing difficulties, but the FBI and Justice Department do not require their investigators to use these less problematic tools in the first instance. The rules on sharing grand jury information should be clarified to permit sharing for national security purposes; until this is accomplished, computer crime investigators working cases with national security implications should be prohibited from using grand jury subpoenas without interagency approval. Because of the atmospherics surrounding the relationship between the Department and the NIPC, there is a perception that there is a large quantity of Grand Jury information being held back from the Department. This is likely not the case, and what little there is, according to the NIPC, would contribute very insignificantly to the understanding of the events it relates to. Clarifying forthrightly what is real and what is not real would go a long way to creating a more positive set of atmospherics around information sharing in general.*

- *Fifth, NIPC is embedded so deep in the Justice and FBI bureaucracy, that it inhibits its interagency role because it cannot assure its counterparts in other agencies that decisions can be rapidly referred to high levels in the Bureau and the Justice Department. NIPC should report directly to the office of the Director of the FBI as well as the office of the Deputy Attorney General.*

- *Sixth, DoD has not taken all the steps necessary to ensure a large and strong contingent of DoD detailees at NIPC. Assuming a successful resolution of the issues*

raised in this report, DoD should upgrade its contribution to NIPC, both in numbers and in quality, and it should treat NIPC service as a "joint" appointment for purposes of military promotion.

- *Seventh, NIPC has much to offer DoD on questions such as when to block a particular hacker from further access and when to let the hacker continue in an effort to learn more about his techniques and purposes. DoD should agree on a role that clarifies NIPC's purely advisory position while guaranteeing that NIPC has a voice in such decisions. DoD should further clarify the commander's decision making authority in this area so that responsibility is unambiguous.*
- *Eighth, NIPC and the Justice Department's computer crime experts appear to have exceeded their jurisdiction in trying to limit what information intelligence agencies may receive; neither NIPC nor the Justice Department's Criminal Division should have a role in deciding whether and how DoD entities share information with NSA or other intelligence agencies.*
- *Finally, the task force notes that "red team" exercises, though vital, have been slowed in the past by multiple legal signoffs and supervision at DoD. This concern is diminishing as red teaming becomes more common, but it remains true that standardized and simple set of procedures should be adopted to allow unannounced "red team" attacks on all DoD networks without excessive high-level intervention by DoD officials.*

All of the recommendations above could be implemented without changing any statute. That is our recommended solution. Nonetheless, there are areas in which our laws have failed to anticipate the need for effective critical infrastructure protection. For that reason, we recommend that the Defense Department support a variety of relatively limited changes in existing law.

- *Most important, DoD should have its own civil authority to seek information about network attacks with national security implications. Under existing law, network service providers may give away information about hacking attacks to private citizens but they are legally prohibited from giving the information to a government agency unless the agency begins a criminal investigation. This is unfortunate for all. It forces hacker investigations into a criminal posture, which is likely to be bad for the hacker as well as for the opportunity to share information among agencies. The government should justify any request for information about its citizens, but it should not have to launch a criminal investigation before it can gather information needed to protect national security.*
- *Second, we encountered a disturbing gap in the ability of the government to maintain wiretap coverage of persons engaged in long-term hacking campaigns against government networks. Ironically, the more likely it is that the attackers are sponsored by foreign governments, the less likely it is that wiretap coverage will be maintained, because the likelihood of successful prosecution will decline over time. In the end, criminal wiretap authorities are inadequate for this problem, and a statutory solution should be sought that protects both national security and the civil liberties of*

Americans. One possibility is a provision denying network trespassers an expectation of privacy for their actions in attacking a victim's information system.

- *Third, current law concerning "trap and trace" orders often requires that law enforcement agencies seek multiple, sequential orders as they trace a single hacker from system to system. This provision should be modified to allow a single, nationwide order aimed at a single attacker who uses multiple computer systems. In addition, there is currently no statutory provision allowing the government to obtain certain types of information without the requisite order, in situations of extreme urgency. This is an oddity, since under the Electronic Communications Privacy Act, wiretaps may be initiated without a judicial order in an "emergency situation." In the interest of enabling law enforcement officials to obtain the crucial information they need for the prompt investigation of critical infrastructure attacks, the provision allowing emergency wiretaps should be extended to court orders and subpoenas as well.*
- *Fourth, if agreement cannot be reached with the Justice Department concerning the Title III and grand jury rules that currently restrict information sharing with DoD, Congress should clarify its intent that the confidentiality of criminal investigations not trump the national security interests of the United States.*
- *Finally, though the majority of the problems we outline focus on information-sharing deficiencies between and among government agencies, greater efforts could be made to encourage voluntary private-sector cooperation in hacking investigations. To this end, the use of nondisclosure agreements in gathering information on network attacks should be expanded, and narrowly-tailored legislation that would restrict the Freedom of Information Act disclosure of information shared pursuant to a hacking investigation should be considered.*

4. Infrastructure Dependencies

The Defense Department is increasingly reliant on a broad range of vital infrastructure services provided by the private sector, municipal facilities, and other non-DoD sources. These private sector dependencies have direct implications on the availability and reliability of DoD's Global Information Grid (GIG). Due to this expanded use, the task force recommends the Department take the following actions to ensure a detailed assessment of potential risks inherent in the interdependent, underlying infrastructures.

- *Accelerate actions to identify critical infrastructure dependencies on the private sector; the DoD effort to produce sector CIP plans is a step in the right direction, but we would note that this is not moving along very quickly, primarily due to lack of funding.*
- *Expand DoD's interactions with the private sector and municipal providers of critical infrastructure services. This is best achieved on a localized level, between base commanders (or other DoD leadership) and the infrastructure owners and operators. Direct DoD installation commanders (with support of JPO-STC) to identify critical infrastructure vulnerabilities, assess mission impact, and take corrective action with private sector service providers.*

- *Explore contractually based guarantees from the providers of critical infrastructure services that improve reliability and redundancy of vital services, while advancing private sector-government partnership through mutual risk-analysis of those services.*
- *Work with Sector Lead Agencies to ensure that DoD requirements are incorporated into the information-sharing processes with the owners and operators of critical infrastructure.*
- *Advocate FOIA and other related legal relief to remove impediments to private sector information sharing.*
- *Fund and resource JPO-STC appropriately to support critical infrastructure assessments. As a minimum starting point, increase funding for such focused efforts to at least $25M per year.*
- *DoD should modify or develop a process to assess the fiscal impact of infrastructure consequences to CIP events.*

5.7 Conclusions

Following the end of the Cold War, and the subsequent changes in the geopolitical climate, the United States now faces a different kind of threat. This threat is characterized by the ability of numerous potential adversaries to engage in an information attack upon the United States, enabled by the lower entry costs associated with such an attack. America's ability to attribute and respond is woefully inadequate to pose a significant deterrent to would be attackers. On the other end of the spectrum, early tactical indications and warning capabilities are virtually non-existent in cyberspace. These factors converge to create a newly and differently vulnerable U.S. homeland.

It is the contention of the task force that immediate actions can work to decrease the threat and potential damage to U.S. national security, including infrastructures, institutions and individuals. The United States national security apparatus must continue to evolve over time to deal with these emerging trans-national threats, including trans-boundary threats where the differences between law enforcement and national defense, between foreign and domestic, between national and transnational, and between government and civilian are increasingly irrelevant.

CHAPTER 6. SUMMARY FINDINGS AND RECOMMENDATIONS

"We must adjust to changing times and still hold to unchanging principles".
-Jimmy Carter

6.1 Findings

In summary, this task force of the Defense Science Board finds this nation in the midst of major global changes, and facing a new and uncertain threat to key information enablers of today's and tomorrow's military advantage. Although there is a perception that countering the information warfare threat is critical in the DoD, there is not an appreciation of the vulnerabilities of America's military to such threats.

JV2020 sets a high standard for achieving Information Superiority. Defensive Information Operations (DIO) are critical "go to war" capabilities and DoD must have confidence in our information and the technology that provides it. At present, DoD cannot measure and assess the readiness of our information infrastructure. This is exacerbated by the absence of a clear set of definitions, policies, procedures, standards, and management structures to implement DIO. Currently, there is not a viable way to exchange DIO information throughout the U.S. government, and the effect of this is magnified by DoD's lack of ability to restore integrity in its systems. Thus, this task force concludes that JV2020 is not achievable, unless DoD builds protection and interoperability into its combat information sphere. These recommendations are critical first steps towards those goals.

6.2 Summary of Recommendations

ARCHITECTURE RECOMMENDATIONS

Information Superiority Board

- *The Secretary of Defense should create the Information Superiority Board, with membership consisting of the Deputy Secretary of Defense (as Chair), the Undersecretary of Defense (Acquisition Technology and Logistics), the Vice-Chair of the Joint Chiefs of Staff (VCJCS), the Assistant Secretary of Defense (Command, Control, Communications, and Intelligence), and the Director of Central Intelligence.[34] A single member from each service may be important as well.*
- *It is further recommended that the Information Superiority Board create an Advisory Group under Federal Advisory Committee Act regulations (or as a permanent DSB panel) consisting of senior private sector IT leaders.*
  - *The Advisory Group's purpose is to provide the Board with up-to-date knowledge of current and emerging commercial information systems, services, and network*

[34] Reference: DSB Task Force on Tactical Battlefield Communications report

technology of potential use to the DoD in the realization of its Global Information Grid.

- *It is also expected to offer experience-based advice from industry as to the best technical and management methods for creating such an infrastructure.*
- *The Advisory Group should consist of recognized industry experts in inter-networking technologies, commercial information and network security technologies, emerging information transfer technologies and systems, and other commercial activities such as standards development, infrastructure development, and the like.*
- *The Advisory Group charter should also ensure that the group provides independent assessments and counsel to the Information Superiority Board concerning the achievement of the goals and objectives set forth in task force recommendations that follow.*

Executive Director and GIG Implementation Process[35]

- ***The Board of Directors for Information Superiority create, by 1 June 2001, an Executive Office responsible for leading the implementation of the DoD-wide common user internetwork on behalf of the board. The Executive Director should be responsible for programmatic oversight for all DoD C4ISR systems acquisitions (including those procured by the Services) and through this oversight ensure that all such systems are interoperable within and as part of the GIG. It would be the Executive Director's primary responsibility to deliver the GIG.***
  - *Implementing the GIG*
    - *The Board should establish an Executive Office responsible for leading and implementing the DoD-wide, common-user internetwork (transport component of GIG)*
  - *Executive Director should be a minimum five year appointment*
  - *The Board should provide system engineering resources to the Executive Office through a dedicated system engineering team comprising 20 to 30 outstanding network systems engineers drawn from throughout DoD.*

Time:

- *Office and Leadership Position Established by 1 June 2001*
- *Systems Engineering Office and Billets set up by 1 June 2001*

Cost: $10M per year

GIG Implementation Plan

- *The Executive Director should be tasked to develop a GIG implementation plan, to include technical milestones, measurable interim goals, and an estimate of the resources necessary to complete transition and realization of the GIG by 30 September 2003.*
  - *The Board of Directors should provide manpower billets for a system engineering team to support the Executive Director.*

