

**NAVY**

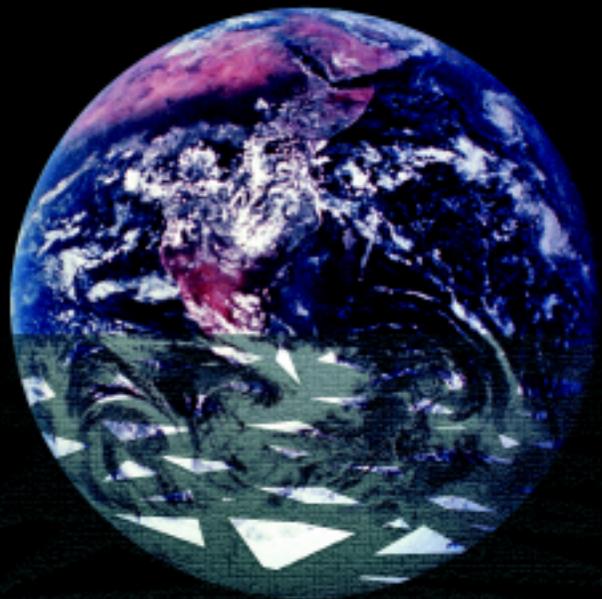
**V**

**A**

**Z**

*Information  
Warfare*

*Strategic Plan*



*IW—Capabilities for the New Millennium*

# Foreword



**T**hroughout our history, new technologies have revolutionized naval warfare. Commodore Matthew Perry led us through the transition from sail to steam; Captain Washington Irving Chambers pioneered the concept of operating aircraft from ships; Admiral Hyman Rickover created a nuclear-powered Navy; and Rear Admiral Grace Hopper ushered in a computerized Fleet.

Today's - and tomorrow's - challenge will involve the collection, analysis, and exploitation of information. Information Warfare (IW) will be as important to future naval operations as modern propulsion, naval aviation, and computerized data links are to today's. IW will have a profound effect on the Navy and will become central to the success of our "Forward...From the Sea" strategy.

For this reason, we are transitioning to Network-Centric Warfare, a warfighting posture which will enable us to respond faster and more effectively to tomorrow's threats. We will do this by leveraging our information dominance to ensure we get the right information, to the right shooter, at the right time— while denying our adversaries the ability to do the same.

This Information Warfare Strategic Plan helps chart the way toward full integration of IW into our Navy's arsenal. As such, it is a critical step in realizing the full potential of this revolutionary capability; one which will rival the introduction of steam propulsion, naval aviation, nuclear power, and computers in importance to - and impact on - our profession.

*J. L. Johnson*  
*Admiral, U. S. Navy*  
*Chief of Naval Operations*

# *Information:*

## *A Resource & a Weapon*

**I**nformation is transforming our world! We are surrounded by information and the machines that produce, process, store, and use it. All of the physical infrastructure upon which modern society relies, including electrical power grids, banking systems, public switched telephone networks, and oil and natural gas pipelines, depend upon the flow of information to function. The same is true of our military forces. Our combat, command and control, and intelligence systems are computer based and information-dependent; as are logistics, maintenance, personnel, and medical systems. This dependence on information is not new; we have always relied upon information, so much so that collecting, exploiting, disseminating and protecting it have long been an integral part of military operations. What is new is the increased access to information brought about by technology and the ensuing need to ensure a degree of information superiority over potential adversaries.

Information technology has improved the ability to see, prioritize, assign and assess information. It has and will continue to significantly impact military operations by providing military decision makers a level of insight never before achievable - or denying them the critical information upon which decisions will hinge. Differences in quality, integrity, accuracy and speed

of information transfer will determine the advantage in future operations and may very well determine outcomes. Ensuring the availability of information while denying it to an adversary will demand that the Navy place a high priority on information superiority.

Military activities performed in the information age and operations conducted in the domain of cyberspace will require that we develop the ability to conduct Information Operations or Information Warfare across the spectrum from peace to conflict and return. The target of this discipline will be the adversary's decision making ability. The target set will be comprised of information-dependent systems; and the objective, to impede the adversary's information flow, decision cycle and battle timelines, while protecting our own.

Information Operations will continue to evolve, pushed by technology, by opportunity and by the threat they portend. The remainder of this publication will present the Navy Vision for IO/IW and the goals and strategies we will employ to bring it to fruition. It should be used as a guide for the evolution of Navy IO/IW to optimize the development, delivery, and maintenance of IO capabilities for the fleet.



# Information Operations . . .

**U.S.** Naval Forces must be prepared to perform missions in peace, conflict and war and in a variety of scenarios from war to non-traditional roles such as peacekeeping, maritime interdiction, and humanitarian operations. To meet this challenge, Navy personnel are organized, trained, equipped and supported to plan and execute operations in a variety of media including that of the information domain.

*These “Information Operations,” as with other forms of military operations, are intended first to deter conflict, and then to protect U.S. information, information - based processes, and information systems, and create the conditions necessary to attain information superiority over potential adversaries in time of conflict. Whether we engage in Information Operations during periods of peaceful competition, or Information Warfare at the point of crisis or conflict, technology will have a predominant role in determining the outcome.*

## Information

*Facts, data, or instructions in any medium or form.*

— DoD INST 3600.1

## Information Superiority

*The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.*

— DoD INST 3600.1

## Information Operations (IO)

*Actions taken to affect adversary information and information systems while defending one’s own information and information systems.*

— DoD INST 3600.1



# Information

## Warfare?

### Information Warfare (IW)

*Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.*

— DoD INST 3600.1

### Information Assurance (IA)

*Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.*

— DoD INST 3600.1

### Defensive Information Warfare (IW-D)

*Using Information Assurance as its basis, IW-D is active in nature, performed by duly authorized and trained personnel, and provides continuous monitoring of our information systems to detect, deny, and respond to unauthorized intrusion, access, or attack.*

### Special Information Operations (SIO)

*Information Operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the U. S., require a special review and approval process.*

— DoD INST 3600.1

# *Information Operations*

**F**or U.S. Naval forces, technology has expanded our target set, improved our aimpoint, and provided alternative means for achieving national security objectives. Information technologies offer us the potential to manipulate or degrade information systems, attack sensor systems and networks, disrupt satellite functions, interdict power grids, or negate sensor-to-shooter links, all without firing a shot. This improvement in our ability to bring force to bear in so precise a manner supports the very essence of warfighting. These operations, concentrated in the information domain, are defined by the timeframe in which they occur; by the approval process required; and in the context of traditional military activities.

Information Operations exploit the opportunities and vulnerabilities inherent in the dependence on information to support military activities. Information Operations include actions taken to affect an adversary's information and information systems, and those taken to protect U.S. information, information-based processes, and information systems. Its goal is to ensure U.S. Forces may act to deter conflict. The Navy must be prepared, should deterrence fail, to gain and maintain information superiority over any potential adversary. The focus of IO/IW is on information-dependent systems, including weapons, infrastructure, command and control, computer, and associated network systems. These operations address hardware, software and associated personnel.

