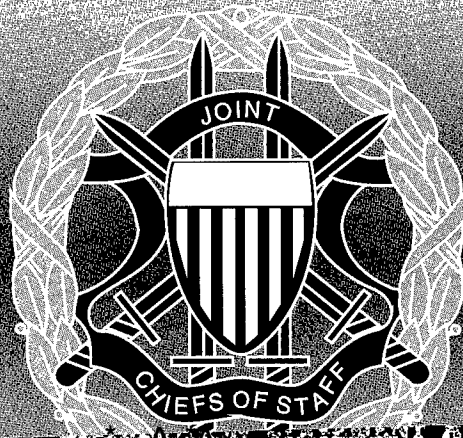


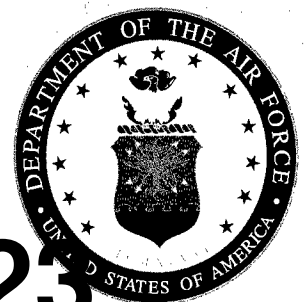


# INFORMATION REREWA



Approved for public release  
Distribution Unlimited

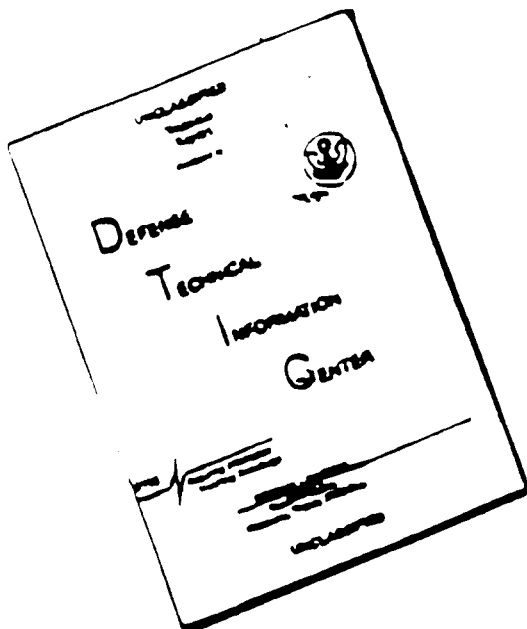
## A Strategy for Peace.... The Decisive Edge in War



1998/20 023

023

# DISCLAIMER NOTICE



THIS DOCUMENT IS BEST  
QUALITY AVAILABLE COPY  
FURNISHED TO DTIC CONTAINED  
A SIGNIFICANT NUMBER OF  
PAGES WHICH DO NOT  
REPRODUCE LEGIBLY.

*"This brochure marks yet another aspect of the tremendous progress being made in Information Warfare (IW). Over the past two years, we have made great strides in raising awareness within DOD, the rest of Government, and industry. With that has come a conviction to act, and within the Joint Staff, we have formulated an IW implementation strategy designed to translate vision into practical processes and capabilities supporting joint warfighting.*

*We developed this brochure to outline basic IW concepts and summarize ongoing initiatives implementing those concepts.*

*Your continued support is needed to develop and support these initiatives and those yet on the horizon."*

PETER PAGE

Lieutenant General, USMC

Director for Operations

ARTHUR K. GEBROWSKI

Vice Admiral, USN

Director for C4 Systems

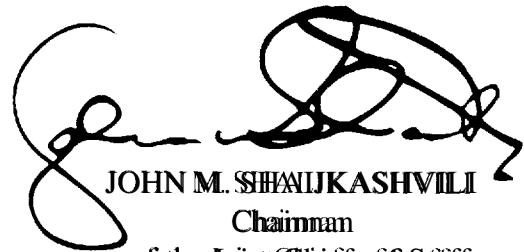
# From the Chairman



Information Warfare (IW) has emerged as a key joint warfighting mission area. The explosive proliferation of information-based technologies significantly impacts warfighting across all phases, the range of military operations and all levels of war.

Our reliance on technology creates dependencies and vulnerabilities throughout our global basing and information support networks and generates requirements for defensive IW capabilities. However, the same technologies also create vulnerabilities for our adversaries that can be exploited using offensive IW capabilities. We are fully developing and integrating IW offers enormous potential to support our warfighters.

A comprehensive IW approach is essential to ensure warfighters have the tools to exploit adversary vulnerabilities while ensuring intelligence is timely, accurate, and relevant information where and when needed. The Joint Staff developed an IW vision and strategy to address our most urgent needs. The concepts outlined in this brochure provide a common framework to guide our continuing and expanding efforts in this mission area.



JOHN M. SHALIKASHVILI  
Chairman  
of the Joint Chiefs of Staff

ERIC QUALITY INSPECTOR

# The Compelling Need

## Relevance to the Warfighter

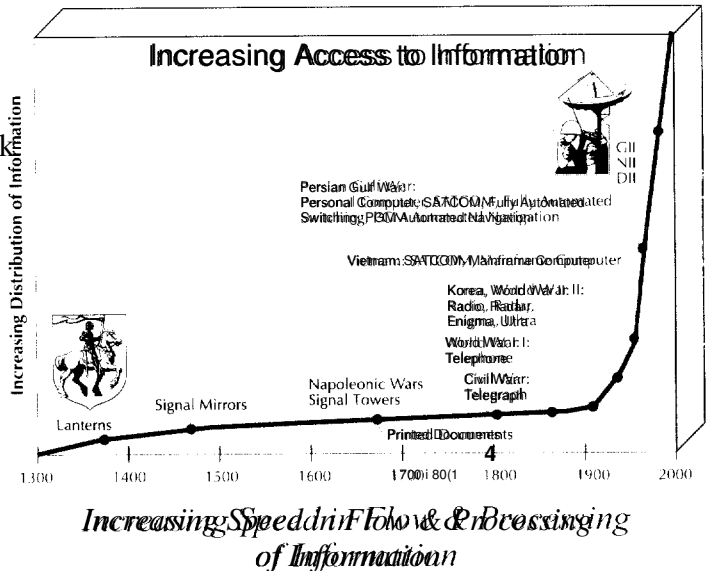
Some potential adversaries are rapidly exploiting information and information system technologies such as telecommunications, automated data processing, sophisticated decision aids, remote sensors, and other related systems. The spectrum of applicable technologies ranges from established radio frequency, microwave, satellite, coaxial, and fiber optic transmission systems to new generations of digital and advanced personal communications systems. The availability and relatively low cost of these technologies in global markets increases the likelihood that they will be employed by potential adversaries in advanced command and control (C<sup>2</sup>) and information systems, as components of advanced weapon systems, and as offensive W<sup>2</sup> capabilities. A National-level infrastructure, including economic, industrial, and transportation systems that support national and military warfighting objectives, are also becoming increasingly dependent on automated control and information systems for their operation.

The information age here rapidly advancing information based technologies and increasingly competitive global environment take thrust information into great stage in society, government, and warfare in the 21st Century. Information and information based technologies are pervasive and impact every facet of warfighting from planning, deployment, and sustainment processes to the plethora of weapon systems employed by joint task force (JTF) commanders. **Timely, accurate and relevant information is absolutely essential to warfighting** as a large force structure gives way to smaller, highly trained and technologically equipped forces. **Although the nature of war remains unchanged, its character is now in constant transition.**

## Use Breeds Dependence

Information itself is becoming a strategic resource vital to national security. The availability extends to warfighters at all levels, increasingly complex information systems are being integrated into traditional disciplines such as mobility, logistics, and C<sup>2</sup>. Systems are being developed with inherent vulnerabilities that are many times the unavoidable consequences of enhanced functionality, efficiency, and convenience to users. The complexities and vulnerabilities of these information systems are often disguised by user friendly software. The low costs associated with such technology makes it efficient and cost effective to extend the capabilities (and vulnerabilities) to an unprecedented number of users. Heretofore access to, and use of, these information systems enhances warfighting. However, these extended capabilities induce dependence and that dependence creates vulnerabilities. These vulnerabilities are a double-edged sword—on one hand representing areas the Department of Defense (DOD) must protect while on the other hand creating new opportunities that can be exploited against the adversary.