---

[35] Reference DSB Task Force on Tactical Battlefield Communications

- *The Executive Director should immediately establish a process to transform DoD information infrastructure systems from their present stovepipe configurations into a global DoD-wide common-user virtual intranet, the GIG. This transformation must embody the current and evolving commercial IT standards, protocols, and technology, with the goal of reducing inefficiency in spectrum usage and the costs of information transport, storage, retrieval and management. Most important, this transition should enable new operational flexibility that can be leveraged by warfighters.*

GIG Policy and Guidance

- *The GIG Executive Director should immediately set policy and guidance for GIG IAA. Specifically, ambiguities regarding an IA reference model, system architecture and technical architecture (as noted in the body of the IAA report) should be clarified. The Executive Director should establish this unified strategy and framework by October 2001.*
  - *Executive director should establish a consistent IA strategy for all GIG networks*
    - *Select reference model*
    - *Define a single system architecture*
    - *Address tactical & strategic systems integration issues*
    - *Utilize Joint Technical Architecture (JTA) security chapter as single source IA standards*

Time: by 1 October 2001

Cost: already included in recommendation II

GIG System Architecture

- *Finally, the GIG Executive Director should work through the CIO Executive Panel and the MCEB to implement the GIG system architecture. Specific system architecture and implementation issues that need immediate attention include:*
  - *Continuing to aggressively deploy PKI, and addressing scalability issues*
  - *Aggressively pursuing NSA KMI initiative, addressing scalability issues*
  - *Deploying PKI-enabled subscriber security protocols: IPsec, SSL/TLS, S/MIME*
  - *Developing Type 1, high speed (multi-gigabit) IPsec devices*
  - *Constraining SIPRNET and JWICS network connectivity security policies*
  - *Deploying network infrastructure security technology: DNSSEC and Secure Boundary Gateway Protocol (S-BGP) (under development now)*
  - *Deploying diverse intrusion detection systems at WAN and enclave boundaries and in hosts*
  - *Moving all public DoD web sites of NIPRNET*
  - *Directing Defense Information Service Agency (DISA) to transition subscriber interfaces to IP (consistent with availability of suitable Type 1 crypto)*
  - *Employing spatial redundancy and design diversity for critical servers*

Budget to Support the GIG

- *To support GIG implementation and to accelerate the DoD PKI/PKE strategy, the Panel recommends an increase in budget of 50% over what is presently planned. This increase should not only accelerate the strategy, but also fund the development of Type 1 high-speed IPsec devices. This funding increase should be complemented and supported by the IA S&T investments discussed in Chapter Three.*

GIG IA Testbed

- *The task force recommends that the Executive Director's system engineering office establish a GIG IA research and development testbed. The testbed nodes should be located at ESC, CECOM, SPAWAR, AFRL, NSA, etc. The participants in the evaluation process will include research and development, evaluation and operational communities (services and agencies). The testbed will provide a means for measurement of system performance in the face of Red Team attacks on Blue Team scenarios and related information traffic. The testbed will also serve as a primary means for DARPA Information Assurance technology insertion and evaluation. The metrics and measurements will evolve as results are analyzed and lessons learned are derived from the data. Lessons learned will be fed back to red and blue teams to refine and update strategies and will be used by developers to improve system defenses. Lessons learned will also be made available to the GIG architects and system engineers to improve IA for the deployed system.*
- *The testbed should be used to engineer, evaluate and update defense-in-depth (DID) strategies and technologies. The testbed will provide the means to understand residual DiD (and GIG) vulnerabilities and thus facilitate cost/benefit analysis for GIG IA investments. As noted in the task force's findings, no rigorous means for evaluating DiD systems, architectures, or technologies exist today.*
- *The testbed should be implemented no later than July 2001, and augmented to support GIG IA technology, architecture and metric evaluation over a five-year period.*
- *Additional tasks for the GIG IA R&D testbed include:*
  - *Develop metrics for protect, detect, and react (consistent with JV2020)*
  - *Combine real networks with simulation to achieve sufficient scale*
  - *Relate testbed experiments to real world via selected exercises and experiments*
  - *Test, evaluate and determine vulnerabilities, including wireless*
  - *Transfer results to GIG as P3I*
  - *Provide feedback to industrial base*

Time:

- *Establish version 1 testbed by 1 July 2001; Support test, evaluation and analysis efforts and testbed upgrades through 2006*

Cost = $200M over five years

Public Key Infrastructure

- ***The task force recommends that the DoD begin the process of incorporating IA, and specifically PKI/PKE, into the DII COE. In discussing alternatives with representatives from DISA, it was noted that the Common Operating Picture (COP) application is critical to CINC and Services Joint-Task-Force-mission success. For a modest investment focused on PKE of this application, an acceleration of PKI into the COE – as generic, run-time utilities – can be accomplished. In addition to gaining important experience with PKE in battlefield applications, PKI could be integrated into the COE setting software standards and infrastructure for use in other Service and CINC C4ISR systems.***
- *Although IA infrastructure is planned to be incorporated into the COE "sometime in the future", the task force believes that accelerating this process is critical to ensure consistent PKE with tactical C4ISR systems. Experience gained sooner rather than later is key to effectively deploying an IA-enabled COE for the GIG.*
  - *Director DII COE office should develop IA infrastructure consistent with GIG system architecture*
    - *Select operational application and integrate PKI with Services (e.g., COP)*
    - *Establish Common Operating Environment (COE) generic IA services using NSA Key Management Infrastructure (KMI)*
    - *Provide generic services as COE infrastructure and DoD PKI as available*

Time:

- *Develop and deploy PKE COP by 1 September 2002*

Cost = $10M over two years

TECHNOLOGY RECOMMENDATIONS:

Invest in R&D to Stay Ahead of the Adversary

- *Task and resource the GIG Executive Director to create a vigorous, sustained and balanced IA R&D program to maintain GIG security. Promising areas for investment include:*
  - *Scaleable network sensing, anomaly detection, diagnosis*
  - *Malicious code detection high-speed network IA*
  - *Self-healing, recovery and reconstitution*
  - *Traceback, forensics, tagging*
  - *IA modeling and simulation*

Time: 1 October 2001

Cost: +$40M in first year, +$350M over 5 years

- *Promising tools and techniques should be tested on the R&D test bed outlined above.*

HUMAN RESOURCES AND READINESS RECOMMENDATIONS:

Integration of DIO into mission planning and execution

The task force recommends that the Secretary of Defense, and Chairman, Joint Chiefs of Staff should:

- *Issue guidance to make DIO a key element of all military planning and operations, to include promulgating ROE, continuity of operations plans, and conducting unit training exercises,*
- *Promulgate guidance in the Joint Military Readiness Review (JMRR) and other appropriate Service readiness reporting systems,*
- *Measure and assess IA readiness, and specify policies to hold commanders accountable for aspects of DIO readiness within their control.*

Time:. Initial actions by October 2001, with completion no later than October 2002

Estimated cost of implementation: Approximately $500K for initial actions. Budget requirements for completion will need to be developed and submitted for the PPBS process.

Red Team Activities

The task force recommends that the Secretary of Defense should formalize and empower DIO Red Teaming throughout the DoD by:

- *Developing a three level assessment capability:*
  - *Level I: Vulnerability Assessment*
  - *Level II: Vulnerability Evaluation*
  - *Level III: IO Red Team*
- *Establishing policy that defines authorities and responsibilities,*
- *Expanding the number, scope and frequency, and*
- *Providing adequate staffing and resources to accomplish expanded mission (technology, tools, manning).*

Time: Begin actions as detailed by October 2001

Estimated cost of implementation: $30M per year

Assessment of Civil Sector Dependencies

The task force recommends that the Joint Project Office- Special Technology Countermeasures (JPO-STC in Dahlgren, VA) should be:

- *Chartered to assist local commanders in identifying and assessing key infrastructure dependencies and vulnerabilities of DoD Elements,*
- *Designated as a critical element in the DoD DIO readiness system,*

- *Subordinated to Joint Forces Command with a military O-6 in charge, and*
- *Manned, equipped and resourced to do the job.*

Time: Begin actions as detailed by October 2001

Estimated cost of implementation: $25M per year

CERT/CIRT Activities and Coordination

The United States Space Command, supported by Office of the Secretary of Defense/Joint Chiefs of Staff Policy should:

- *Develop doctrine/ Tactics, Techniques and Procedures (TTPs) on emergency response, including deployment when necessary,*
- *Implement CERT clearinghouse capabilities,*
- *Provide access to standardized & advanced tools and methodologies,*
- *Establish common reporting formats and a shared common database,*
- *Develop a standardized alerting process, and*
- *Establish additional CERTs where needed at C/S/A.*

Time: To be implemented by October 2001

Estimated cost of implementation: $50-70M over the FYDP

Roles, Missions and Responsibilities

The task force recommends the following action be taken by the Department:

- *SecDef and CJCS should clearly define roles, missions and responsibilities of organizations tasked with DIO functions, including clarifying chains of command and relationships with other organizations.*
- *When tasking organizations to perform these additional functions, resources should be provided, along with priorities of execution of missions.*

Time: To be implemented by October 2001

Estimated cost of implementation: Minimal for definitions. Resources for tasking addressed in separate recommendation.

The IT Workforce

To find and keep the IT talent necessary for successful implementation and execution of the GIG, the task force recommends the following actions be taken by the Department:

- *The Secretary of Defense should direct more aggressive recruitment and retention efforts. The SecDef should also direct a proficiency pay for critical DIO skills. The authorities to accomplish this already exist.*
- *ASD/C3I in coordination with USD/P&R, should develop formal career paths for DIO officer, enlisted, civilian personnel.*
- *DoD needs to develop an outsource strategy to complement DoD key DIO resource needs and develop an "Education and Training for Service" program, for example, of 5 years tenure.*

Time: To be implemented by October 2001

Estimated cost of implementation: $25M per year

DIO Training and Awareness

The task force makes the following recommendations:

- *SecDef, ASD(C3I), USD(P&R), USD(AT&L) and Military Departments should establish policy to develop and implement formal Education, Training, and Awareness (ETA) programs for DIO throughout DoD. These programs should:*
  - *Codify the DIO training program within the formal DoD Joint Training System (JTS)*
  - *Ensure DIO programs are consistent with commercial and DoD certification standards*
  - *Require contractor personnel performing outsourced DIO functions to meet ETA criteria required for government employees.*

Time: Establish the recommended program by 1 October 2001.

Estimated cost of implementation: $150M over the FYDP.