# Joint Vision 2010 & the Challenge of IW

**J**oint Vision 2010 provides us a vision of future warfare in which US forces will enjoy full spectrum dominance by achieving total Information Superiority. The basis for this framework lies in the command and control and intelligence, along with other applications of new technology, which will transform the traditional military functions of maneuver, strike, protection and logistics. These transformations are so powerful that the Joint Staff has presented them as emerging operational concepts for Dominant Maneuver, Precision Engagement, Full Dimensional Protection and Focused Logistics. Achieving the level of information superiority needed to facilitate this revolution in military operations requires the services to develop both Offensive and Defensive IW capabilities. These will transcend the strategic, operational, and tactical levels of warfare to include Military Operations Other Than War.

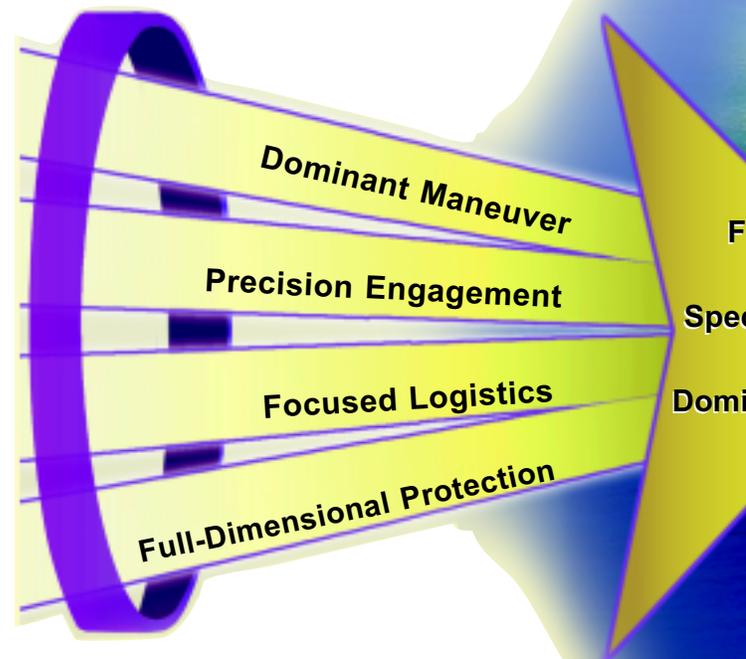
**Offensive IW** will employ traditional methods such as precision attacks to destroy adversary key command and control nodes, and non-traditional methods such as electronic intrusion into information networks to deny, deceive or degrade the adversary decision process.

Effective **Defensive IW** will be our only guarantee that we can maintain information superiority in the face of similar attacks on our own information systems. Together, they will provide the leverage needed to implement Joint Vision 2010.

The unique nature of IW, the necessarily covert nature of certain offensive IW operations, and the wide range of possibilities for using IW to support military operations or as an alternative means of achieving national security goals, presents the very significant challenge of establishing IW applications for future integration in national policy. In the absence of a current policy, we will look to the CINCs' campaign plans to provide a means of resolving policy issues related to IW. A fully integrated IW plan will serve to surface the information needed to establish Rules of Engagement (ROE) and coordinate

through an interagency process to reduce, if not eliminate, the need for going outside DoD once execution of the campaign begins. Progress in this vital warfare area must continue as national policy evolves.

Although there is a general mandate for DoD to protect the nation from foreign military attack, the unfamiliar nature of IW, difficulties in identifying "computer network attack", and existing laws will constrain DoD from taking an overly proactive role in defending the National Information Infrastructure (NII). Offensive IW suffers similar concerns. Until required mechanisms for planning and approving potentially sensitive operations are put in place, and the relationship between traditional military activities and covert operations are established, there



will be no clear division of effort among government agencies. Resolution of these and related IW problems await an improved understanding of IW among all concerned parties. However, this does not translate to inaction or postponement of IW initiatives by DoD. The services will continue to lead the nation in the development of IW weapons, doctrine, organization and training.

# The Navy's IW Mission

**T**

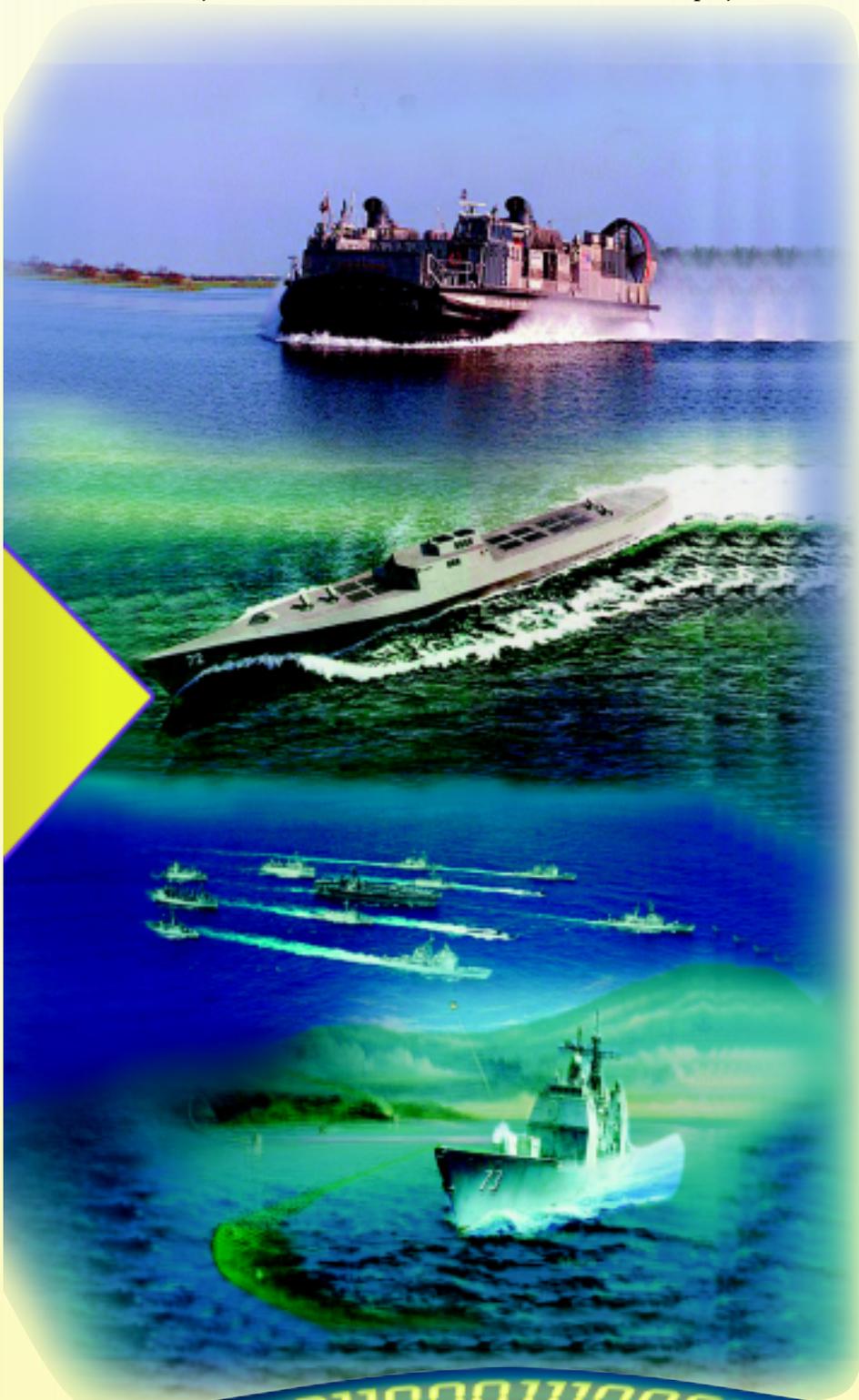
he Navy's IW mission is to sustain Information Superiority across the continuum of peace, crisis, and conflict—enabling and enhancing the ability of naval forces to successfully execute joint military operations. Time and time again, the Navy has answered the nation's call, with forward-deployed naval forces, to deter aggression, enhance regional stability, provide timely crisis response and — when necessary — conduct offensive combat operations... from the sea.