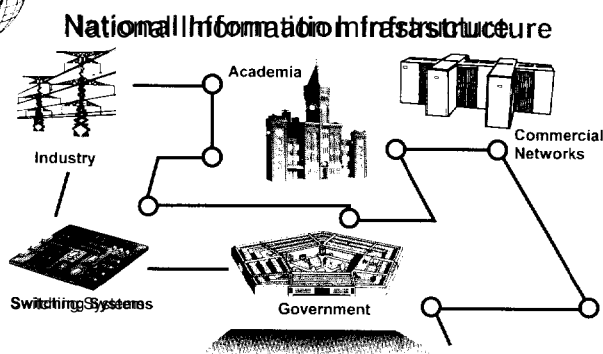
IJSSE  
BRHITS  
DHPLNDFNCL-...  
DEPENDENCE  
CRIM.S.S  
VULNERABILITY



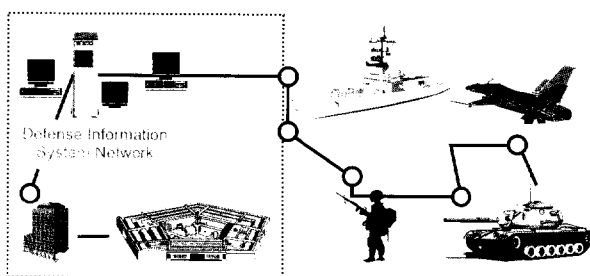
Operation DESERT STORM highlighted the increasing dependence of the US Armed Forces on information-based technologies and their powerful advantages. However, the impact was only the tip of a much larger and more complex reality of the evolving information age. Military operations and the precise application of decisive combat power are critically dependent on many simultaneous and integrated tasks that in turn depend on information and information systems, especially those tasks associated with critical command and control processes. Some of these tasks include:

- Conducting strategic deployment.
- Sustaining theater forces.
- Ensuring force protection, both in garrison and in forward deployed areas.
- Preserving theater strategic command and control.
- Developing strategic and tactical intelligence.

Many vital warfighting tasks are dependent upon information and information-based



**Defense Information Infrastructure**



**Information Warfare**

IW focuses on a target set. IW is an amalgam of warfighting capabilities integrated into a CINC's theater campaign strategy and applied across the range of military operations and all levels of war.

technologies. Warfighting information systems are linked through supporting infrastructure, thus exposed to attacks by a broad range of adversaries whose motives may be difficult to measure. Therefore, the difficulty of defending systems and processes upon which our warfighting capability depends is increasing, and their defense is absolutely essential.

The continuing growth of information systems and technologies offers a nearly unlimited potential for exploiting the power of information in joint warfighting. Because there are no fixed boundaries in the information environment, the labels placed on information systems and associated networks may be misleading. Open and interconnected systems are coalescing into rapidly expanding global information infrastructure that has replaced the US National Information Infrastructure (NI) and the Defense Information Infrastructure (DII).

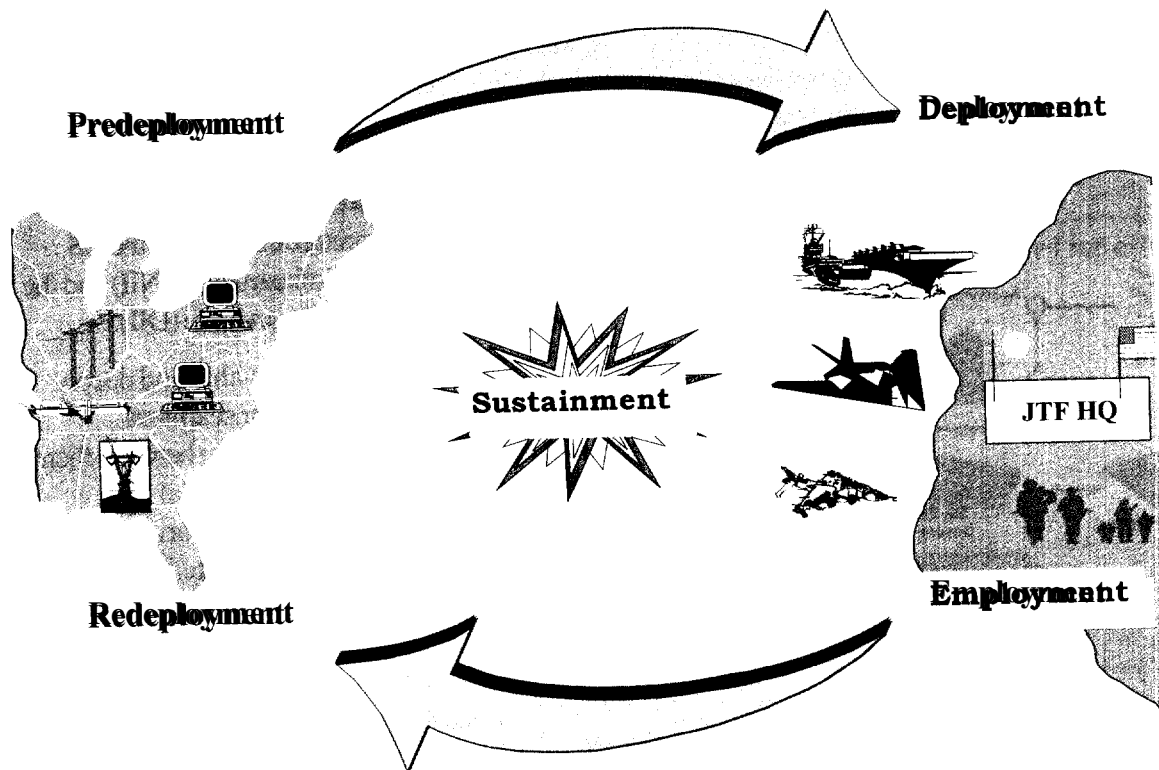
The DII is embedded within and deeply integrated into the NI. This seamless relationship makes distinguishing between them impossible. The two share terrestrial telecommunication networks, a variety of information databases and satellite communications networks. These infrastructures cannot be geographically separated or administratively separated by national boundaries.

## Reach-Back Support for the Warfighter

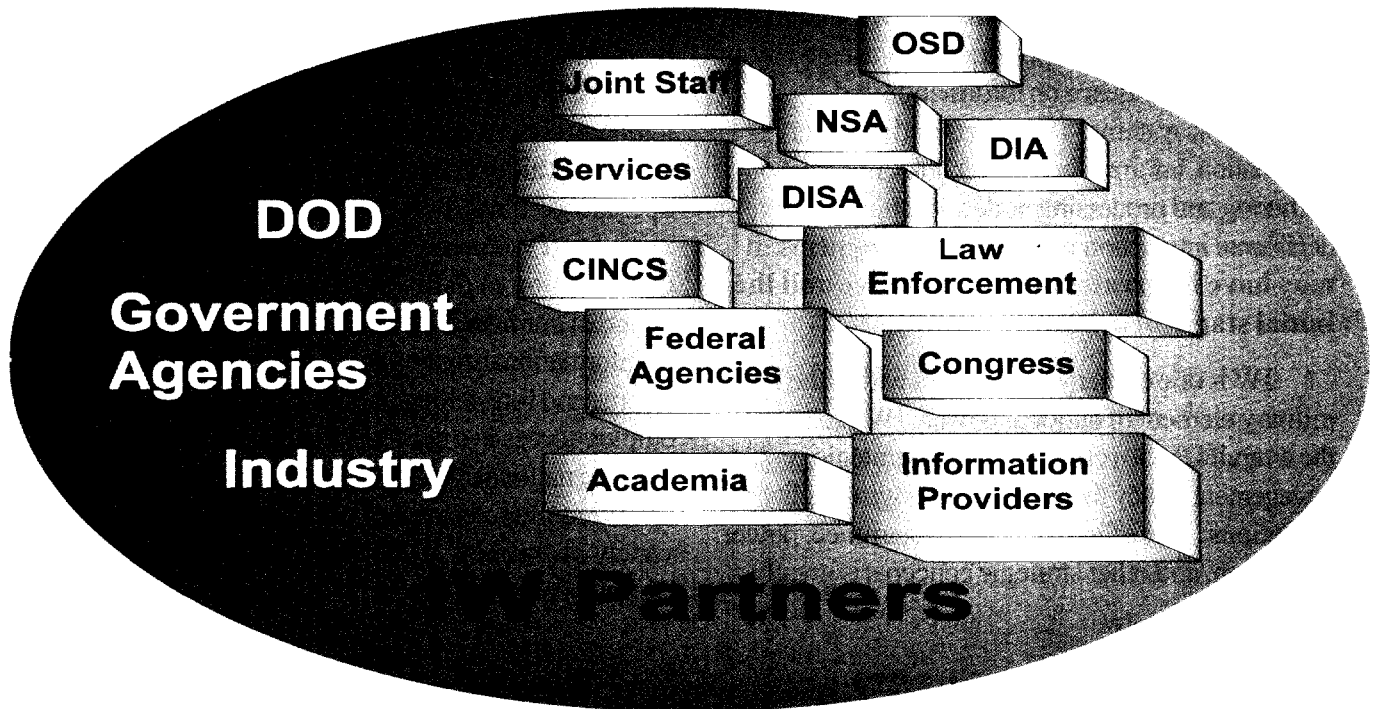
The successful conduct of warfare in the information age requires access to information available outside the theater of operations. Information infrastructure is no longer parallel traditional command lines and warfighters need frequent, instant and reliable access to information at locations in CONUS as well as in theater. For example, mobility and sustainment of forces are highly dependent on commercial "reach back" infrastructures that include international telecommunications, the public switched network, transportation systems, and commercial electric power grids. Warfighters require secure, wide area, real-time, detailed imagery from national sources, intelligence, logistics,