Personnel Shortfalls and Reserve Component Configurations

The task force recommends the following:

- *The Deputy Secretary of Defense should direct USD(P&R) and ASD(C3I) to implement the recommendations from both the Reserve Component Study and the Defense Science Board task force on Human Resources Strategy.*

Time: To be implemented by October 2001

Estimated cost of implementation:

- *For Human Resource Management DSB: as determined by the study, applicable to IT workforce*
- *For Reserve Component Study: $10.5M over the FYDP*

IT Personnel Security

The task force recommends the following actions be taken by the Deputy Secretary of Defense:

- *Mandate an innovative and effective security program for critical IT professionals, which might include:*
  - *System Administrator auditing software,*
  - *Open source commercial style background investigations,*
  - *Peer accountability,*
  - *Pre-employment agreements,*
  - *Credit Checks, and*
  - *Two-person integrity for certain functions.*

Time: To be implemented immediately

Estimated cost of implementation: $5M per year

DIO Funding Strategy

The task force recommends the Secretary of Defense should:

- *Develop a DIO funding strategy and profile, establishing priorities where sufficient funding does not exist and provide implementation guidance on this strategy to DoD components.*
- *Where funding is insufficient to meet requirements, reallocate, reprioritize existing programs and support justification in the budget process for necessary across- the-board increases in budget allocations.*

Time: To be implemented by October 2001

Estimated cost of implementation: Total IA Budget for DoD should be around $3B/year, an increase of about $1.4B over current documented funding.

POLICY AND LEGAL RECOMMENDATIONS:

Terminology and Definitions

To facilitate the standardization of DIO-related definitions, the task force recommends the following actions:

- *The Secretary of Defense and the Director of the CIAO should jointly sponsor an effort to produce an authoritative document (perhaps an Executive Order) containing DIO-related terms which would be useful in both the national security and civil sectors of government. This effort should draw upon the work of the IWG established by the PRD on IO.*

To assist this effort, the following Office of the Secretary of Defense (OSD) actions should be undertaken:

- *DoD & IC General Counsels (GCs) should work with the DOJ to develop a common concept for and set of terms to be used when conducting "investigations" in cyberspace.*
- *The Bilateral IO Steering Group (BIOSG) should create a joint DoD/IC working group to produce the largest possible set of common IO-related definitions. The term DIO should be included..*
- *USD(P) should initiate a dialogue with the State Department regarding common DIO definitions. The goal of these talks would be to encourage the use of common DIO-related terms throughout the State Department and the DoD.*

The challenge will be to reach out beyond DoD and the IC to include the private sector, the law enforcement community, and the rest of government in the process. For this reason, the effort requires sponsorship at the National Security Council (NSC) or Executive Office of the President (EOP) level.

DIO Responsibilities and Coordination

To foster an environment where effective and timely decision-making can occur, the task force makes the following recommendations:

- *The Secretary of Defense should propose the creation of a national DIO coordinator. Prior to congressional action, the Coordinator's authorities will be limited. In the interim, he could serve as the focal point for of DIO policy development. Eventually, this individual should sponsor the development of national-level, coordinated DoD/IC/Law Enforcement mechanisms to provide I&W of a cyber-attack, respond to it, and recover from its effects.*

To support this effort the SecDef and DCI should:

- *Create a joint DoD/IC panel to work with the DOJ and NSC staffs to draft a DIO Executive Order (EO). The EO should clearly establish the preeminence of the national security response over the law enforcement response in cases having a national security impact.*
- *Create a panel to examine relevant law, policy, and regulations in light of emerging DIO realities (to include EO 12333.)*
- *Create a standing GC's working group to monitor legal precedents for decisions useful and inimical to DIO efforts and to explore the latitude available for DIO under existing law.*
- *Task the BIOSG to propose mechanisms for the military services and the IC to resolve conflicts relating to DIO (especially related to Computer Network Operations.)*
- *Declare the Information Operations threat a "Hard Intelligence Problem" and initiate the following steps:*
  - *The SecDef should request that the Director of Central Intelligence critically evaluate the Intelligence Community's ability to collect, analyze, and report intelligence that would allow more confident national estimates of the foreign IO threat.*
  - *The SecDef should establish a viable Research and Development program to develop new tactical- and operational-level ISR systems to provide warning of IO attacks to operational commanders.*

Information Sharing and the NIPC

To encourage information sharing and cooperation in response to a cyber attack the task force makes the following recommendations:

- *The Secretary of Defense and the Attorney general should agree that information available to the NIPC or to the DoD (including the National Security Agency) regarding network intrusions or defense should be shared with the other agency absent a specific legal bar to such sharing, and that DoD will have a role in determining whether sharing should be restricted. The FBI should advise DoD that the "law enforcement sensitive" label placed upon information from the NIPC is to alert recipients to the sensitive nature of the information rather than prevent its flow to those requiring the information within the DoD.*
- *The Secretary of Defense should urge that the Attorney general direct the NIPC to share relevant network attack information with the National Security Council. Presently, this does not occur readily because of DOJ policy against sharing information on criminal investigations with White House personnel. There is, in the judgment of this task force, a clear distinction between information pertaining to network attacks and investigations of possible criminal activities by the White House staff.*
- *The Secretary of Defense should request that the DOJ reconsider its policy regarding the sharing of information gathered under Title III (wiretap statue) about network attacks. The task force finds that the law permits such sharing by DOJ regarding issues of national security.*

- *The Secretary of Defense should request that the DOJ reexamine its policies regarding grand jury secrecy. The task force believes that the law permits sharing by DOJ/FBI/NIPC regarding issues of national security. The NIPC does not agree with this interpretation. The rules on sharing grand jury information should be clarified to permit sharing for national security purposes. Until this is accomplished, computer crime investigations working cases with national security implications should be prohibited from using grand jury subpoenas without interagency approval.*
- *The Secretary of Defense should request that DOJ agree to allow a free flow of information about network attacks from NIPC to the National Security Council.*
- *The Secretary of Defense should request that the NIPC report directly to the office of the Director of the FBI as well as the office of the Deputy Attorney General. This would facilitate much more rapid decisions on issues relating to national security.*
- *Assuming a satisfactory resolution of the issues raised above, the Secretary of Defense should take specific steps to upgrade the DoD staffing to the NIPC.*
- *The Secretary of Defense should reduce legal barriers to defensive information operations by reducing unnecessary paperwork relating to "Red Teaming" and unnecessary restrictions on sharing of system logs with information security experts at the National Security Agency.*

Infrastructure Dependencies

The task force recommends the Department take the following actions to ensure a detailed assessment of potential risks inherent in the interdependent, underlying infrastructures.

- *Accelerate actions to identify critical infrastructure dependencies on the private sector; the DoD effort to produce sector CIP plans is a step in the right direction, but we would note that this is not moving along very quickly, primarily due to lack of funding.*
- *Expand DoD's interactions with the private sector and municipal providers of critical infrastructure services. This is best achieved on a localized level, between base commanders (or other DoD leadership) and the infrastructure owners and operators. Direct DoD installation commanders (with support of JPO-STC) to identify critical infrastructure vulnerabilities, assess mission impact, and take corrective action with private sector service providers.*
- *Explore contractually based guarantees from the providers of critical infrastructure services that improve reliability and redundancy of vital services, while advancing private sector-government partnership through mutual risk-analysis of those services.*
- *Work with Sector Lead Agencies to ensure that DoD requirements are incorporated into the information-sharing processes with the owners and operators of critical infrastructure.*
- *Advocate FOIA and other related legal relief to remove impediments to private sector information sharing.*

- *Fund and resource JPO-STC appropriately to support critical infrastructure assessments. As a minimum starting point, increase funding for such focused efforts to at least $25M per year.*
- *DoD should modify or develop a process to assess the fiscal impact of infrastructure consequences to CIP events.*

6.3 Concluding Comments

Achieving information and decision superiority is very challenging. It will take time and it will be expensive. However, Joint Vision 2020 requires such superiority. Within this context, information systems are truly a weapon system, and the DoD should take action to assure that they remain viable even under hostile attack. This task force does not see today the comprehensive set of DIO initiatives that are needed to implement the Department's vision.

APPENDIX A.

Terms of Reference

ACQUISITION AND
TECHNOLOGY

THE UNDER SECRETARY OF DEFENSE

3010 DEFENSE PENTAGON
WASHINGTON, DC 20301-3010

FEB 29 2000

MEMORANDUM FOR CHAIRMAN, DEFENSE SCIENCE BOARD

SUBJECT: Terms of Reference -- Defense Science Board Task Force on Defensive Information Operations

You are requested to form a Defense Science Board (DSB) Task Force to review and evaluate DoD's ability to provide information assurance to carry out Joint Vision 2010 in the face of information warfare attack.

Tasks to be accomplished:

Using the "1996 DSB report on Information Warfare – Defense" as the departure point, address the following:

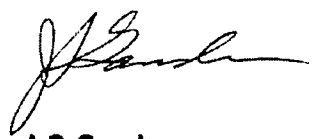
- What is the status of action on the recommendations?
- Where there are shortfalls, what are the barriers to action and what should be done?
- What important aspects did the 1996 Task Force miss that should have been addressed?
- Assess the recommendations of other important reports that have addressed information assurance issues.

The Defensive Information Operations Task Force will determine:

- Adequacy of the process toward the information assurance goals needed to carry out Joint Vision 2010.
- Adequacy of the Department's readiness to project and sustain power in the face of information warfare attacks.
- The appropriate role(s) and capability of DoD to provide information assurance in support of Homeland Defense and in support of Critical Infrastructure Protection.
- Recommendations for research and development which are uniquely in DoD's interest, and thus not likely to be accomplished by the private sector in the time required to meet DoD's Defensive Information Operations objectives.
- Areas in which DoD should seek strong partnering relationships outside DoD, such as with the Critical Infrastructure Assurance Office (CIAO).
- The Task Force should provide an interim report by June 30, 2000 and the final report around October 2000.

The study will be co-sponsored by the Under Secretary of Defense (Acquisition, Technology and Logistics) and Assistant Secretary of Defense for C3I. Mr. Larry Wright will serve as the Task Force Chairman; Col Gregory Frick will serve as the Executive Secretary; and Maj Tony Yang, USAF, will serve as the Defense Science Board Secretariat Representative.

The Task Force will be operated in accordance with the provisions of P.L. 92-463, the "Federal Advisory Committee Act," and DoD Directive 5104.5, "DoD Federal Advisory Committee Management Program." It is not anticipated that this Task Force will need to go into any "particular matters" within the meaning of Section 208 of Title 18, United States Code, nor will it cause any member to be placed in the position of acting as a procurement official.



J. S. Gansler

APPENDIX B.