Today, IW offers naval forces an array of precision strike weapons, opening up lucrative and previously inaccessible target opportunities and offering planners enhanced options for winning decisively in the information-dependent engagements of the future.

## IW Functional Areas

- **OFFENSIVE IW** - Actions taken to manipulate, deny, deceive, delay, and destroy an adversary's information, systems, and networks.
- **DEFENSIVE IW** - Actions taken to protect friendly information from exploitation and attack by unauthorized entities or adversaries.

As in all warfare areas, commanders use their own sensors as well as off-board assets to develop a common operational picture of the battle space. IW commanders use organic sensors for the planning, real-time execution, and IW re-attack options for Offensive IW and to detect and defend against an adversary's efforts. This tactical information, along with information from other sensors, is injected into the analytical intelligence process and contributes to the formal support provided to the IW Commander.



# The Threat...



The IW threat takes many forms. It takes material form by corrupting computer databases, overriding control systems, inserting malicious software, conducting classic jamming of sensors and control links, employing psychological and deceptive practices, and physically attacking, destroying, or disrupting critical links and control nodes. With the advent of IW, the geographic sanctuary traditionally enjoyed by the U.S. is all but gone. The threat posed by IW has reached across time and space to close the gap with potential adversaries.

In the evolving IW battle space, connectivity to a global network provides comprehensive access for friends and foes alike. As our infrastructure and military forces become more interconnected, sanctuary vanishes.

The development and rapid proliferation of digital technology in sensors, weapons, communications and C2 systems has rapidly increased and expanded the threat. While we must continue our focus on a few technologically advanced nations, we must also be concerned with every individual or group with military, political, or economic motivations who has access to even the most rudimentary computer and communications capabilities.

The threat to our infrastructure exists *today* with countless individuals, groups and nations having the capability to attack across the continuum of peace, crisis, and conflict.

*...Is Out  
There*

**“CIA Gears Up to Thwart  
‘Information Attacks’  
Deutch Lists Computer  
Break-in, Terrorism as  
High-Priority Potential  
Threats to National Security”**

**— The Washington Post  
June 1996**

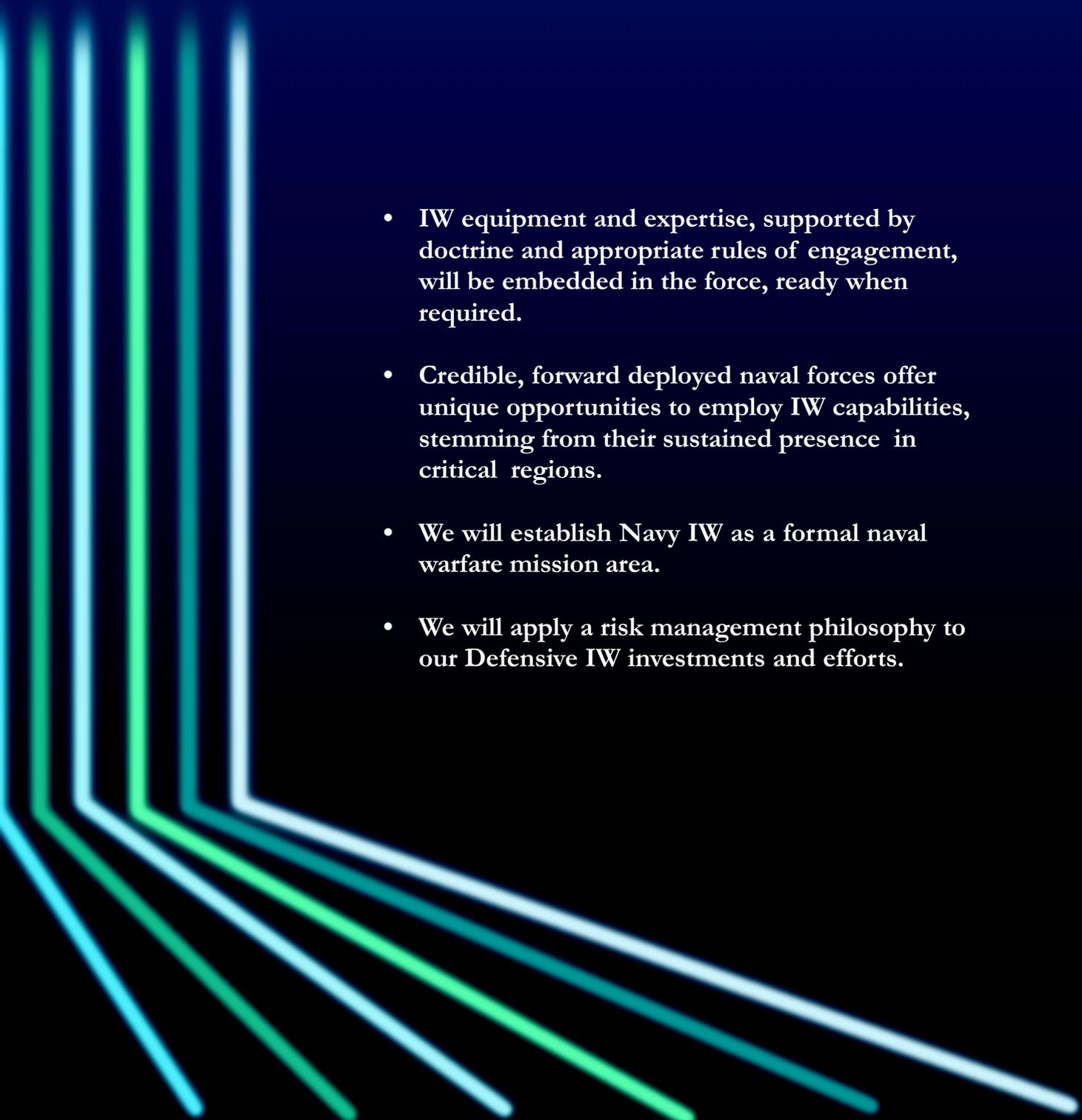
**“Argentine, 22,  
Charged with Hacking  
Computer Networks”**

**— The Washington Post  
March 1996**



# Principles for Evolution

- Navy IW will be conducted as an integral part of Joint Operations; or may be executed on a stand-alone basis as an enabler and enhancer of service capabilities; interoperability and adherence to standards are paramount.
- We will exploit technology and leverage intelligence to support Offensive and Defensive IW functions.
- We will build on existing fleet capabilities and maximize the use of our operational, organizational, and technological resources.
- We will apply a system design philosophy of modifying installed shipboard and aircraft systems for Offensive and Defensive IW purposes, whenever possible.