and support data from diverse locations. The technical nature of these information infrastructures inhibits a commander's ability to control the flow of information or dynamically manage available information and telecommunications resources. To support offensive operations, warfighters may reach back to employ information attack capabilities and techniques that provide an information advantage in the area of responsibility.

Providing capabilities to support military operations require the expansion of our information infrastructure beyond the established peacetime information environment. Warfighters must have assurance that this expanded infrastructure can attain the level of protection required to enable mission



*IW impacts all phases, the range of military operations, and all levels of a war*



*A teamed approach is essential to develop a comprehensive IW strategy*

## Information Warfare Basics

success. The authority to implement this is any other level of protection of the NII is outside of the Department of Defense and government. **It must assist in demonstrating to service providers the compelling need for a collaborative, teamed approach in crafting solutions not just to support the Department of Defense and to protect our national security, but to protect their own proprietary interests as well.**

Our dependence on information and information systems and the exposure of our vulnerabilities to a full range of threats from computer hackers through criminals, stalkers, and terrorists to nation states, have brought to focus and compelling relevance to the emerging discipline of IW. Its unique characteristics set in motion revolutionary capabilities that will enhance and support war fighting into the next century.

IW involves actions taken to achieve information superiority by affecting adversary information, information-based processes, information systems, and computer-based networks while defending one's own information, information-based processes, information systems, and computer-based networks. **IW applies across all phases, the range of military operations, and at every level of warfare.** Defensive IW activities are conducted on a continuous basis in both peacetime and war and are an inherent part of force protection. Offensive IW capabilities may be employed in a variety of circumstances across the range of military operations. IW operations may involve complex legal and policy issues requiring careful review and data at the level of operational and approval.



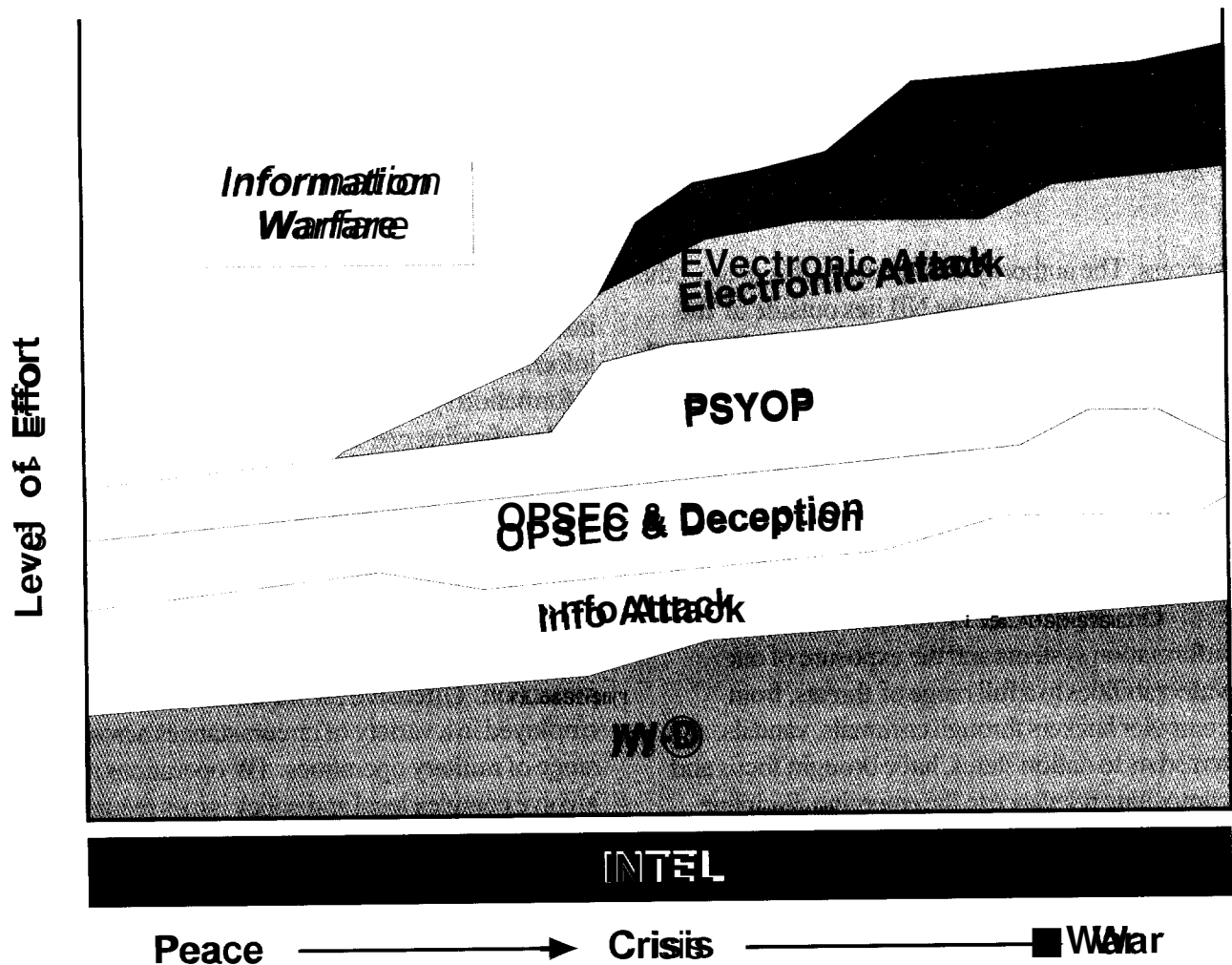
# A strategy for peace...

As an integrating strategy, IW focuses on the vulnerabilities and opportunities presented by an increasing dependence on information and information systems. IW targets and protects information into information assets and links for information gathering and processing nodes, and human decisional interaction with information systems. It may have its greatest impact in peace and the initial stages of crisis.

IW is one of many capabilities within the US military element of national power. IW can support the overall US Government (USG) strategic engagement policy throughout the range of military operations. The effectiveness of deterrence, power projection, and other strategic concepts is greatly

affected by the ability of the USG to influence the perceptions and decision making of others. In times of crisis, IW can help deter a crisis or from initiating a crisis and deter the interests of the USG on its allies on the broad and of friendly military operations. If carefully conceived, coordinated and executed, IW can make an important contribution to deterring crises, during the period of confrontation and enhancing the impact of informational, diplomatic, economic, and military efforts; and forestalling or eliminating the need to employ force in a combat situation. Thus, IW at both the national strategic and theater strategic levels requires close coordination among a wide variety of elements of the USG, including the Department of Defense.