Members and Government Advisors

Task Force Chairman:

Mr. Larry Wright	Booz-Allen & Hamilton

Panel Membership

Information Assurance Architecture Panel:

Chairman: Dr. Michael Frankel	SRI International
Members: Dr. Stephen Kent	BBN Technologies
Dr. Patrick Lincoln	SRI International
Mr. Al McLaughlin	MIT/LL
Mr. Peter Steensma	ITT Aerospace/Communications
Mr. John Woodward	MITRE Corporation
Government Advisor: Dr. Jaynarayan Lala	DARPA/ISO

Technology Panel:

Co-Chairs: Mr. Rich Mendelowitz	General Dynamics
Dr. Robert Mueller	Raytheon Company
Members: Mr. Bruce MacDonald	Consultant
Dr. Joe Markowitz	Consultant
Dr. Roy Maxion	Carnegie Mellon University
Dr. Dennis Polla	University of Minnesota
Government Advisors: Dr. Doug Maughan	DARPA/ITO

Human Resources and Readiness Panel:

Chairman: Mr. John Grimes	Raytheon Company
Members: MajGen John Casciano, USAF (Ret)	Litton/TASC
Mr. William Gravell	TRW
LTG Patrick Hughes, USA (Ret)	Private Consultant
Mr. Lowell Thomas	Verizon Communications
Government Advisors: Mr. Arnold Abraham	OASD (C3I)
CAPT Katharine Burton, USN	OASD (C3I)/DIAP
Mr. Peter Fonash	National Communications System
Mr. Gus Guissanie	OASD (C31)
CAPT Basil Harris, USN	J6K Joint Staff
BrigGen Paul LeBras, USAF	J-2 Joint Staff

LtCol Susan Pardo, USAF	AF/SCMI

Legal Panel:

Chairman: Mr. Stewart Baker	Steptoe & Johnson
Members: Ms. Elizabeth Banker	Yahoo! Inc.
Mr. Bill Burrington	AOL Europe
Mr. Roger Callahan	Bank Of America
Mr. Scott Charney	Pricewater-HouseCoopers LLP
Mr. Steven DeGeorge	AT&T Law Division
Mr. Lawrence Greenberg	The Motley Fool, Inc.
Mr. Jonathan Spear	MCI Telecommunications Corporation

Policy Panel:

Chairman: Mr. Richard Wilhelm	Booz-Allen & Hamilton
Mr. Brenton Greene	Sandia National Laboratories
Mr. David Henry	Scitor
Mr. Owen Wormser	C3I

Executive Secretary:

Col Gregory Frick, USAF	OASD(C3I)/I&IA

Defense Science Board Representative:

LtCol Tony Yang, USAF	DSB

Staff Support:

Mrs. Marya Bergloff	Strategic Analysis
Mr. Bob Evans	Booz-Allen & Hamilton
Ms. Julie Evans	Strategic Analysis
Mrs. Tyra Flynn	Strategic Analysis
Mr. Brad Smith	Strategic Analysis

APPENDIX C.

Briefings to the Task Force

January Meeting:

	Information Assurance and Survivability Vision Video (DARPA)
Honorable Arthur Money	C3I Perspectives
Mr. Richard Schaeffer, OASD (C3I)	DoD's Vision for Information Assurance
Mr. Bob Stoss, OSD/GC	Legal Ethics Briefing
MajGen John Campbell, JTF-CND	Joint Task Force- Computer Network Defense
CAPT Katherine Burton, OASD (C3I)	Current Status of 1996 DSB Study on IW-D Recommendations
Mr. Duane Andrews	1996 DSB Task Force on Information Warfare-Defense

February Meeting:

LtCol Perry Luzwick, OSD	Eligible Receiver/Solar Sunrise
CDR Bob Gourley, JTF-CND	Network Intrusion
Mr. Tom Bozek, OSD	DoD Insider Threat IPT Results
Mr. John Osterholz/Mr. Terry Hagle, OSD	Global Information Grid Architecture
Ms. Linda Brown, OSD	DoD Web Security Initiatives
	DIA Threat/I&W
	NSA Briefs: DIO Overview/Strategy
Ms. Maureen McHugh	Threat Briefing
CAPT Ed Kanerva	Red Teaming
CAPT James Newman, USN	Navy IA Overview/Capabilities
LtCol Dave Warner, USAF/	

LtCol Susan Pardo, USAF	AF IA Overview/Capabilities
	DIA IA Capabilities/Initiatives
Col Larry Huffman	DISA DoD CERT/IA VA Process

March Meeting:

LTC Leroy Lundgren, USA	Army IA Initiatives
BG Marilyn Quagliotti, USA JS/J6	Joint Staff Perspectives
	CIAO/National Plan
Mr. Chris Christiansen, IDC	Industry IA Perspectives
Ms. Bonnie Hammersley	Overview of DoD CIP Program
Mr. Doug Perritt	NIPC Overview
Maj Darwyn Banks, USAF	FedCIRC and FIDNET

April Meeting:

CAPT Katherine Burton, USN	OSD Human Resources IPT Studies
COL Andrew Twomey, USA	Joint Vision 2010/2020
Mr. Mike Green	DoD PKI Program
Mr. Richard Hale	DISA Future Concepts
Ms. Virginia Wiggins	Logistics IA Study: Theater Distribution
Mr. Jacques Sabrie	TRANSCOM IA Initiatives/GTN
Dr. John Mclean/Dr. Carl Landwehr	InfoSec Research Council (IRC)
Dr. William Mularie	DARPA Initiatives

May Meeting:

Dr. Sami Saydjari	
Dr. Michael Skroch	DARPA IA&S Program
Col Larry Klooster	USSPACE
Mr. Ed Lopez and Mr. Jacques Romain	CISCO Perspectives
Mr. Jeff Dunn	Biometrics
	NSA Senior IA Perspectives

June Meeting:

Dr. Lee Hammarstrom & Mr. Pat Dowd	Performance Needs/Developing technology
Dr. Mike Shore	Chessmaster and recent events
ADM Bill Studeman, USN (Ret)	History of IW
	CIA Strategic Warning/ Threat
Mr. John Keenan	U.S. Infrastructure Assurance Supporting Military Operations
Dr. Alan Royal	IOTC

July Meeting:

Mr. Jim Pinner and Mr. Dave Wilcox	IA Budget Brief
Mr. Lin Wells	"IO definitions"

APPENDIX D.

Status of Implementation of 1996 DSB Recommendations

Current Assessment of Recommendations from the *Report of the Defense Science Board Task Force on Information Warfare – Defense (IW-D)*

(November 1996)

1996 Recommendation	Current Status	Current Shortfalls
1. Designate an accountable IW focal point. The SECDEF should:		
1a. Designate ASD(C3I) as the accountable focal point for all IW issues.	DoD Directive S-3600.1 "Information Operations," 9 Dec 96, designates ASD(C3I) as the responsible authority for IW/IO.	
1a(1). Develop a plan and associated budget beginning in FY97 to obtain the needed IW-D capability.	Components were required to address IA budgets beginning with FYDP 1999-2002. The DIAP was established by DEPSECDEF to better coordinate and align IA budgets and assure adequate funding. – this effort has provided better visibility for overall DoD IA budget.	• There are no specific line items for IA. • Shortfalls identified by DIAP have been faced with a shortage of additional funds.
1a(2). Authorize ASD(C3I) to issue IW instructions.	DoD Directive S-3600.1 "Information Operations," 9 Dec 96, designates ASD(C3I) as the responsible authority for IW/IO. In addition, the DoD implementation of the Clinger-Cohen Act designates the ASD(C3I) as the DoD CIO and assigns the responsibility for IA to the DoD CIO.	
1a(3). Consider establishing a USD(Information).	No longer required; the ASD(C3I) has been designated the DoD CIO.	
1b. Establish a DASD(IW) and supporting staff to bring together as many IW functions as possible.	The June 1998 reorganization within OASD(C3I) resulted in the creation of a DASD for Security & Information Operations, a position that includes responsibility for Information Assurance, Infrastructure Assurance, Security, Counterintelligence, and Information Operations Strategy and Integration.	This organizational structure resides within OASD(C3I) and primarily includes those activities currently within the purview of OASD(C3I). This structure does not readily accommodate the corresponding DIO-related requirements/issues within OUSD(A&T), including related R&D within DARPA and the Military Departments.
2. Organize for IW-D.		

1996 Recommendation	Current Status	Current Shortfalls
2a. Establish a center to provide strategic indications and warning, current intelligence, and threat assessments. The SECDEF should request the DCI to:	NSA established the National Security Incident Response Center (NSIRC).	This organization is primarily focused on tactical activities rather than strategic activities, although in some cases, tactical level incidents may yield strategic insights.
2a(1). Establish an I&W/TA center at NSA with CIA and DIA support.	The DIA and JWAC are involved in this area.	There appears to be no overall DoD orchestrated approach to providing a strategic capability for DIO.
2a(2). Task and resource the Intelligence Community to develop the processes for Current Intelligence, Indications and Warning, and Threat Assessments for IW-D.	There are numerous activities within the Intelligence Community to address the intelligence requirements.	It is unclear as to how well these various activities are coordinated.
2a(3). Encourage the Intelligence Community to develop information-age trade craft, staff with the right skills, and train for the information age.	The DCI established the Advanced Research and Development Technology activity under NSA to focus on information technology as a multidisciplinary capability to the Intelligence Community.	The available skill set continues to fall well below the need.
2a(4). Conduct comprehensive case studies of U.S. offensive programs and a former foreign program to identify potential indicators – collection, funding, training, etc.	The DTRA "Chessmaster" case study is an example of the type of activity currently ongoing. Assessments continue as the capabilities and intentions of potential opponents change.	
2a(5). Establish an organization to examine and analyze probable causes of all security breaches.	NSA established the Network Incident Analysis Cell (NIAC) within the NSIRC to perform post network intrusion, forensic-style analysis of data received from incident response centers.	Analytical results and lessons learned are not effectively disseminated.
2a(6). Develop and implement an integrated National Intelligence Exploitation Architecture to support the organization and processes.	Intelligence Community activities in this area are ongoing.	Efforts are disparate and not integrated into a well-described plan.
2a(7). The SECDEF should direct the development of IW Essential Elements of Information (EEI).	Intelligence Community activities in this area are ongoing and JTF-CND is providing input into development of EEIs.	No final product or publication date has been set.
2b. Establish a center for IW-D operations to provide tactical warning, attack assessment, emergency response, and infrastructure restoration capabilities. The SECDEF should:	The DoD established the Joint Task Force – Computer Network Defense (JTF-CND) and the DISA Global Network Operations Center (GNOSC).	Concepts of Operations (CONOPS) for DIO mission execution are immature or do not exist. Where mission assignments have been made, lack of resources inhibits execution (e.g., USSPACECOM, JPO-STC).