- 
- IW equipment and expertise, supported by doctrine and appropriate rules of engagement, will be embedded in the force, ready when required.
  - Credible, forward deployed naval forces offer unique opportunities to employ IW capabilities, stemming from their sustained presence in critical regions.
  - We will establish Navy IW as a formal naval warfare mission area.
  - We will apply a risk management philosophy to our Defensive IW investments and efforts.

# Evo Navy IW

**T**he origins of the Battle Force IW Commander can be traced to the 1970s and 1980s when distinct staff EW and Cryptologic officers were elements of the Battle Group Commander's staff. With the infusion of modern digital technology into communications, sensors, and weapons systems in the early 1990s, the duties of the staff EWO, Cryptologist and Deception Planner were integrated under the Space and Electronic Warfare Commander (SEWC) to provide mission area focus and synergy.

## ***EXECUTIVE AGENCY***

*Commander, Naval Security Group Command, at the Direction of the CNO, serves as the Navy Executive Agent (EA) for Information Warfare. In his capacity as EA, COMNAVSECGRU brings a number of core competencies to the conduct of Information Operations/Information Warfare which are unique to NSG or compliment developing fleet capability to perform IW functions.*

*As the Navy Service Cryptologic Element (SCE), NSG conducts Signals Intelligence (IW Exploit); responds to a CNO charter to develop Special Technical Attack capabilities (IW Attack); and executes NSA - delegated responsibilities to ensure the proper training, legal compliance and conduct of all Navy personnel engaged in Navy Communications Information Systems Security monitoring efforts (IW Protect).*

warfare disciplines under the Command and Control Warfare Commander (C2WC). The C2WC's mission was to attack enemy C2 in order to isolate enemy commanders from their forces. The elements of C2W were then defined as Operations Security, Psychological Operations, Military Deception, Electronic Warfare, and Physical Destruction.

*IW and C2W.* The growing sophistication, expansion, and reliance on information technology in the mid 1990s made it apparent that the role of the C2WC needed to evolve and expand to incorporate the information process, whether human or automated. To support this, the C2WC concept was expanded to focus on the vulnerabilities and opportunities presented by our adversaries' dependence on information and information systems, as well as to protect our own forces from attack.

To support the evolution of IW in the operational arena, CNO reorganized in 1994, designating OPNAV N64 as the Director, Information Warfare and appointed COMNAVSECGRU as the Executive Agent (EA) for IW.

The Naval Information Warfare Activity (NIWA) was established in 1994 and designated a Reinvention Laboratory to field state-of-the-art IW systems, assess the vulnerability of naval systems, and manage naval IW-related modeling and simulation efforts.

*The focus of the Navy IW organizational structure is to support the operating forces and their embedded IW capabilities and operations. The adjacent graphic depicts various organizations which support military requirements to man, train and equip the force; the areas of Offensive and Defensive IW; development of IW policy, doctrine, and tactics; and augmentation by specially trained IW personnel.*

Recognizing the importance of C2 and counter-C2 during Desert Storm, the Joint Staff, and subsequently the Navy, reorganized to integrate and coordinate disparate



# The IW Foundation...

**N**aval forces are critically dependent on information-intensive systems to generate dominant combat power. Our growing dependence on information places vital demands upon its availability and integrity. Defense of our information and information systems against intrusion and attack must be made a priority in order to achieve Information Superiority. Recognizing this, the Secretary of the Navy, the Honorable John Dalton, outlined a comprehensive Defensive IW program to achieve and sustain Information Assurance (the availability, confidentiality and integrity of our information and information systems) for naval forces. This program constitutes a roadmap to increased security of the Navy Protected Information Environment (PIE).

Identify information systems that are critical to our military effectiveness and national security. Designate these systems, in total, as the Protected Information Environment, or PIE. Focus INFOSEC efforts and investments on the PIE.

Establish the means to model three critical aspects of the PIE: (a) vulnerability of components and systems to attack; (b) consequences of different types of information attack; and (c) means of restoration from successful attacks.

Apply the information developed from these analyses to the design of new systems, so as to minimize risk of intrusion on these systems and achieve the most "graceful degradation" if they are successfully attacked.

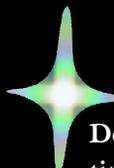
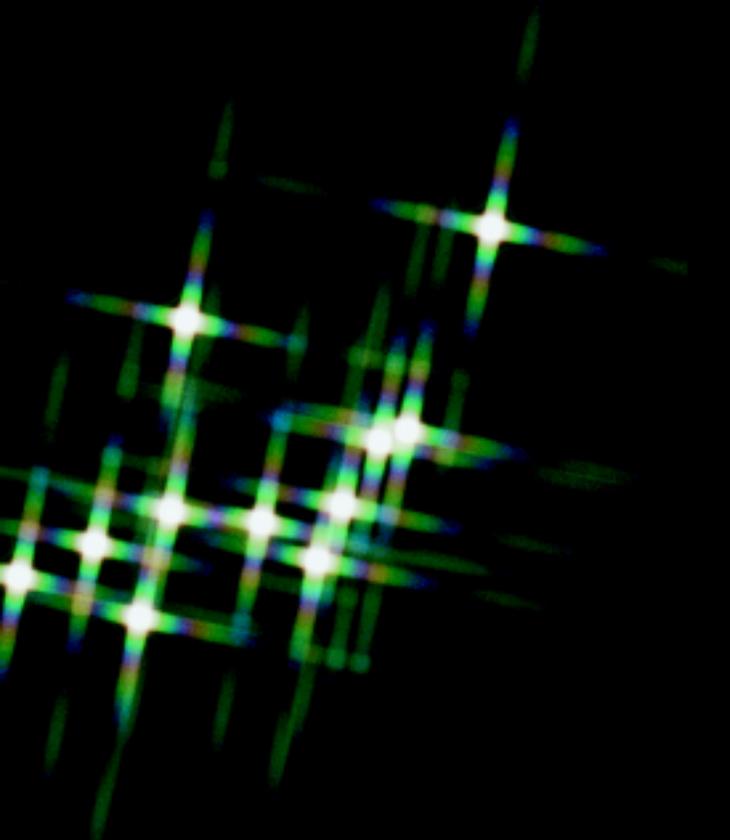
Develop and maintain a consistent and rigorous risk and consequence management methodology for protecting existing systems and processes within the PIE. This methodology must balance threat, cost and system criticality.

Invest in methods and systems designed to enhance the probability that information attacks are promptly detected and their consequences rapidly assessed.

Develop policy, strategy and tactics for responding to attacks so as to deter and defend against further attacks and deceive as to the effects of attacks that have been conducted. Identify policy, legal and administrative issues that present opportunities or obstacles in this effort. Develop plans to clarify or overcome them, as appropriate.