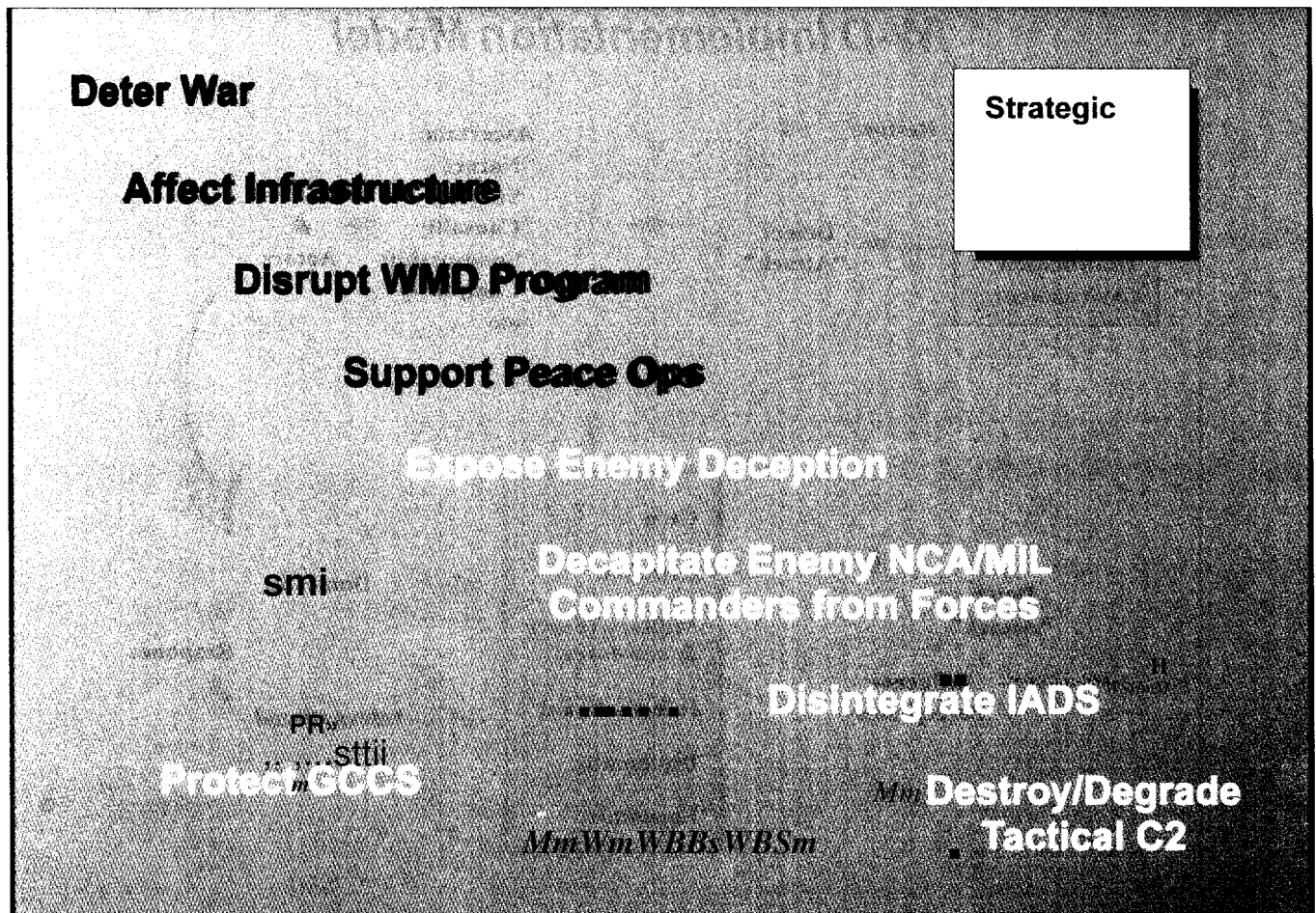
## Engagement Timeline



IW can be waged in wartime within and beyond the traditional military battlefield. As a subset of IW, command and control warfare (C2W) is an application of IW in military operations that specifically attacks and defeats the C2 target set. However, the capabilities and disciplines employed in C2W (psychological operations (PSYOP), deception, operations security, and electronic warfare) as well as other less traditional bases of focus in information systems can be employed to achieve IW objectives that are outside the C2 target set.

There are both offensive and defensive aspects of IW. A common link between the two aspects is the target set in which IW - information and information systems must be used. DOD can use IW to affect the information and information systems of an adversary, so to can an adversary target DOD's information and information systems. Understanding the basic elements and the potential of offensive and defensive IW prepares us to grasp the integrated IW strategy currently being developed within the Department of Defense. The remainder of this brochure will introduce the concepts and ongoing initiatives in the emerging discipline of IW.

## Spectrum of Information Warfare Objectives



# Defining the IW Vision

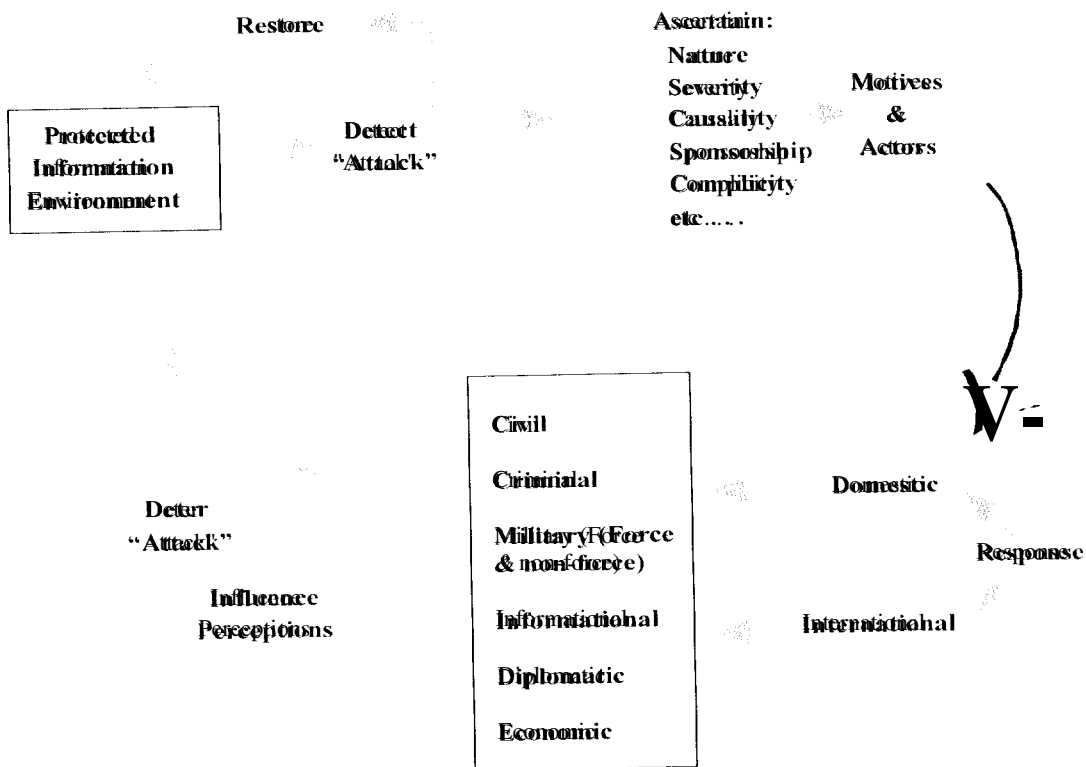
*"The threat to our military and commercial information systems poses a significant risk to national security and is being addressed."*  
 1996 National Security Strategy 1996 National Security Strategy

## Organizing Defensive IW (IW-D)

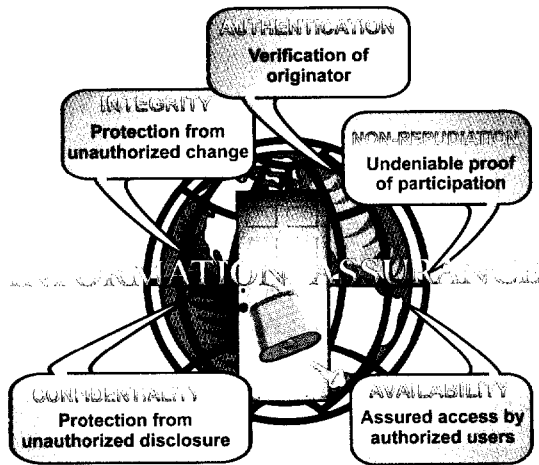
IW-D actions must be carefully considered, integrated at all levels of war and applied across the range of military operations. This requires IW-D to be organized as a system headed together by policy, doctrine, technology capability assessments, education, training, exercises, and a mutually supporting national organizational infrastructure. Along the way, the IW-D system can be integrated

into the larger system of war fighting with the overall objective of capturing the latent potential of IW to dramatically enhance our fighting capability. Collaborative efforts with the Department of Defense and elsewhere in the Federal Government are moving rapidly to organize and implement IW-D as a system.