1996 Recommendation	Current Status	Current Shortfalls
2b(1). Establish a DoD IW-D operations center at DISA with NCS, NSA, and DIA support.	The DoD established the DISA Global Network Operations Center (GNOSC).	DoD does not universally collocate its Network Operations Centers with Information Assurance (IA) / Computer Network Defense (CND) activities.
2b(2). Develop and implement distributed tactical warning, attack assessment, emergency response, and infrastructure restoration procedures.	Currently, JTF-CND does distribute tactical warning, but has minimal attach assessment capability. Emergency response is primarily coordinated through the various CERTS/CIRTS of the Services / Agencies. JTF-CND also assists in establishment of restoration priorities with DISA and other activities.	Recommended improvements in GIG architecture and security could provide a technology baseline to permit creation of a tactical/time-sensitive information attack warning sensor grid. Such a network would also support goals of assigning attacker attribution confidently and rapidly. However, any plan to achieve this outcome must span the domains of policy/law, technology and organization, and would require actions in several sectors of government, as well as private industry.
2b(3). Interface the operations center with Service and Agency capabilities and I&W/TA support.	This requirement is stated in the JTF-CND Concept of Operations; JTF-CND interfaces with these organizations continue to strengthen.	DoD CERT/CIRT activities vary in their execution and are not inclusive of all DoD CINCs/Services/Agencies.
2b(4). Establish necessary liaison (e.g., with military and government operations centers, service providers, intelligence agencies, and computer emergency response centers).	This requirement was completed as a result of the JTF-CND Concept of Operations.	
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.	The Defense-wide Information Assurance Program (DIAP) was established in 1998. It serves primarily as a facilitator for the gathering and sharing of IA-related information. In that role, the DIAP has accomplished much in identifying what is being done throughout DoD, and continues to focus on unifying/integrating various IW-D activities.	• The DIAP has no real authority to direct the Military Departments or Agencies, and does not control or impact any IW-D aspects of Service/Agency budgets. • Internal staffing and funding shortfalls have further hampered the DIAP's ability to accomplish the mission.
2d. Establish a joint office for system, network and infrastructure design.	There are current activities to develop, promulgate and implement Joint Technical Architecture (JTA), Joint Operational Architecture (JOA) and Joint Systems Architecture (JSA). Many recent efforts have centered on development of GIG architecture.	• There is no joint office to coordinate these various activities. • The GIG IATF standards and protocols for providing security are inconsistent with the JTA.

1996 Recommendation	Current Status	Current Shortfalls
2d(1). Establish a joint security architecture/design office within DISA to shape the design of the DoD information infrastructure.	OASD(C3I), DISA, NSA, Joint Staff and Service representatives participate in the activities cited in 2d.	• There is no joint office to coordinate these various activities. • The IATF is a collection of history and general information; it is not a document that can be used to implement interoperable, secured information systems for DoD.
2d(2). Establish a process to verify independently and enforce adherence to these design principles.	The DoD established the Defense Information Technology System Certification and Accreditation Process (DITSCAP), as well the Secret And Below Interoperability (SABI) and Top Secret And Below Interoperability (TSABI) processes. Processes within the GIG governance arena are also being established to enforce adherence to GIG architecture requirements.	There are insufficient resources to implement DITSCAP, SABI, and TSABI at a pace that meets the demands within the DoD. Temporary waivers or work-arounds can prove counterproductive to the process.
2e. Establish a Red Team for independent assessments.	Some Red Team capabilities exist within the Services, NSA, and DIA.	Due to lack of clear policy and resources, aggressive, comprehensive, effective operational Red Team activities are lacking across DoD.
2e(1). Establish a Red Team which is accountable to SECDEF/DEPSECDEF and independent of design, acquisition, and operations activities.	No Red Team has been established to be directly accountable to the SECDEF/DEPSECDEF, independent of design, acquisition, and operations activities.	Without such an independent Red Team capability, current Red Team results may be questionable because of organizational affiliation/loyalties.
2e(2). Develop procedures for employment of the Red Team.	Thus far, the DoD has developed the Defensive Information Assurance Red Team (DIART) Manual.	Due to the lack of clear Red Team policy, there is no formal requirement for DIART to be implemented DoD-wide, and it is often ignored. This Red Team Manual provides the standardized procedures for any DoD Red Team, but absent a DoD Directive, there is no way to mandate their use. Additional, guidance needs to be provided on how results of the Red Teams (and any other assessment) are collected and analyzed to determine trends and lessons learned.
3. Increase awareness. The SECDEF should:		

1996 Recommendation	Current Status	Current Shortfalls
3a. Establish an internal and external IW-D awareness campaign for the public, industry, CINCs, Services, and Agencies	In June 1998 the ASD(C3I) and the USD(P&R) jointly issued a memorandum that required IW-D user awareness and training. There are currently numerous IW-D training activities throughout the DoD.	Conflicting definitions and usage related to IO, IA and CIP within the DoD and Intelligence Community causes resource and equity fights within the federal National Security Community and inhibits progress in resource management, training, and other important areas.
3b. Expand the IW Net Assessment recommended by the 1994 Summer Study to include assessing the vulnerabilities of the DII and NII.	Over the past five years, OSD - Net Assessment made several attempts to assess various aspects of IO. In each case, the assessment's value was limited by a lack of meaningful metrics. While the assessment could catalog and relate interesting anecdotal information, it would not provide the Secretary with the factual information necessary to make programmatic decisions. Accordingly, Net Assessment shifted its focus toward developing metrics by which the value of information under differing circumstances could be measured.	The IW Net Assessment has not yet been accomplished.
3c. Review joint doctrine for needed IW-D emphasis.	Joint Pub 3-13 (Defensive IO) was issued on October 9, 1998. CJCSI 6510.01B (Defensive IO Implementation), issued 26 August 1998, is currently under revision, with the new version expected to be issued in January 2001.	Doctrine and implementation instructions need to be adequately tested in exercises and integrated into mission planning and execution.
3d. Explore possibility of large-scale IW-D demonstrations for the purpose of understanding cascading effects and collecting data for simulations.	The Joint Staff and CINCs have sponsored exercises in which IW-D was a component.	It is unknown as to whether there have been large scale IW-D demonstrations conducted solely for the purpose of understanding the cascading effects and for collecting data for simulations. The modeling and simulation community lacks maturity in tools to assess these effects.
3e. Develop and implement simulations to demonstrate and play IW-D effects (USD(A&T) lead)	Current status is unknown.	Current status is unknown.
3f. Implement policy to include IW-D realism in exercises.	The Joint Staff and CINCs have sponsored numerous exercises in which IW-D is a component. Exercise plans are increasing in sophistication to address these issues.	IW-D demonstrations do not effectively reflect cascading effects for collecting data for simulations.

1996 Recommendation	Current Status	Current Shortfalls
3g. Conduct IW-D experiments.	DARPA and the C4I Joint Battle Center have conducted IW-D experiments.	It is unknown as to whether there have been large scale IW-D experiments conducted for the purpose of understanding cascading effects and collecting data.
4. Assess infrastructure dependencies and vulnerabilities. The SECDEF should:		There appears to be no overall DoD orchestrated approach to providing a strategic capability for DIO.
4a. Develop a process and metrics for assessing infrastructure dependency.	CIP (physical & cyber) analytical methodology has been identified and prototyped to link OPLANS / TPFDDs / Defense sector assets to analyze interdependencies	Prototype methodologies require thorough testing.
4b. Assess/document operations plans infrastructure dependencies.	CIP (physical & cyber) analytical methodology has been identified and prototyped to link OPLANS / TPFDDs / Defense sector assets to analyze interdependencies	Prototype methodologies require thorough testing.
4c. Assess/document functional infrastructure dependencies.	Defense infrastructure sectors are in the initial stages of performing sector characterization which will include intradependencies and interdependencies with other sectors	
4d. Assess infrastructure vulnerabilities.	DoD and JPO are beginning to develop protocol to include/integrate CIP (physical & cyber) assessments of defense infrastructures into existing assessment processes/procedures.	
4e. Develop a list of essential infrastructure protection needs.	Work in this area is currently ongoing.	No anticipated delivery date has been set for a final product/report.
4f. Develop and report to the SECDEF the resource estimates for essential infrastructure protection.	Estimates have been generated for initial CIP (physical & cyber) requirements to perform limited analysis and assessment.	Estimates must be refined, documented, and formally reported in order to promote appropriate action.
4g. Review vulnerabilities of hardware and software embedded in weapons systems.	Not yet addressed. Recent changes in the DoD 5000 series and a Memo from USD(AT&L) adding security as an equal element to cost, schedule and performance for acquisition programs will assist in accomplishing this task. Reviews of some weapons systems were performed as a part of the Y2K effort and lessons learned should be incorporated.	• Lack of a formal requirement inhibits incentive to integrate these assessments into system development plans. • This area remains significantly vulnerable.

1996 Recommendation	Current Status	Current Shortfalls
5. Define threat conditions and responses. 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.	INFOCONS have been established. CJCSI Memorandum of March 1999 served as vehicle for dissemination throughout the DoD. USSPACECOM is in the process of reviewing and revising the INFOCON process to make it more usable and ensure appropriate establishment and promulgation throughout DoD.	Interpretation of the INFOCONS varies within organizations, which can adversely impact their collective implementation.
5b. Define and implement responses to IW-D threat conditions.	Rules of engagement are currently undergoing legal review at Secret level.	DoD implementation of responses is hampered by existing and conflicting governing authorities and related rules of engagement.
5c. Explore legislative and regulatory implications.	Legislative and regulatory implications are currently being addressed through various activities within the federal government, as well as the DoD.	Current legislation and conflicting roles/responsibilities/authorities with the Department of Justice are impediments to the process.
6. Assess IW-D readiness. The SECDEF should:		
6a. Establish a standardized IW-D assessment system for use by CINCs, MilDeps, Services, and Combat Support Agencies.	CJCSI 6510.04 (Information Assurance Readiness Metrics), 15 May 2000, provides a standardized information assurance list of items to consider when preparing the information assurance portion within the JMRR C4 functional area.	There is no adequate system for assessing DIO readiness across DoD. CJCSI 6510.04 is relatively unknown within the Military Departments and, buried within the C4 functional area, has relatively little impact on assessing readiness. Although it establishes a baseline, it is neither mandatory, nor does it apply to all DoD activities.
6b. Incorporate IW preparedness assessments in Joint Reporting System and Joint Doctrine, for example.	CJCSI 6510.04 (Information Assurance Readiness Metrics), 15 May 2000, provides a standardized information assurance list of items to consider when preparing the information assurance portion within the JMRR C4 functional area.	DIO is not adequately integrated into mission planning and execution. CJCSI 6510.04 is relatively unknown within the Military Departments and, buried within the C4 functional area, has relatively little impact on assessing readiness.
7. "Raise the bar" with high-payoff, low-cost items. The SECDEF should:		

1996 Recommendation	Current Status	Current Shortfalls
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.	NSTISSP No. 11, January 2000, requires that by 1 January 2002, acquisition of all COTS IA and IA-enabled IT products must be evaluated through the NIAP process. The NIAP provides a mechanism for certification of security products. NIST Special Publication 800-23 provides additional guidance in this area. In addition, the Defense in Depth strategy requires several levels of protection of networks and systems. Related security products include access control mechanisms (password control, PKI, biometrics), firewalls, intrusion detection devices, secure routers, etc.	
7b. Examine the feasibility of using approved products for identification and authentication.	The DoD PKI policy memorandum of May 1999 (replaced by the August 2000 Memo), establishes the DoD Public Key Infrastructure policy and Program Management Office (PMO). It establishes the desire to seek maximum use of COTS technology.	
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.	Current DoD PKI policy addresses the use of escrowed encryption. The "insider threat" issue is being addressed by various efforts, one of which is through the Insider Threat IPT, which is looking at a spectrum of technical, policy, training, and other options to address this issue.	Systems Administrators have the "keys to the kingdom," yet often require no special "reliability" investigations, such as those in the Personnel Reliability Program.
8. Establish and maintain a minimum essential information infrastructure. The SECDEF should:	Through the Y2K efforts, the DoD identified its minimum essential information systems ("thin-line"). This effort serves as a starting point for the CIP (physical & cyber) activities.	The critical infrastructures that are essential to the minimum operations of the economy and government are predominantly owned by the private sector. The DoD is extremely dependent upon these private sector systems, networks and infrastructures, but industry is not motivated to share information on their vulnerabilities with the government.
8a. Define options with associated costs and schedules.	Processes for defining and resolving associated funding requirements are under development.	