# *Reducing Our Greatest Risk*



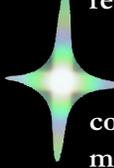
Establish a Red Team to simulate attacks on DoN systems. Include simulated attacks, the contingency plans that would respond to them, and information warfare disaster recovery as a regular part of fleet and field exercises. Integrate information warfare defensive capability and vulnerabilities into readiness reporting systems.



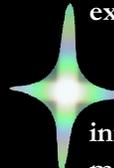
Establish appropriate counter-intelligence capabilities to cope with information warfare threats. As part of this effort, maintain and strengthen the closest ties to intelligence and law-enforcement organizations.



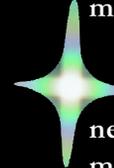
Establish close liaison with civilian and other governmental organizations that are developing defensive information strategies and tactics. Place the highest priority on coordination with the other services and the National Security Agency in these respects.



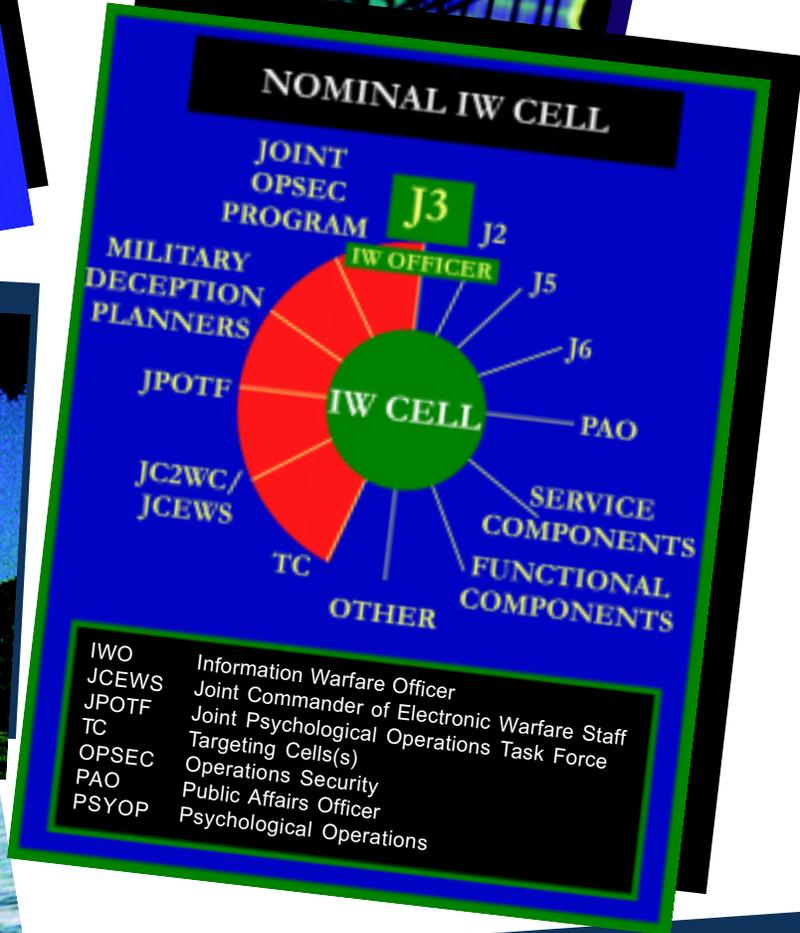
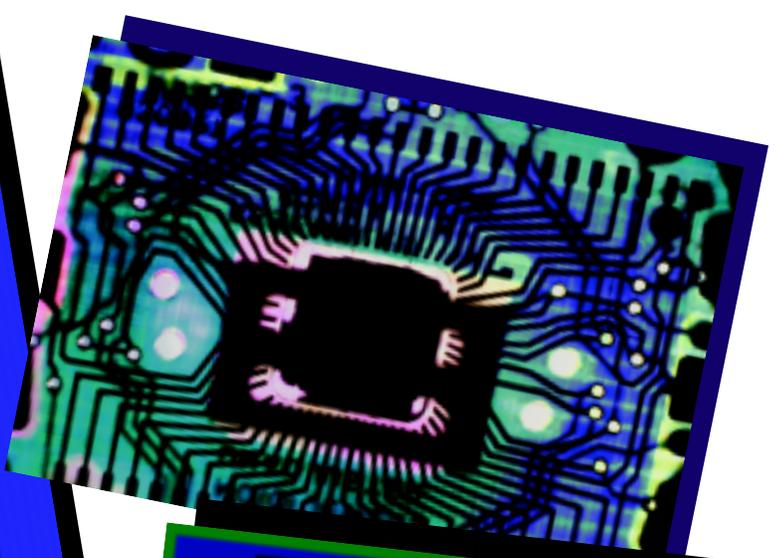
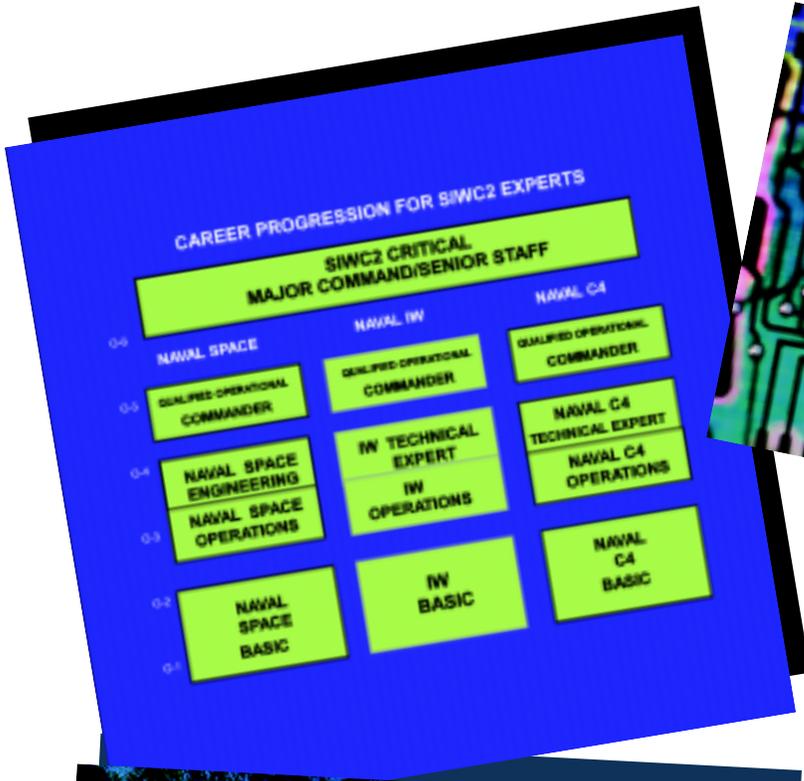
Provide support to IW R&D efforts, ensuring continuing access to the most advanced developments in tools and processes. Capitalize on the flexibility and leverage resulting from modern information technology by sharing technology and processes between the traditional attack and exploit disciplines.