## IW-D Implementation Model



*A comprehensive model is available to all levels of war*



### The IW-D System

Organizing IW-D as a system begins with a broad vision implemented by collaborative efforts that move the vision and concepts from the abstract into a focused set of questions and answers on specific aspects of policy and standards. The five critical components that should be included in any attempt to implement an IW-D system are integrity, authentication, non repudiation, availability and confidentiality. **IW-D implementation is designed with an objective of information assurance to protect access to timely accurate and relevant information whenever and wherever needed.** At the national level, the Department of Defense and other elements of government are working with industry to ultimately build the means to appropriately protect and defend the NII and DDII, using a managed-risk approach. The true extent and implications of IW-D are only visible in a top level implementation model. This model is scalable, as it is applicable at all levels of war and across the range of military operations.

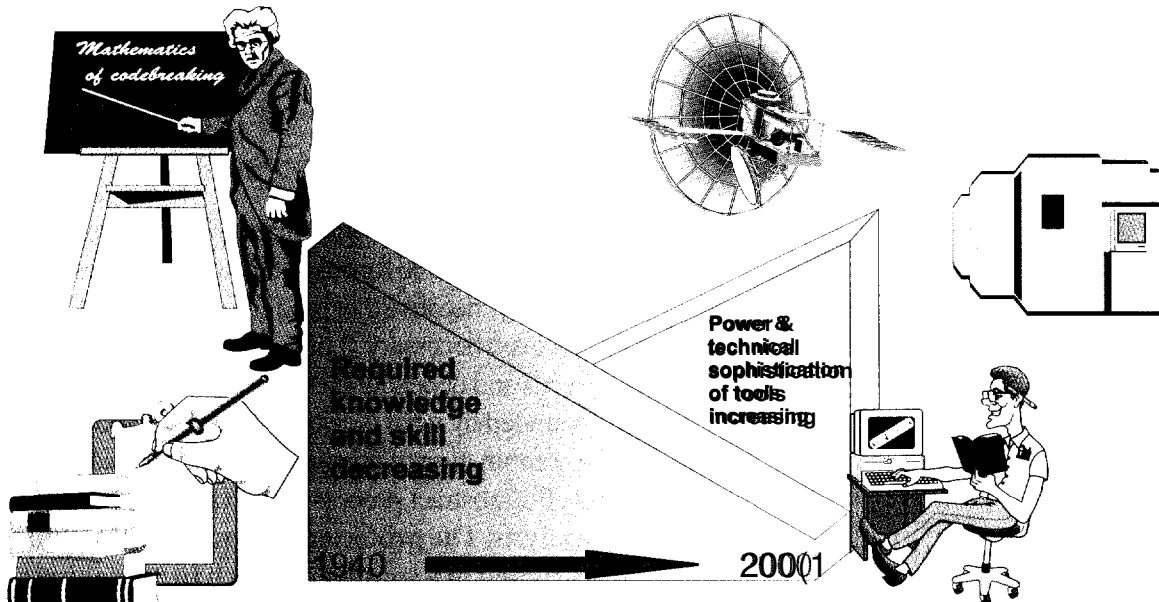
### Elements of the Model

The model begins with a defined and appropriately protected and defended information environment. Interacting with the protected environment is a process to identify threats, attacks, or other degrading conditions and to disseminate warnings when and if these occur. Attack detection initiates both restoration and response processes.

### The Protected Information Environment

The protected information environment is not an impenetrable fortress that guarantees absolute security, because that is neither practical, affordable, nor even necessary. The focus is on defining real needs and dependencies. The environment is bounded by what is critical to national security. It is a combination of physical systems and places, as well as abstract processes such as intelligence analysis. **The protected information environment is rooted in a sound approach to managing risk.** Risk management processes include consideration of information needs, the value of information that may be compromised or lost if the protected information environment is breached (loss of access control), system vulnerabilities, threats posed by potential adversaries and natural phenomena, and resources available for protection and defense. In addition, **the value of information changes in each phase of military operations and must be considered in the risk management process.** The protected information environment not only provides the degree of protection commensurate with the value of its contents, but also ensures mechanisms are in place to respond to a broad range of attacks.





**The required technical sophistication of the average intruder has dramatically decreased**

**Threat**

Articulation of the threat must be comprehensive—overstating the threat leads to unnecessary levels of protection, expense, and effort. Conversely, understating the threat leads to overconfidence in system reliability and resilience under adverse conditions. This simplification underscores the vital importance of a clearly defined and articulated threat. A National Intelligence organization's continued characterization of the evolving threat—adynamic mission that adjust just to changing threat conditions.

To get at the essence of the threat requires an understanding of three elements:

- Identities and intentions of possible attackers.
- Possible attack techniques and methods.
- Potential targets, extending from the strategic to the tactical levels.

**Indications and Warning**

Threat knowledge is a input to processes that analyze attack indicators and disseminate warnings to persons, organizations, and processes that are

determined to be at risk or require reawakening indications to assist them in other decision-making processes. A comprehensive WIndications and warning (I&W) regime will require a policy structure to establish authorities, roles, and responsibilities across local, state, and national jurisdictions. Functionally, I&W for W will require the closest cooperation between law enforcement, the Intelligence Community, and private enterprise. In this environment, tripping attacks occur at speeds exceeding guided human capacity to detect, analyze, and disseminate warnings. I&W will not occur without a robust collaborative government/industry effort.

**Attack Detection**

Defensive efforts to detect and identify adversary activities require collaboration among government, industry, and society. A critical element of the detection process is identifying indicators of adversary activity, analysis of those indicators, and dissemination of warnings. This process requires a knowledge of the threat capability information from various sources including law enforcement, the Intelligence

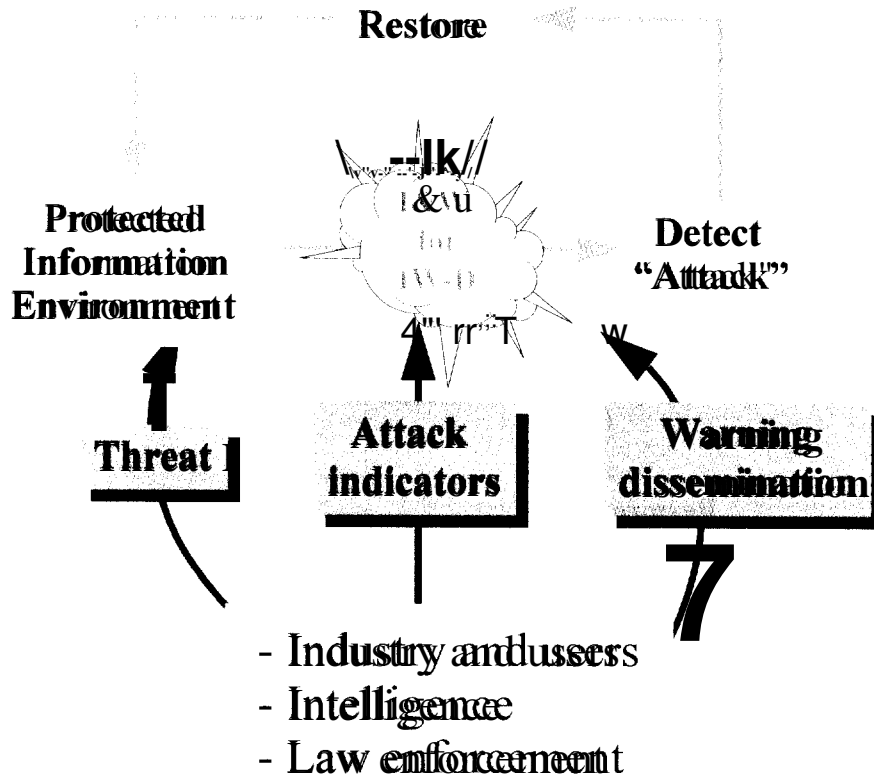
Community, system providers, and users. Finally, automated attack detection capabilities are necessary, given what may be extremely short timelines from initiation to the culmination of attacks. Defending against an attack, whether against a JTK's intelligence data base or against an automated component of the commercial national power grid, is predicated on how well the intelligence threat and associated indications and warning processes function and on the agility of systems providers, users, and administrators in implementing protective countermeasures.