1996 Recommendation	Current Status	Current Shortfalls
8b. Identify minimum essential conventional force structure and supporting information infrastructure needs.	Addressed, in part, in JV2010 and JV2020.	Significant personnel resource shortfalls impact execution of the DIO mission at all levels in DoD.
8c. Prioritize critical functions and infrastructure dependencies.	Under development.	No final product/report or due date has been defined or funding applied.
8d. Design a Defense MEII and a failsafe restoration capability.	The CIO organization is applying lessons learned from the Y2K experience in registering applications, determining mission critical/mission support and policies concerning NIPRNET access.	
8e. Issue direction to the Defense Components to fence funds for a Defense MEII and failsafe restoration capability.	No guidance issued to date.	The DoD continues to remain vulnerable.
9. Focus the R&D. The SECDEF should focus the DoD R&D program on the following areas:	The DIAP Research & Technology (R&T) functional area was established to provide focus in the DoD IA R&D areas. This functional area works primarily with the InfoSec Research Council (IRC), a voluntary member organization of a number of activities (DoD and non-DoD), doing IA research.	
9a. Develop robust survivable system architectures.	DARPA sponsored major program in this area.	• The DoD is managing its current information assurance R&D in a fragmented way that is not sufficiently focused on the information assurance requirements of the GIG. • The current DoD network architecture calls for a secure network with authorized access via tokens (i.e., PKI). The scope of this security apparatus is enormous, and PKI has not been modeled and tested under extreme requirements.
9b. Develop techniques and tools for modeling, monitoring, and management of large-scale distributed/networked systems.	Previous and ongoing IA R&D efforts are addressing this area.	Development and deployment of new network technology has greatly outpaced information assurance technology, thereby increasing the vulnerability of DoD systems.

1996 Recommendation	Current Status	Current Shortfalls
9c. Develop tools and techniques for automated detection and analysis of localized or coordinated large-scale attacks.	Previous and ongoing IA R&D efforts are addressing this area.	• One of the weakest aspects of U.S. DIO is our extremely limited ability to detect, assess, and understand both hostile IO capabilities and precursor indications and warning of attack. • No methods exist for automated or assisted discovery of existing or novel attack patterns or signatures, particularly for those attacks which are distributed across many computes or networks. • Intrusion detection technologies curently produce only moderately reliable results in simple environments, and even less reliable results in complex environments.
9d. Develop tools for synthesizing and projecting the anticipated performance of survivable distributed systems.	Previous and ongoing IA R&D efforts are address this area.	DoD does not have a methodology for restoring integrity in its systems.
9e. Develop tools and environments for IW-D oriented operational training.	The Joint Battle Center is chartered to perform this work and has a number of on-going activities to address issues in this area.	The DoD is not aggressively or innovatively addressing its IA R&D personnel requirements, which will likely lead to more serious problems in the next few years as more personnel leave the department and fewer high caliber R&D managers remain.
9f. Develop testbeds and simulation-based mechanisms for evaluating emerging IW-D technology and tactics.	Previous and ongoing IA R&D efforts are address this area.	Progress in defending and protecting the GIG will require a far greater ability to model and simulate the performance of information infrastructures than we have today.
9g. The SECDEF should work with the NSF to develop research in U.S. computer science and computer engineering programs.	NSA's Information System Security Engineering program is working with 7 universities in this area.	This NSA program is independent and not implemented with NSF.
9h. The SECDEF should work with the NSF to develop educational programs for curriculum development at the undergraduate and graduate levels in resilient system design practices.	NSA's Information System Security Engineering program is working with 7 universities in this area.	The degree to which the NSA program, which is implemented independent of NSF, is addressing curriculum development is unknown.
10. Staff for success. The SECDEF should:		

1996 Recommendation	Current Status	Current Shortfalls
10a. Establish a career path and mandate training and certification of systems and network administrators.	An IT/IA Human Resources IPT was established to examine issues associated with the establishment of an IA/IO career path. An OSD memorandum in June 1998 addressed mandatory training.	The shortage of DoD IT professionals is serious and growing.
10b. Establish a military skill specialty for IW-D.	Skill specialties have yet to be established. The Joint Staff has a tasking to develop common skill sets for specific functions in this area. The military Services have all undergone major restructuring of their military skill sets to identify, recruit and retain professionals in this area.	The appropriate staffing of DIO positions continues to be severely hampered.
10c. Develop specific IW awareness courses with strong focus on operational preparedness in DoD's professional schools.	There are numerous activities in this area. IA awareness products and activities, and IA/IO courses, are provided at all professional military education facilities.	The DoD workforce at all levels is ill prepared to execute the DIO mission because current training efforts are fragmented, inadequately scoped, and poorly documented.
11. Resolve the legal issues. The SECDEF should:		

1996 Recommendation	Current Status	Current Shortfalls
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.	• Legal guidance has been promulgated and policies are under review regarding the monitoring and auditing of network activities. • Intrusion Detection Systems perform a portion of this function. • Guidance on configuration of the various devices is provided as technology changes. • Additional mechanisms to identify and warn intruders are being investigated, as well as a general announcement of DoD policy and intent through the normal media channels. • Rules of engagement issues, including active defense are being investigated to determine possible actions.	The use of banners can only address the "insider issue." Intruders into systems generally bypass standard entry routes and it is virtually impossible to set up mechanisms for banners to be present on all entry points.

1996 Recommendation	Current Status	Current Shortfalls
11b. Provide to the Presidential Commission on Critical Infrastructure Protection proposed legislation, regulation, or executive orders for defending other systems.	OBE, since PDD 63 was signed. However, there are a number of ongoing legislative activities being addressed among the NIPC, Federal CIO Council, and the CIAO.	• The DoD is suffering under existing legislation. Although it has the responsibility for national defense, it has been forced to rely on law enforcement agencies such as the FBI and the Justice Department to gather information about attacks. • Under existing law, network service providers may give away information about hacking attacks to the public, but they are legally prohibited from giving the information to a government agency unless the agency begins a criminal investigation. • There is no clear guidance as to which takes precedence: the confidentiality of criminal investigations or the national security interests of the United States. • Criminal wiretap authorities are inadequate for the government to maintain wiretap coverage of persons engaged in long-term hacking campaigns against government networks. • Current law concerning "trap and trace" orders often requires that law enforcement agencies seek multiple, sequential orders as they trace a single hacker from system to system.
12. Participate fully in critical infrastructure protection. Regarding the activities of the President's Commission on Critical Infrastructure Protection, the SECDEF should:		
12a. Offer specific Department capabilities to the President's Commission.	OBE, since PDD 63 was signed. However, there are a number of activities in the CIP area that are working with the CIAO to address the spirit of this recommendation.	

1996 Recommendation	Current Status	Current Shortfalls
12b. Advocate the Department's interests to the President's Commission.	OBE, since PDD 63 was signed. However, there are a number of activities in the CIP area that are working with the CIAO to address the spirit of this recommendation.	• No one has the responsibility or authority to make response and recovery decisions and take actions across stovepipes. Coordination depends upon personalities. • The State Department is potentially very important to DIO, but is not sufficiently engaged. • A great portion of government doesn't understand DIO issues or appreciate the potential impact of information technology vulnerabilities on their operations.
12c. Request the Commission provide certain national-level capabilities for the Department.	OBE, since PDD 63 was signed. However, the NIPC, for which the DoD provides personnel resources, provides the law enforcement capabilities.	• There is no clear responsibility for rationalizing law enforcement and national defense equities when certain types of cyber attack are detected. • There is currently a bias toward using law enforcement authorities and procedures when a cyber incident is detected. Although this will be satisfactory in the vast majority of cases, no formal means exists to review cases to determine if national security procedures might be more appropriate.
12d. Suggest IW-D roles for government and the private sector.	OBE, since PDD 63 was signed. PDD 63 established roles and responsibilities.	
13. Provide the resources. Develop a plan and associated budget beginning in FY97 to obtain needed IW-D capability (ASD(C3I) lead)	The DIAP is currently attempting to obtain IW-D funding requirements from DoD organizations. With the improved visibility into DoD component budgets, areas requiring additional funding are being identified. The DIAP has established appropriate mechanisms through the PPBS process to identify and justify shortfalls – the issue is how to prioritize and obtain additional funding in a tight budget environment.	The Department has not sufficiently funded protection of its networks and DIO programs. Of particular concern in the Sensitive, But Unclassified (SBU) information, which is critical to JV2020.

APPENDIX E.

Information for Decision Superiority

INFORMATION FOR DECISION SUPERIORITY

"Decision superiority" is the ability to use information and experience to make battlespace decisions faster and better than any adversary, ensuring a continuing and overwhelming pace and effectiveness of operations, as illustrated in Figure E-1. If adversaries and potential adversaries believe the U.S. military is consistently able to use decision superiority to achieve execution superiority, the nation will have created a useful strategic deterrent in addition to a superior capability in conflict and other operations. Decision superiority is a central enabler for achieving U.S. military dominance in future crises. It is also a potential vulnerability, since it depends on Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR) resources that an adversary might disrupt in a variety of ways.

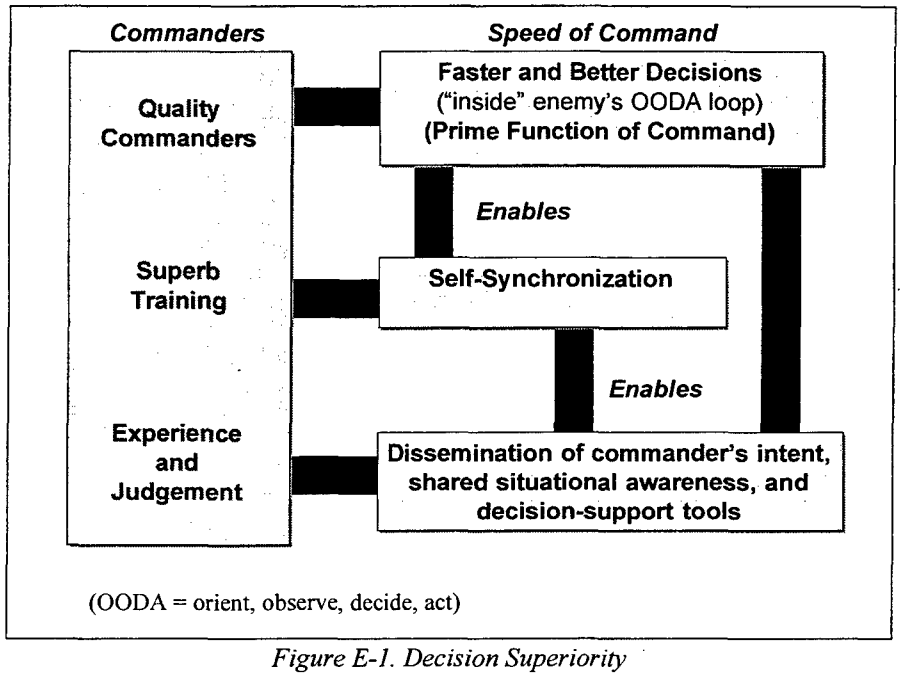


Figure E-1. Decision Superiority

The task force focused on decision superiority because of its key role in efficient and rapid execution of military missions. It is a central and difficult challenge for the Department. Effective decision superiority requires that every commander, at every level, know what the next higher commander wants him to accomplish – the purpose, the commander's intent, and what is going on in and around an individual unit, regardless of unit size. While there are technical aspects to this objective, the challenges in providing operational decision superiority have more to do with human capability and human understanding. The task is to provide information in such a way that commanders can absorb it, understand it, and use it quickly and effectively to shape their battlespace decisions.