Ensure that DoN doctrine emphasizes information dominance in the battle space. Implement effective technical and managerial training programs so that the DoN has sufficient personnel who are trained and skilled in network information systems administration and security.



Institute a DoN-wide education and awareness effort focused on steps to increase information assurance and instituting best practices into Navy and Marine Corps Standard Operating Procedures.



# *Navy IW Strategic Action Areas*

## ***STEERING THE COURSE***

The following pages address specific courses of action for these Strategic Action Areas:

- Policy and Doctrine
- Organization
- Career Development
- Training and Education
- Research & Development
- Acquisition
- Mission Planning and Simulation
- Intelligence Support



# *Policy & Doctrine*

## **BACKGROUND**

DoD Directive TS3600.1, Information Warfare, December 1992, established the foundation for all IW policy within DoD. JCS followed with MOP 30 in March of 1993 which integrated Psychological Operations (PSYOP), Military Deception, Operations Security (OPSEC), Electronic Warfare (EW), and destruction into a new warfare area, Command and Control Warfare. CNO issued OPNAVINST 3430.25, April 1994, which broadly outlined Navy IW policy. It was closely followed by an IW/C2W implementation instruction, OPNAVINST 3430.26 in January 1995. CJCS instruction 3210.01 defined Joint policy for IW. Joint Publication 3-13, Joint IW doctrine, is in draft.

## **DESIRED OUTCOME**

. . . a powerful naval force guided by IW policy and doctrine which will have a decisive impact, from the sea, in times of peace, crisis, and conflict. To achieve this outcome we must develop IW policy and doctrine which:

- Ensures compatibility with evolving Joint policy and doctrine.
- Implements a dominant IW capability within the Navy.
- Emphasizes coherency and synergy between the Offensive and Defensive aspects of Navy IW.
- Recognizes and supports the critical role IW sensors play in providing precision information essential for Offensive and Defensive IW.

## **COURSE OF ACTION**

OPNAV will continuously review and revise IW related policies to ensure they authorize, enable, and guide research, development, acquisition, and maintenance of IW technologies, systems and programs to support a superior naval Offensive and Defensive IW force.

OPNAV will develop, regularly update, and refine the Navy IW implementation plan to ensure it contains clear objectives, authorities, and accountabilities.

OPNAV and Naval Doctrine Command (NDC) will establish IW as a formal warfare area.

OPNAV will coordinate with NDC to ensure IW is included in the long term vision for the Navy as well as in current doctrine.

CNO/CMC will ensure complementary Navy and Marine Corps IW policy and doctrine.

# Organization

## BACKGROUND

OPNAV Instruction 3430.26 contained implementation guidance and identified organizational relationships and responsibilities for IW. This instruction laid the foundation for Navy's IW organizational structure, doctrine, equipment procurement, and training which will ensure the successful conduct of Navy IW.

## DESIRED OUTCOME

Development of well defined organizational responsibilities and interrelationships that ensure the availability of superior IW capabilities to support naval forces.

## COURSE OF ACTION

Fleet CINCs establish a standardized IW Commander and staff in the Composite Warfare Commander (CWC) organization commensurate with increased IW mission and structured in consideration of the recent Joint Staff designation of the Operations Directorate J-3 (J-39) as the primary focal point for all IW operations.

OPNAV will, in coordination with the Fleet CINCs, refine the interrelationships and support requirements between the IW shore infrastructure and afloat IW organizations.

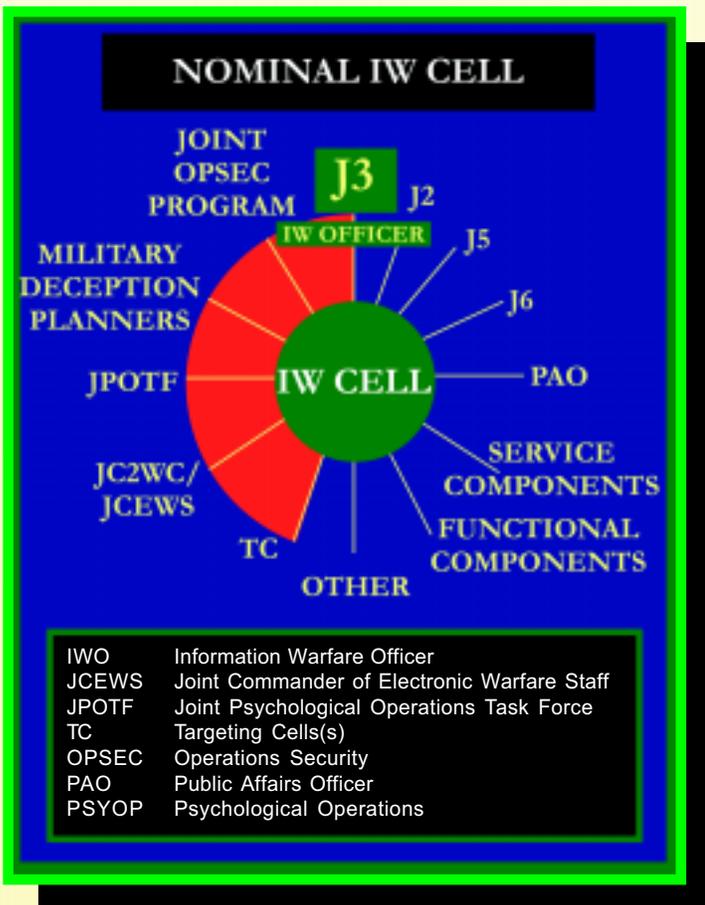
COMNAVSECGRU will formalize its technical control relationship to FIWC for defensive IW activities.

OPNAV, in coordination with the Commander, Naval Security Group Command, will investigate the concept of an IW Wing at NAS Whidbey Island, to focus VAQ, VQ, VPU, and NSGA Whidbey IW capabilities.

OPNAV will ensure IW expertise is resident on the CNO N3/N5 staff.

The Navy IW Council will make recommendations on IW implementation in the Navy.

OPNAV will establish a Flag Officer Steering Committee to review and approve recommendations for the conduct and implementation of IW within the Navy.



# Career Development

## BACKGROUND

IW is a technologically intensive warfare area. It relies on many officer and civilian designations and enlisted ratings to bring necessary technical skills to the IW profession. Successful IW will rely on the development of knowledgeable IW professionals from all communities committed to integrating IW capabilities into all aspects of the Navy mission. Related areas of expertise in space and command and control, when combined with IW professionals, make up the Space, IW and C2 (SIWC2) professional resource pool. In addition, warfighters from all disciplines should take lessons learned from IW experience tours back to their own warfare community.

## DESIRED OUTCOME

- To develop a cadre of officer and enlisted personnel with requisite technical and operational skills to ensure our naval forces are capable of meeting Navy and Joint IW mission requirements.
- Establish an incentive and opportunity-based career path supported by a visible and viable personnel management process.

## COURSE OF ACTION

Director of Naval Training establish basic, intermediate, and advanced training and education opportunities, both service and Joint, to produce highly capable career IW professionals.

COMNAVSECGRU will establish a mechanism for managing officer, enlisted, and civilian personnel with IW expertise to ensure their technical and professional IW competency.