The potential subtlety of early indications of adversary prestrike reconnaissance and exploitation techniques, as well as the speed with which a powerful attack can proceed from initiation to culmination, mandates a need for automated intrusion detection capabilities. **These capabilities**

**must automatically detect system intrusions or aberrations and instantly generate alerts.** Additionally, automatic threat mitigation that limits the extent of damage or spread of attack must be self-initiating.

## Restoration

Attack detection mechanisms trigger reactive processes. The first of these processes is restoration. **Restoration relies on a pre-established understanding of the desired levels and conditions of system performance and functionality.** Priorities may be then derived for restoring access to and availability of essential information, as well as detect when anomalous conditions have degraded systems and processes below their desired steady-state performance thresholds. Procedures for restoration of



The key elements of a comprehensive indications and warning planning process

# A strategy for peace...

telecommunications exist for the Department of Defense and the National Communications System (NCS). The NCS facilitates executive and technical expert dialogues between industry and the NCSA through the National Security Telecommunications Advisory Committee (NSTAC). In the information age, the NSTAC continues to play a vital role in the Nation's total IWED posture.

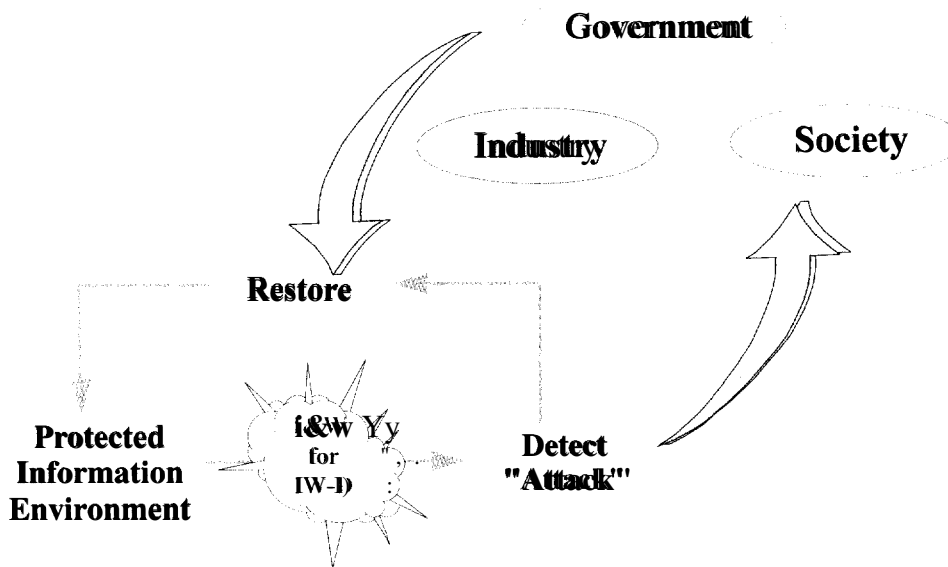
## Response Process - Motives and Actors

Attack detection mechanisms serve to trigger the response process. If they identify motives and actors, this is the cornerstone of effective and properly focused responses, linking the analytic results of the I&W process to national level decision makers.

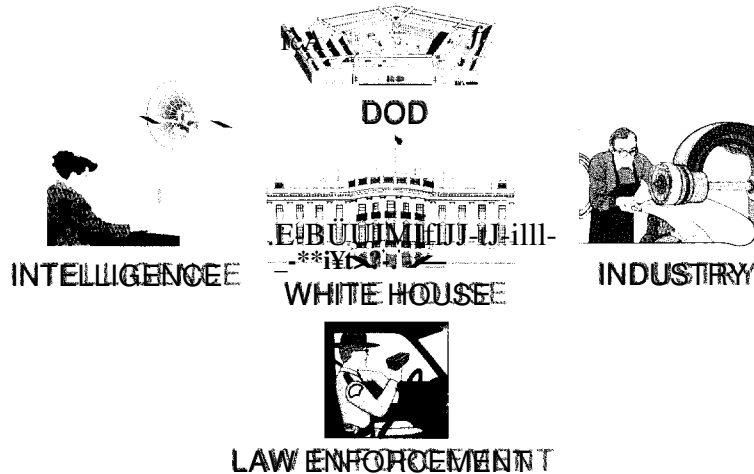
The true nature of motives and actors engaged in attacks and ISN information systems, processes of national interests, whether domestic or international, permits a deeper understanding of the

jurisdictional environment in the response process. In the present IW environment, the clear identification of motives and actors will lead to a simplified set of automatic response processes and options. This is true because the search between civil and military roles in national security is blurred in the case of IWED. An attack against a commercial system that manifests itself in DOD networks raises legal and public issues, which highlight the need for increased interagency coordination and joint civil-military response operations. Through all of this, the limits of the proper and legitimate role of government to provide for the economic defense must be recognized and respected, ensuring no violation of personal freedoms and rights of privacy.

The effectiveness of the response process is dependent upon efficient integration of attack detection and analysis capabilities. **Timely response is essential to influence adversary perceptions, establish user confidence, and maintain public support.**



*Attack detection and restoration requires a team effort of participants by a combination*



*Effective response requires collaboration, integration and efficiency efforts*

Attacks themselves do not inherently point to the motives and actors in an unambiguous way. Apparently similar events or indications may have completely different causes, sponsorship, complicity, and severity. The different implications for national security point to the wisdom of providing decision makers with the best and most comprehensive information available on which to base decisions regarding response options. As such, the need for full cooperation between C4 technology and intelligence processes and capabilities is clear.

### An Assembled IWD System

Warfighters depend upon information to plan operations, deploy forces, and execute missions. Additionally, advanced information technologies have significantly altered these processes. Complex information systems support powerful infrastructures that dramatically enhance warfighter capabilities; however, increasing dependence upon these rapidly evolving technologies make joint forces more vulnerable.

IW-D is a comprehensive strategy being implemented to protect and defend information and information systems. When combined with offensive

IW, the net result will be the opportunity to use IW to exploit situations and to win.

### Offensive IW (IW-O)

As with the IW-D system described above, IW-O capabilities are employed at every level of warfare and across the range of military operations. The employment of offensive IW capabilities to affect an adversary's information and information systems can yield a tremendous advantage to US military forces during times of crisis and conflict. As a result, **combatant commanders must carefully consider the potential of IW for deterring and rolling back crisis.**

When viewed as an integrating strategy, IW weaves together related disciplines and capabilities to meet and satisfy a stated objective. Offensive IW applies traditional perception management disciplines such as PSYOP and information system attack to produce a synergistic effect against the remaining elements of an adversary's information systems, information transfer links, and information nodes.