"Information superiority," as it has generally been understood, is essential to achieving decision superiority, but not sufficient. Given the rapid growth of wide-band commercial communications and high-resolution commercial imagery, many adversaries will have access to

information similar to that available to U.S. forces. The ability to gain decision superiority will be based on two general areas: the cognitive capability and preparedness of the decision-maker and the available technical tools. The cognitive issue revolves around quality people and quality training.

Quality personnel, with training and experience, are an essential basis for decision superiority to enhance the commander's ability to make decisions. Enhanced communications, better information presentation, expanded bandwidth, decision support agents, and intelligent agents are all keys to enhancing the commander's ability to gather, assess, analyze, and act on data. These tools also enhance the commander's ability to transform decisions to actions, assess the result of the actions, and iterate through the decision loop. These requirements frame the "grand challenge" for the decision system: to create data and translate it into information at a rate adequate for a commander to access the information and convert it into decisions.

The goal is to ensure a speed of command, pace of operations, and level of operational efficiency and effectiveness that no adversary can manage, regardless of available information resources. Decision superiority comes from the ability to leverage the quantity and type of information available about the battlespace and the forces within it – both friendly and adversary. More timely and better-informed decisions will allow decision-makers to operate "inside" the enemy's orient-observe-decide-act (OODA) loop, generating an operational tempo with which the enemy is unable to cope. Thus, information superiority will lead to decision superiority, and ultimately, to execution superiority.

Operational Architecture

At the core of decision superiority is a high-level operational architecture. The centerpiece of the architecture, as illustrated in Figure E-2, is the premise that ***the warfighter must define and assemble his or her own information ensemble using information sources made available and accessible by the information community.*** No single individual or group of people can decide, in advance, what kind of information needs to be assembled and pushed to commanders under constantly changing operational conditions, at multiple-command levels, and in multiple complex situations. Thus, the task of assembling needed information must be left to the individual – from Commander in Chief (CINC) to platoon leader.

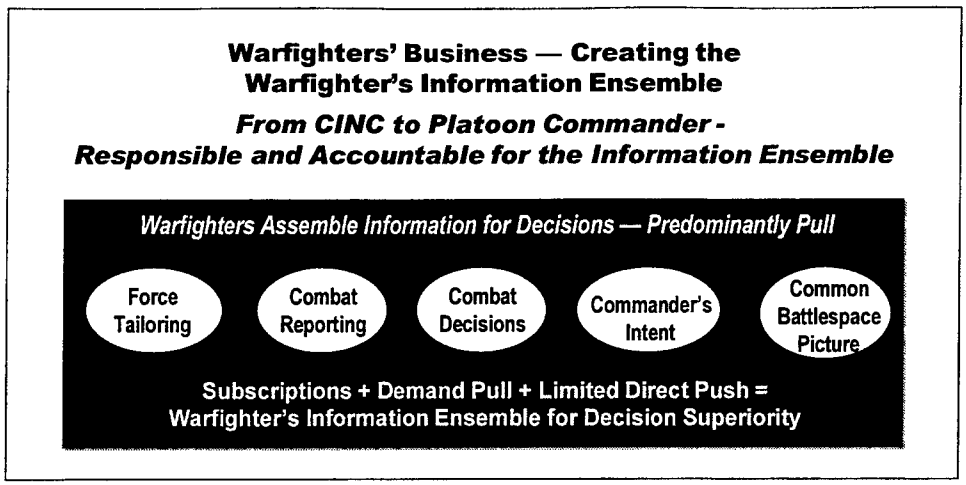


Figure E-2. Warfighter's Information Ensemble

The rest of the operational architecture needs to assist the warfighter in creating a tailored information ensemble. Thus, the warfighter must be responsible and accountable for assembling an information ensemble and for ensuring that information needs are known. Commanders must be aggressive in making certain that the right information is made available when and where it is needed.

The infrastructure level of the operational architecture is the ***Integrated Information Infrastructure***, as shown in Figure E-3.[36] This level requires a set of enablers to help the warfighter access, absorb, and assess information. The infrastructure is composed of a warfighter-tailored battlespace information display, distributed information collection and storage repositories, and automated aids for reliable transmission, storage, retrieval, and management of large amounts of information. It will provide a common operating picture for all users. In effect, the Integrated Information Infrastructure contains a "super database" of everything relevant to the battlespace.

[36] Chapter 2 describes both a conceptual and systems view of the Integrated Information Infrastructure, as well as a series of recommendations for its implementation.

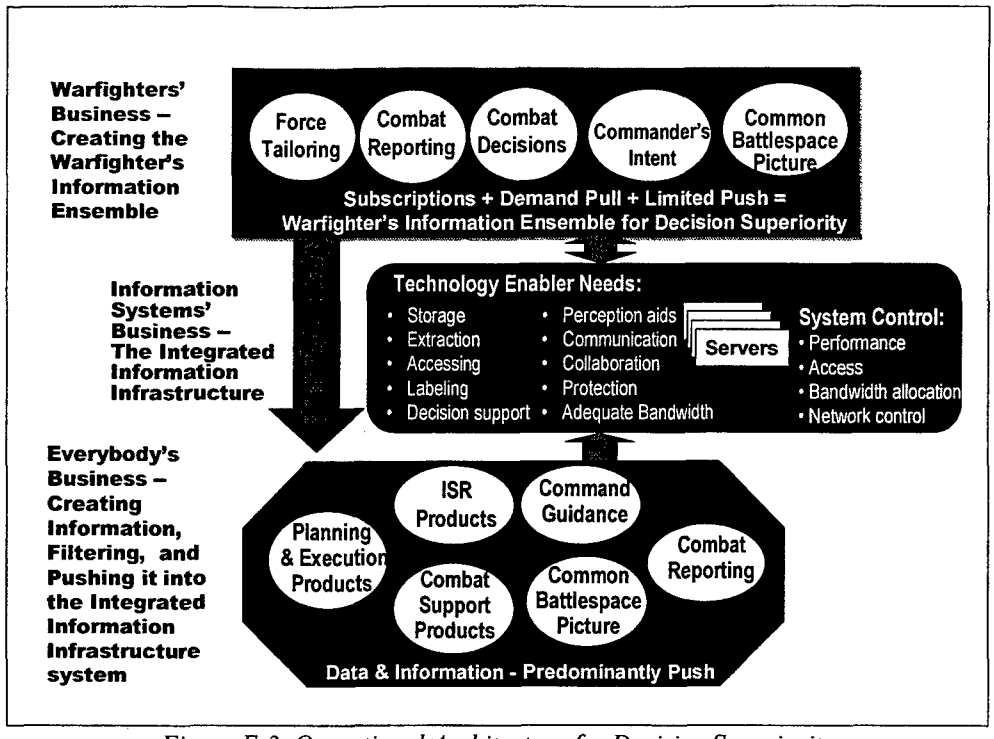


Figure E-3. Operational Architecture for Decision Superiority

The warfighter will be able to create a personalized information ensemble using a suite of tools developed by the technology community and embedded as services in the Integrated Information Infrastructure. These will include software tools such as browsers and search engines in the near term and intelligent software agents in the future to both manage the infrastructure and the information residing therein. The guiding principal is that the decision-maker be able to "pull" information from the architecture, using automation to sort, arrange, filter, and find items of interest. A "pull" system works in a variety of ways. The user may subscribe to information known to be available. The system must also allow for "demand" pull for specific information that the commander needs but to which he did not subscribe at the outset. And, at times, the system will need to accommodate a limited amount of information "push" – such as the commander's intent or warnings. The Internet has validated that the "pull" system works. The user needs information that is presented and tailored to his needs, and the system provides automation to help the user find information quickly and without error. "Information overload" should not be a problem in a pull-dominated system, unless commanders intentionally choose to overload themselves.

To enable the warfighter to receive and assess information, the Integrated Information Infrastructure provides housekeeping and information management services that ensure accurate, timely, synchronized, and consistent information. For example, if new intelligence is gathered that raises inconsistencies between various pieces of information, the infrastructure must ensure that the information is re-analyzed to sort out and resolve the inconsistency. When the issue is resolved, the infrastructure must make sure that related databases are updated and relevant information is brought into synchronization. Methods for accomplishing this task include circulating dynamic smart agents, constant error-checking software, and effective and robust synchronization capabilities. Other functions include managing information and data flow,

modifying network architectures, and presenting information to network managers so that it can be adapted in response to changing mission needs.

The input level of the operational architecture is the ***data and information-gathering*** layer. At this level, data and information contributors "push" information into the information infrastructure level where it is indexed, categorized, and assessed. Analysts and automated processes work with the data to create information, which is then "pulled" from the system by the warfighter, as described above. It is important to note, as shown by the feedback arrow in Figure E-3, that warfighters at all levels are responsible for ensuring that deficiencies in data and information are well understood and transmitted to those pushing information into the system. This will be effective only if the information system is in continual use. It cannot work if it is assembled and exercised only periodically and sporadically in response to contingencies and exercises.

APPENDIX F.