Primary manpower claimants will establish a career progression to produce officer, enlisted, and civilian personnel with the skills and experience required to advance to key senior leadership positions in Joint and service assignments within their designated warfare area as well as in the IW area.

Fleet CINCs, with assistance from COMNAVSECGRU, identify IW billet requirements to support Joint and Navy IW missions.

Deputy Chief of Naval Operations for Manpower and Personnel identify Navy personnel with the appropriate aptitude, training, education and experience levels for assignment to Joint and Navy IW billets.

Deputy Chief of Naval Operations for Manpower and Personnel establish Navy officer Additional Qualification Designator (AQD) codes and assign them to IW billets and personnel for use in detailing personnel to all IW assignments.



# Training & Education

## BACKGROUND

Technological change in information systems occurs at a startling rate. New products—hardware and software—are announced daily. As these products are integrated into military C2 and weapons systems and into government and civilian infrastructure, IW opportunities as well as vulnerabilities will constantly recur.

The speed of advance in modern information technology requires aggressive training and education approach to ensure Navy professionals keep pace with emerging technologies and are able to successfully meet Navy IW mission requirements.

Maintaining mastery of the IW Battle Space will require a level of responsiveness in our technical training that will be difficult to achieve via traditional classroom training. Therefore, Navy must consider alternative “non-traditional” training solutions such as Computer Based Training (CBT), Commercial Off-The-Shelf (COTS) packages, and specially-tasked quick reaction training efforts. While these approaches have superior potential for keeping pace with technological and operational advances, they also demand more management time and attention.

## DESIRED OUTCOME

- Provide all Navy personnel with an understanding of the importance of IW and an awareness of the opportunities and risks associated with the use of information technology.
- Establish a cadre of designated officer and enlisted personnel who are equipped with the required specialized skills to successfully perform Navy IW missions and functions.



## COURSE OF ACTION

Director of Naval Training establish broad-based IW curricula to be included in officer and enlisted career progression training. Ensure timely updates to IW training materials to stay abreast of IW technological and operational developments; pursue “non-traditional” education and training approaches that optimize and improve upon the responsiveness and timeliness of training.

Fleet CINCs include IW in Navy exercises, wargames and predeployment evolutions to improve fleet IW skills.

Director of Naval Training expand IW tactics training at Tactical Training Groups, Atlantic and Pacific.

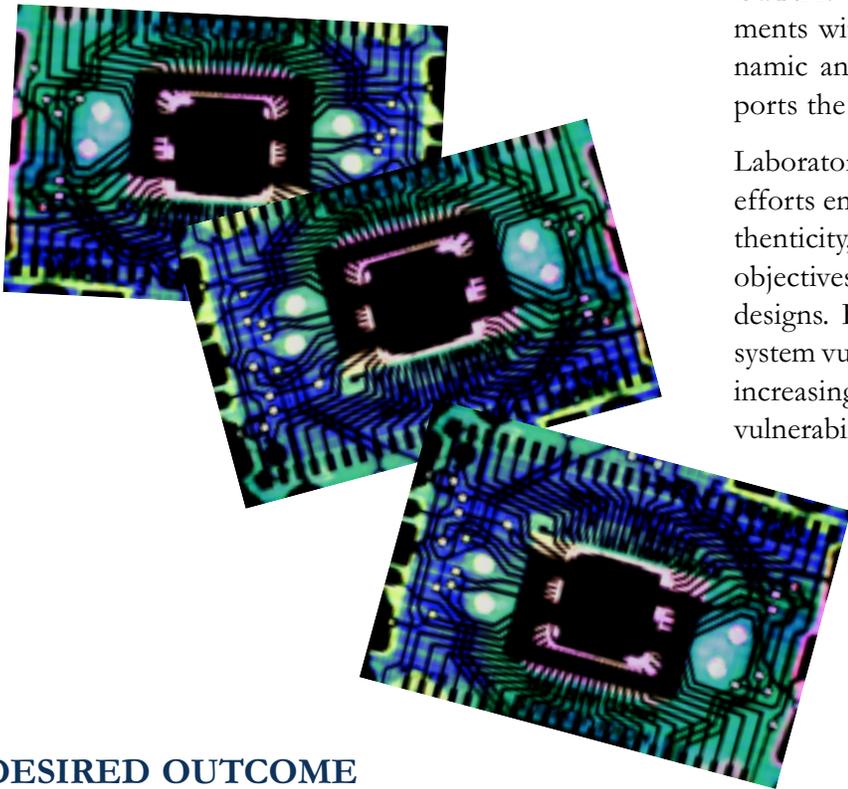
Naval Post Graduate School expand the IW curriculum to confront the challenge and anticipate the future.



# Research & Development

## BACKGROUND

IW is characterized by a dynamic environment manifested in a variety of emerging technologies and applications. Naval warfighters require state-of-the-art technologies to stay ahead of our adversaries. The IW R&D process must proactively support the warfighter and must also be responsive and dynamic. The CNO staff will provide oversight of IW requirements and resources to ensure a common forum to drive IW R&D efforts.



## COURSE OF ACTION

OPNAV engage defense and national laboratories, defense colleges, civilian universities, engineering organizations, and commercial enterprises to expand the IW technology envelope.

OPNAV ensure other Service/Agency R&D activities are leveraged for Navy benefit; maximize the use of Commercial/Government Off-The-Shelf (COTS/GOTS) technologies.

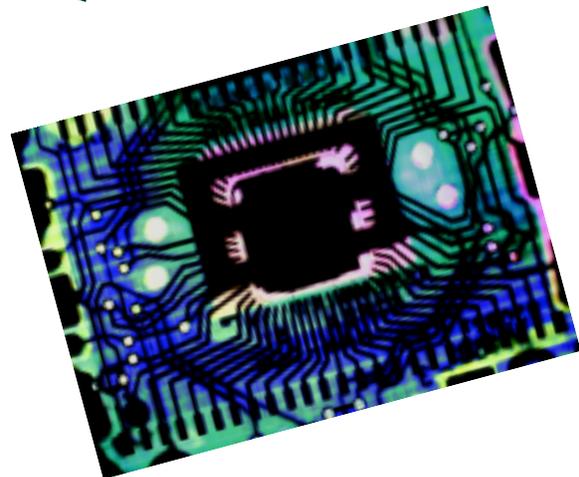
OPNAV combine and integrate operational requirements with technology assessments to develop a dynamic and proactive IW R&D program which supports the warfighter.

Laboratories and agencies prioritize ongoing IW R&D efforts emphasizing the timeliness, confidentiality, authenticity, and protection of information as principal objectives to be preserved and attained in all system designs. Emphasize efforts to assess and mitigate own system vulnerabilities to an adversary's IW efforts while increasing our ability to exploit and attack adversary vulnerabilities.

Laboratories and agencies sponsor a continuing series of IW R&D and technology development seminars involving military, government, academia, and industry to exchange information and serve as a catalyst for expanding the IW technology envelope.