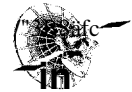
## Examples of I/W Targets

### Leadership



- Key Personnel
- ADP Support
- Strategic Comms
- Power Base

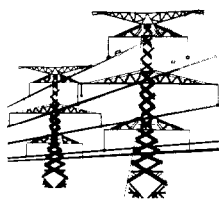
### Military Infrastructure



- Commanders
- C2 Comm Links
- C2 Nodes
- Troops
- Intel Collectors



### Civil Infrastructure



- Comms (Links/Nodes)
- Industry
- Financial
- Populace

### Weapons Systems

- Planes
- Ships
- Artillery
- PGMs
- Air Defense



*Attack the information systems and providers that support these target sets*

### IW-Dir Military Operations Other Than War (MOOTW)

Offensive IW related plans with their associated capabilities may be employed in peacetime to deter a crisis, control crisis escalation, project power, or promote peace. The employment of offensive IW capabilities in these circumstances may require NSA approval with support, coordination, deconfliction, cooperation, and/or participation by other USG departments and agencies. Although IW-OC capabilities can be employed to undermine an adversary's regime, the primary focus of IW efforts in MOOTW should be to

preserve the peace, deter escalation of a conflict, and prepare the battlefield so that if a crisis is escalated to conflict, the US military can effectively employ IW-OC capabilities in an wartime scenario. Examples of other potential peacetime applications of offensive IW include the employment of IW capabilities to disrupt drug cartel communications lines in support of drug interdiction efforts and conducting a PSYOP campaign against a belligerent's potential allies with the goal of severing external sources of military, economic, and political support.

## Wartime Employment of IW-0

Beyond the threshold of crisis, IW can be a critical force enabler for the joint warfighter. In addition to protecting information systems vital to the US military, **employment of IW-0 capabilities can affect every aspect of an adversary's decision cycle by impacting its information centers of gravity.** Many of the activities associated with wartime employment of IW-0 capabilities focus on the military command and control target set. However, there are many other important information system targets for the warfighter to focus on to fully realize the power of IW in wartime.

One type of information attack could be the application of IW capabilities against an adversary's automated information systems to disrupt production of critical war supporting industries. Another application might be the use of IW capabilities to sever an adversary's communications networks from the external military, economic, and political support-base.

## Deterrence

There are two aspects of deterrence associated with IW. The first is the **deterrent effect IW-0 capabilities can have on a potential adversary during peace and crisis.** As new IW capabilities continue to emerge, their potential usefulness to deter technology-dependent adversaries must be leveraged as much as possible.

The second, more specific aspect is the **deterrence of an information-based attack against the United States.** Detering IW attack requires the application of both offensive and defensive capabilities. Strong IW defenses help to discourage casual threats, thereby narrowing the playing field to a more distinct set of actors. When faced with an information-based attack, the ability of

the Nation to respond quickly, effectively, and decisively will influence perceptions and assist in deterring future attack. In this regard, information joins economic, political, diplomatic, legal, and military power as an element of total national strength. The preservation of information contributes to the total power of our Nation and society. The result is a new form of strategic deterrence for the information age.

## The Vision Comes to Closure

National leaders are able to choose from a broad range of options that are flexible and combinable to achieve the desired effect in most circumstances. **The IW vision does not demonstrate a nation that is invulnerable but rather one that is vigilant, decisive, and prepared to respond to any threat, foreign or domestic.** That reality contributes to strategic deterrence in a context appropriate to the information age.

The IW vision...  
supporting vital strategic  
deterrence  
til the Information Age

# Implementing the Joint Vision

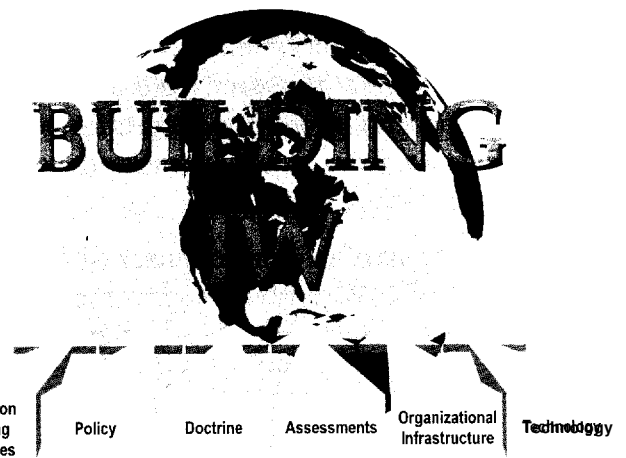
"We must have Information Superiority. Information Superiority will require both offensive and defensive information warfare."

Joint Vision 2010

## Taking It to the Troops

A common focus is essential to ensure a credible IW vision becomes a reality. The three principles of the Joint Staffs implementation vision are:

- Reduce the opportunities presented to potential adversaries by educating, training, and increasing the awareness of warriors to vulnerabilities and protective measures.
- Improve information attack capabilities and measures to protect against and detect attack on information and information systems by pursuing emerging technological capabilities and the synergy created by integrated defense-in-depth solutions.
- Build the necessary relationships, within government and throughout the Nation, to secure the information needs of all constituents. Seal those arrangements in law and policy, resulting in reconstituted national deterrence to preserve peace, security, and stability. Efforts are underway to integrate IW into all



aspects of joint warfare. The Joint Staff, in cooperation with the Services and Defense agencies, is focusing on a common approach toward operationalizing JW. Efforts in six major areas are coming together to support the warfighter. They include:

- Education, training, and exercises
- Policy
- Doctrine
- Assessments
- Organizational infrastructure
- Technology

Education, Training and Exercises



User Training • System Administration  
Access Controls • Emergency Response  
Multilevel Security

**Education, training and exercises offer the greatest return on investment.** High level military education at the National Defense University and Service professional military education institutions focus on the study of IW concepts, policy issues, doctrine integration, and the role of IW throughout the range of military operations and all levels of war. Additionally, the DOD Inter-Service Training Review (Organizational Initiative) for Joint IW Training (DIITIR) initiated 111 courses for DOD personnel. These courses range from senior-level awareness to technical training for systems administrators.

**The DIITIR is a great success story that epitomizes jointness.** Additional courses are forthcoming that will continue to generate and focus IW study throughout the joint environment.

Information systems incident reports continue to reveal that most intrusions result from a lack of understanding and improper implementation of security measures by information users. Awareness and training modules are being inserted into a broad range of officer, enlisted and civilian curriculum that explain vulnerabilities inherent in information systems, describe potential adversary threats, and educate people in proper system use.

**Training for system and network administrators to identify and mitigate vulnerabilities is another investment yielding high dividends.** Industry places a premium on and commits a great deal of resources to acquire and train specialists to administer and defend information systems security policies. The Department of Defense should follow suit in this area.

At the organizational level, the Joint Staff is accelerating the integration of IW into joint exercises. Demonstration of IW concepts and capabilities in CINC-sponsored exercises will help planners and users better integrate IW into operations. **Lessons learned from cooperating**

**IW into joint exercises also will help accelerate and shape policy and doctrine.**

## IW Policy

The Department of Defense is participating in interagency discussions that focuses on IW policy issues and has created internal executive and working-level forums to identify, develop, and implement policies and concepts. Across a broad range of issues, IW efforts are examining DOD's role, the role of government in society, and the potential impact of emerging technologies and other factors. A Defense Science Board study is also helping to fuse national-level and DOD efforts in broad areas.

Given these considerations, appropriate policy positions and designation of responsibilities are being thoughtfully considered and reflected in DOD and CICS policy documents. **The Joint Staff is participating in the revision of existing policy in addition to developing new IW instructions where needed.** Consistent with those efforts, Chairman of the Joint Chiefs of Staff

### Defense Science Board Objectives

- Identifying the information users of national interest.
- Determining the scope of national information interests to be defended.
- Characterizing the proposed processes, and operational arrangements required to establish a comprehensive national defense-in-depth strategy.
- Identifying the reasonable roles of government and the private sector in creating, managing, and operating a national IW-D capability.

# A strategy for peace...

Instruction (CJCSI) 3210.01, established "Joint IW Policy" to support warfighting. Also, CJCSI 6510.01 A, established "Defensive Information Warfare Implementation," that focuses on key areas of protecting and defending information and information systems.

## IW Doctrine

The Joint Staff is the lead agent for developing joint doctrine for information warfare. This doctrine will include both offensive and defensive IW principles. Joint IW doctrine will cover the organization for IW, responsibilities, coordination between levels of command, IW planning considerations, integration and deconfliction of IW activities, and intelligence support to IW. IW doctrine also will expand upon the principles of the Joint Pub 3313.1, "Joint Doctrine for Command and Control Warfare (C2W)." DOD experiences will assist in illuminating broader IW concepts extending beyond the base doctrine of C2W. To complement this doctrine effort, the revision to the Joint Operation Planning and Execution System will fully integrate IW into the operations planning process.