Glossary

ACLU	American Civil Liberties Union
AFRL	Air Force Research Laboratory
AFIWC	Air Force Information Warfare Center
AOR	Area Of Responsibility
API	Application Program Interface
ASD(C3I)	Assistant Secretary of Defense for Command, Control, Communications and Intelligence
ATD	Advanced Technical Demonstrations
ATM	Asynchronous Transfer Mode
AWE	Advanced Warfighting Experiment
BoD	Board of Directors
BIOSG	Bilateral IO Steering Group
BSC	Base Switching Center
BTS	Base Transmission Systems
C2	Command and Control
C3I	Command, Control, Communications, and Intelligence
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance, and Reconnaissance
C4RDP	Command, Control, Communications, Computers, Requirements Definition Program
CAC	Common Access Card
CAP	Common Air Picture
CC	Common Criteria
CCA	Clinger-Cohen Act
CCITT	Consultive Committee on International Telegraph and Telephone
CDPD	Cellular Digital Packet Data
CDSA	Common Data Security Architecture
CECOM	U.S. Army Communications Electronics Command
CEC	Cooperative Engagement Capabilities
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CGP	Common Ground Picture
CIA	Central Intelligence Agency
CIAO	Critical Infrastructure Assurance Office
CINC	Commander in Chief
CIO	Chief Information Officer
CIP	Critical Infrastructure Program/Protection

CIPIS	Critical Infrastructure Protection Integration Staff
CJCS	Chairman, Joint Chiefs of Staff
CJCSI	Chairman, Joint Chiefs of Staff Instruction
CMA	Collection Management Authority
CMP	Common Maritime Picture
CNA	Computer Network Attack
CND	Computer Network Defense
CNE	Computer Network Exploitation
CNO	Computer Network Operations
COE	Common Operating Environment
COI	Community of interest connection-oriented interconnection
COMSEC	Communication Security
CONUS	Continental United States
COP	Common Operational Picture
COOP	Continuity of Operations Plan
CORBA	Common Object Request Broker Architecture
CORT	Cyber Operations Readiness Triad
COTS	Commercial-off-the-shelf
CRD	Capstone Requirements Document
CSCI	Commercial Satellite Communications Initiative
CVE	Common Vulnerabilities and Exposure
CWAN	Coalition Wide Area Network
DARPA	Defense Advanced Research Projects Agency
DASD	Deputy Assistant Secretary of Defense
DBS	Direct Broadcast Satellite
DCE	Distributed computing environment
DCI	Director Central Intelligence
DDCI	Deputy Director of Central Intelligence (CIA)
DDOS	Distributed Denial of Service (network attack)
DDR&E	Director Defense Research and Engineering
DEERS	Defense Enrollment Eligibility Reporting System
DepSecDef	Deputy Secretary of Defense
DES	Data Encryption Standard
DIA	Defense Intelligence Agency
DIAP	Defense-Wide Information Assurance Program

DIART	Defense Information Assurance Red Team
DiD	Defense-in-Depth
DII	Defensive Information Infrastructure
DIO	Defensive Information Operations
DISA	Defense Information Services Agency
DISN	Defense Information Systems Network
DITSCAP	Defense Information Technology System Certification and Accreditation Process
DNS	Domain Name System
DNSSEC	Domain Name Systems Security
DoD	Department of Defense
DOJ	Justice of Department
DoS	Disk Operating System; Day of Supply
DOS	Department of State
DOS	Denial of Service
DSB	Defense Science Board
DSC	Decision Support Center
DSCS	Defense Satellite Communications System
DSL	Digital Subscriber Line
DSTS-G	DISN Satellite Transmission Services - Global
DTRA	Defense Threat Reduction Agency
DWDM	Dense Wave Division Multiplexing
EDS	Electronic Data Systems
EFX	Expeditionary Force Experiment
EKMS	Electronic Key Management System
ELB	Extended Littoral Battlespace
EO	Executive Order
EOP	Executive Office of the President
ESC	Electronic Systems Command
ETA	Education, Training, & Awareness
ETS	Education and Training for Service
FBI	Federal Bureau of Investigation
FGAC	Fine-Grained Access Control
FIWC	Fleet Information Warfare Center
FOIA	Freedom of Information Act
FTX	Field Training Exercises

FYDP	Fiscal Year Defense Plan
G&PM	Guidance and Policy Memorandum
GAO	Government Accounting Office
GC	General Council
GCCS	Global Command and Control System
GEO	Geostationary Earth Orbiting
GIG	Global Information Grid
GloMo	Global Mobile
GNIE	Global Networked Information Enterprise
GNOSC	Global Network Operations Center
GSM	General Standard for Mobile
GSM	Ground Station Module
HALE	High Altitude Long Enduring
HLR	Home Location Register
HRM	Human Resources Management
IA	Information Assurance
IAA	Information Assurance Architecture
IC	Intelligence Community
ICAP	Integrated Communications Access Package
ICMP	Internet Control Message Protocol (DoD, TCP/IP)
ID/IQ	Indefinite Delivery/Indefinite Quality
IDC	International Data Corporation
IDS	Intrusion Detection System
IER	Information Exchange Requirements
IETF	Internet Engineering task force
IFF	Identification Friend or Foe
III	Integrated Information Infrastructure
IKE	Internet Key Encryption
IM	Information Management
IN	Intelligent Network
INFOCON	Information Condition
InfoSec	Information Security
IO	Information Operations
IOC	Initial Operational Capability
IP	Internet Protocol

IPSec	Internet Protocol security
IPT	Integrated Process Team
ISAC	Information Sharing and Analysis Center
ISDN	Integrated Service Digital Network
ISO	International Organization of Standardization
ISR	Intelligence, Surveillance and Reconnaissance
ISX	Information Superiority Experiment
IT	Information Technology
ITEF	Internet Engineering task force
ITSEC	Information Technology Security Evaluation Criteria
IW	Information Warfare
I&W	Indications and Warning
IWG	Interagency Working Group
JCS	Joint Chiefs of Staff
JIER	Joint Information Exchange Requirements
JMRR	Joint Military Readiness Review
JOA	Joint Operational Architecture
JPO	Joint Program Office
JPO-STC	Joint Program Office for Special Technology Countermeasures
JROC	Joint Requirements Oversight Council
JRVIO	Joint Reserve Virtual Information Operations
JSA	Joint System Architecture
JSMB	Joint Space Management Board
JSTARS	Joint Surveillance Target Attack Radar System
JTA	Joint Technical Architecture
JTF	Joint task force
JTF-CND	Joint Task Force for Computer Network Defense
JTS	Joint Training System
JTIDS	Joint Tactical Information Distribution System
JTRS	Joint Tactical Radio System
JV2010	Joint Vision 2010
JV2020	Joint Vision 2020
JWAC	Joint Warfare Analysis Center
JWRAC	Joint Web Risk Assessment Cell
JWICS	Joint Worldwide Intelligence Communications System

KMI	Key Management Infrastructure
LAN	Local Area Networks
LDAP	Lite Directory Access Protocol
LEO	Low Earth Orbiting
LIWA	Land Information Warfare Activity
LMDS	Local Multipoint Distribution System
LTM	Last Tactical Mile
M&S	Modeling and Simulation
MCEB	Military Communications and Electronics Board
MEO	Mid Earth Orbiting
MEII	Minimum Essential Information Infrastructure
MIB	Management Information Byte
MIB	Military Intelligence Board
MilDeps	Military Departments
MilSatCom	Military Satellite Communications
MILSPEC	Military Specification
MISSI	Multi-Level Information System Security Initiative
MMDS	Multichannel Multipoint Distribution System
MOS	Military Operations Specialties
MOU	Memorandum of Understanding
MRC	Major Regional Conflict
MSC	Mobile Switching Center
MTW	Major Theaters of War
MUOS	Mobile Users Objective System
NAD	Naval Architecture Database
NAN	Navy After Next
NATO	North American Treaty Organization
NCS	National Communications System
NCW	Network Centric Warfare
NED	Network Encryption Devices
NETWARS	Network Warfare Simulation
NGI	Next Generation Internet
NIAC	National Incident Analysis Cell
NIAP	National Information Assurance Partnership
NII	National Information Infrastructure

NIPC	National Infrastructure Protection Center
NIPRNET	Non Secure Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NRE	Non-Recurring Engineering
NRO	National Reconnaissance Office
NSA	National Security Agency
NSB	Naval Studies Board
NSC	National Security Council
NSIRC	National Security Incident Response Center
NSF	National Science Foundation
NSSN	Next Subsurface Nuclear (submarine)
NSTISSC	National Security Telecommunications and Information Systems Security Committee
NVLAP	National Voluntary Laboratory Accreditation Program
O&M	Operation and Maintenance
OA	Operational Architecture
OASD/C3I	Office of the Assistant Secretary of Defense, Command, Control, Communications & Intelligence
OBE	Overcome by Events
OMFTS	Operational Maneuver from the Sea
OPM	Office of Personnel Management
OODA	Observe, Orient, Decide, Act
OPFAC	Operations Facility
OPNET	Operations Network
OSD	Office of the Secretary of Defense
OT&E	Operations, Test and Evaluation
PCS	Personal Communications Systems
PDA	Personal Digital Assistants
PDD	Presidential Decision Directive
PEO	Program Executive Office
PFF	Packet Filtering Firewall
PGP	Pretty Good Privacy
PKE	Public Key Encryption
PKI	Public Key Infrastructure
PKIX WG	Public Key Infrastructure Working Group
PM	Program Manager
POM	Program Objective Memorandum

PRD	Presidential Review Directive
PSTN	Public Switched Telecommunications Networks
QoS	Quality-of-service
R&D	Research and Development
RAPIDS	Real-Time Automated Personnel Identification System
RC	Reserve Component
RFC 822	Response Force Commander
ROE	Rules of engagement
RSTA	Reconnaissance Surveillance and Target Acquisition
RSVP	Resource Reservation Protocol
RTP	Real-Time Protocol
S&T	Science and Technology
SA	System Architecture
SABI	Secret and Below Interoperability
SAM	Surface to Air Missile
SatCom	Satellite Communications
S-BGP	Secure Boundary Gateway Protocol
SBU	Sensitive But Unclassified
SCP	Service Control Points
SDR	Surrogate Digital Radio
SET	Secure Electronic Transactions
SecDef	Secretary of Defense
SINCGARS	Single Channel Ground and Airborne Radio System
SIPRNET	Secure Internet Protocol Router Network
SLA	Service Level Agreements
SLEP	Service Life Enhancement Program
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPAWAR	Space and Naval Warfare Systems Command
SPKI	Secure Public Key Infrastructure
SSG	Senior Steering Group
SSH	Secure Shell
SSL	Secure Socket Layer
SSNMP	Secure Simple Network Management Protocol
SSP	Service Switching Point

STE	Secure Telephone Equipment
STEP	Standardized Tactical Entry Point
STP	Signal Transfer Points
SUO	Small Unit Operations
SYN	Synchronization
TA	Technical Architecture
TADIL J	Tactical digital information link, type J (JTIDS)
TAFIM	Technical Architecture Framework for Information Management
TBC	Tactical Battlefield Communications
TCSEC	Trusted Computer System Evaluation Criteria
TCP/IP	Transmission Control Protocol/Internet Protocol
TDC	Theater Deployable Communications
TF	Technical Architecture Framework
TIARA	Tactical Intelligence and Related Activities
TLS	Transport Layer Security
TOR	Terms of Reference
TPFDL	Time-Phased Force and Deployment List
TRANSEC	Transmission Security
TSABI	Top Secret and Below Interoperability
TTP	Tactics Techniques and Procedures
UAV	Unmanned Aerial Vehicle
UFO	UHF Follow-On Satellite System
UHF	Ultra High Frequency
UL	Underwriters Laboratory
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology and Logistics
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
USJFCOM	United States Joint Forces Command
USSPACECOM	U.S. Space Command
VCJCS	Vice Chairman Joint Chiefs of Staff
VLR	Visitor Location Register
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VTC	Video Teleconferencing
WAN	Wide Area Network
WG	Working Group

WIN-T	Warfighter Information Network-Tactical
WMD	Weapon of Mass Destruction
XML	Extensible Markup Language