## Assessments

Capability assessments focus on the programmatic aspects of IW. The Joint Warfighting Capabilities Assessment process, under the guidance of the Joint Requirements Oversight Council and with CINC participation, serves as the primary analytic tool to support the Chairman in articulating joint warfighting requirements. This process achieves its objective by zeroing in on two key milestones of the Planning, Programming, and Budgeting System (PPBS). First is the Chairman's Program Recommendations leading to focused language in the Defense Planning Guidance. This is followed later in the PPBS

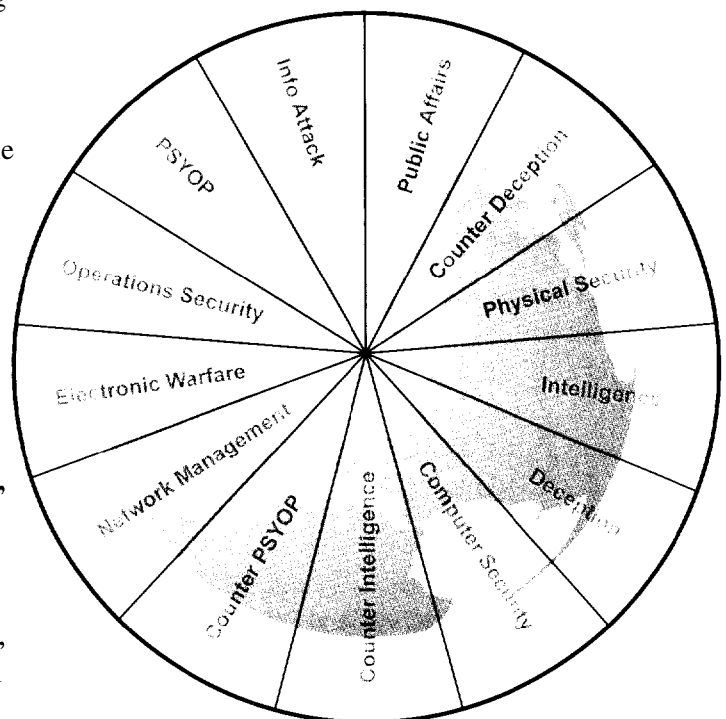
process by the Chairman's Program Assessment.

## Organizational Infrastructure

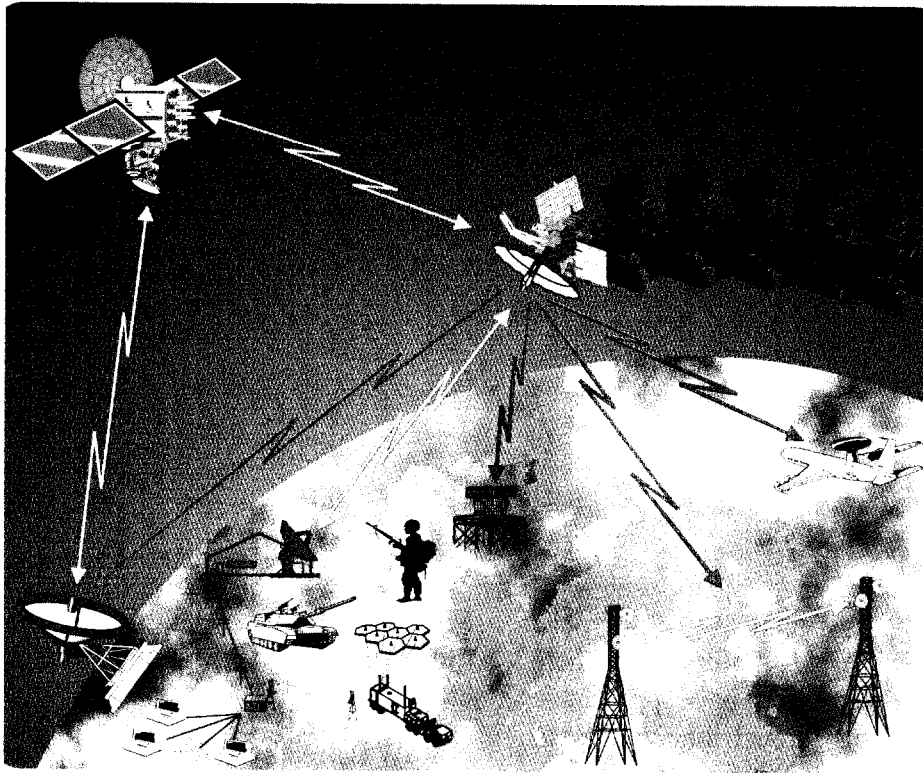
Many components have begun to organize to support IW activities. The interagency coordination requirements so central to IW effectiveness require careful attention to current organizational approaches.

Services and Defense agencies have initiated or expanded some capabilities to respond to security incidents and perform vulnerability assessments to fielded systems. These capabilities will play a vital role in mitigating vulnerabilities over time.

Most of the combatant commands have formed a tailored IW cell to meet the challenges presented by this emerging area. To provide the support the CINCs require, the Joint Staff has focused responsibility for CINC/operational support



*Building information warfare focus means merging traditionally disparate disciplines*



*Advanced information-based technologies...  
a key enabler of the IJW vision*

aspects of IW within the Operations Directorate through the creation of an IW cell that mirrors those at the combatant commands.

Intelligence underpins IW operations in peace, crisis, and war. **Critical to the continued success of IW efforts will be the availability of intelligence to support a comprehensive threat awareness.** Ongoing Intelligence Community efforts have produced initial assessments of the foreign threat, and other efforts are under way to expand that work. A comprehensive and rigorous understanding of the total threat is a critical requirement to develop a credible risk management strategy, effective and focused training, education, and awareness programs.

The Intelligence Community also is stepping up to the unique requirements of targeting and battle damage assessment. These efforts will require new processes and techniques to link the intelligence and operational communities. The net effect will be an intelligence community that is prepared and focused

to meet the significant challenges that await in IJW.

## Technology

Information-based technology is a principal enabler of the IJW vision. The Joint Staff continues to develop and maintain ties with government and industry laboratories to keep abreast of the latest discoveries and to explore ways to leverage technology to support IW requirements.

**Maintaining ties to academic and scientific organizations provides a glimpse at the leading edge thinking that may influence future warfighting strategy and doctrine.** This process also provides valuable insights that can direct current IW capabilities and architectures in favor of emerging trends.

# Conclusions

## An Assembled Vision

We have entered an age of information where nations and military organizations have opportunities to gain decisive advantage through timely access to accurate, relevant information. Information is fast becoming a strategic resource that will drive a global competitive environment and permeate every facet of warfighting in the 21<sup>st</sup> century.

Warfighters depend upon information to plan operations, deploy forces, and execute missions. Additionally, advanced information technologies have significantly altered these processes. Complex information systems support powerful infrastructures that dramatically enhance warfighter capabilities; however, increasing dependence upon these rapidly evolving technologies makes joint forces more vulnerable. Conversely, many of these same vulnerabilities extend to our adversaries, offering new opportunities to use offensive capabilities to help gain a friendly advantage.

IW concepts are being implemented to protect and defend information and information systems. When combined with offensive IW, the net result

will be the opportunity to use IW to exploit situations—and to win.

IW is a reality today and in the future; it impacts societies, governments, and the range of military operations, and all levels of war. Implementing the IW vision is a challenging task. Warriors should understand IW and its relevance to survive and fight, now and in the future. This concept has set forth a common vision that will generate an awareness of the strategy and the many complex issues yet on the horizon.

The Joint Staff, in cooperation with the Services, combatant commands and Defense agencies, is working toward implementing the common vision highlighted in this brochure. Efforts are under way now. Warriors must help implement these concepts to capture the latent potential of **Information Warfare—a strategy for peace...the decisive edge in war.**

*"The joint campaign should fully exploit the information differential, that is, the superior access to and ability to effectively employ information on the strategic, operational, and tactical situations which advanced US technologies provide our forces."*

Joint Pub. 1

For questions, comments, or additional copies of this document, please contact  
The Joint Staff, Information Assurance Division (J6K1) (703) 612-2916; the Information  
Warfare - Special Technical Operations Division, 38387 (703) 695-9292