## DESIRED OUTCOME

- A coordinated, aggressive R&D effort, supported by intelligence, that optimizes advancing technology and investments through “dual use” and interoperability.
- An IW R&D program that triggers revolutionary, threat responsive technology advances which can be rapidly integrated into the Joint warfighting environment.



# Acquisition

## BACKGROUND

IW system interoperability and effective integration of IW capabilities in the operating forces are critical. The Space and Naval Warfare Systems Command has established the Information and Electronic Warfare Program Directorate (PD 16) with two major objectives: adopt standards for all IW capabilities; and ensure Navy IW capabilities can be integrated force-wide and in a joint warfighting environment. The establishment of PD-16 consolidated the Navy acquisition agents for IW Protect (PMW 161), IW Attack (PMW 162), and IW Exploit (PMW 163).

## DESIRED OUTCOME

A coordinated, requirements-driven Navy IW acquisition effort, supported by intelligence, that delivers integrated and embedded capabilities and systems meeting warfighter requirements for IW Protect, Attack, and Exploit.

## COURSE OF ACTION

Adopt/develop standards to minimize vulnerabilities, embed IW capabilities in the operating forces, and integrate capabilities in the Joint environment consistent with the Joint Requirement Oversight Council approved Mission Need Statement on IW.

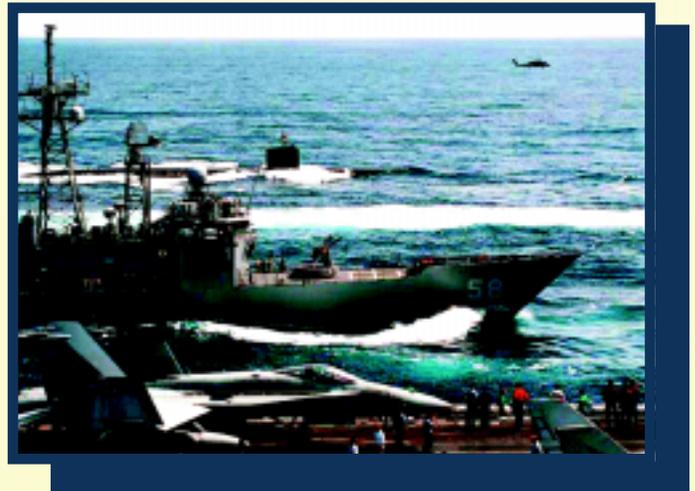
All information intensive system developers conduct information vulnerability analyses during system design. In accordance with OPNAV and DASN (C4I) security standards, they will: focus on risk management and incorporating information security features during system design; test security features during development; review test results as part of milestone decision agent actions.

Incorporate Technical Architecture Framework for Information Management standards, emphasize open architectures, and design naval information-intensive

systems for maximum joint interoperability while preserving system security.

Invest specifically identifiable resources from information-intensive systems' programs for life cycle vulnerability assessments, analysis, and the acquisition of defensive system resources.

Develop formal relationships with the national intelligence community and other services to optimize contributions to IW capabilities assessments and development.



Systematically catalog Navy at-risk systems and drive prioritization of resource investments in concert with the Planning Programming and Budgeting System cycle and the FLTCINC requirements definition process.

Assess all information systems destined for forward deployed platforms for "dual use" potential as IW exploit and attack resources. Use exit criteria for acquisition milestones to reflect and aid adherence to this objective.

Expand Navy "Carry-On" programs which will enhance Quick Reaction Capabilities to rapidly respond to emergent Offensive and Defensive IW requirements.



# Mission Planning & Simulation



## COURSE OF ACTION

Within the structure of the DoD and DoN M&S planning guidance, initiate processes to participate in the development of M&S interoperability standards in the areas of:

- IW Acquisition Support. Concentrate on virtual prototyping, capabilities visualization/simulation tools, statistically-based and physics-based nodal, terrain, antenna, IW system models and analysis tools, and modeling of the IW battle space to address consequences of and restoration from successful IW attacks.
- IW Assessment Support/Training Support. Build on IW acquisition/M&S support. Concentrate on IW mission planning to include: C2 nodes, links, and sensor data bases; C2 target capabilities, limitations and vulnerabilities; and political and military leadership decision making processes. Provide tailored computer graphics and visualization tools to support IW technical operations and mission rehearsals.
- IW Operations Support. In a forward deployed, JMCIS Flagship configuration, provide for planning and rehearsal of IW missions in a synthetic environment that accurately simulates expected terrain, environment, and threat considerations, as well as a synergistic display of red and blue C4I architectures and dependencies.

FIWC will take the lead in developing and consolidating fleet requirements for IW mission planning and tactical decision aid tools. Liaise with NIWA and other service IW centers to obtain IW M&S capabilities for FIWC and fleet training and planning missions.

NIWA will manage naval IW related M&S efforts with assistance from SPAWAR, service and national laboratories, and joint agencies as appropriate.

NIWA will take the lead in integrating detailed technical analysis and M&S methodology into acquisition, operation, and training of Navy IW systems and operators.

## BACKGROUND

The success of IW operations is contingent upon planning, pre-mission rehearsal, and situational awareness. The tools which support this capability are resident in computer-based decision aids, primarily through Modeling and Simulation (M&S). Application of these techniques can greatly enhance the mission planning process by identifying and evaluating alternative courses of action, likely outcomes, unintended consequences, resource utilization and employment, and battle damage assessment.

IW Situational Awareness (SA) will furnish the warfighter with the information required to operate inside the enemy's decision cycle, while at the same time understanding his own vulnerabilities. The principal Navy vehicle for providing IW SA and mission planning is the Joint Maritime Command Information System (JMCIS). All tools developed within JMCIS will be compliant with the DII common operating environments, in effect, becoming IW shareware.

## DESIRED OUTCOME

- User-friendly, intuitive, and collaborative Offensive and Defensive IW SA displays, mission planning tools, and pre-mission rehearsal capabilities to serve Navy forces.
- Incorporate IW into the common operational picture and the Combat Direction System.



# Intelligence Support



## BACKGROUND

IW requires that we modify traditional intelligence strategies and forge closer linkages between intelligence support, operations, and acquisition staffs to assure the best possible knowledge about potential enemies; to accommodate the technologies and dynamics of information systems, networks and uses; and to be able to understand the impact of IW on potential enemies.

Technology in the information domain is largely driven by the commercial sector. Accesses, applications, and services are in a continuous state of change. Significant leadtime is required to generate the intelligence necessary to develop offensive IW capabilities, to protect friendly information, and to target IW weapons. The full potential of the Navy's IW program cannot be realized without precise, timely, and technically credible intelligence. Commanders should develop operational requirements for IW that will drive intelligence support and capabilities development. The resultant long-term intelligence analysis may assist commanders in understanding how adversaries use and interpret information.

## DESIRED OUTCOME

- To provide accurate, timely intelligence on IW targets, information technology, and processes.
- Intelligence support must assist in Intelligence Preparation of the Battle Space and crisis end-game; accurately guide precision IW targeting; support IW research, development, and acquisition, and facilitate information awareness for naval forces.

## COURSE OF ACTION

Ensure Naval Intelligence support to IW is in consonance with Joint intelligence efforts including those at the Joint Staff, National Agencies and Joint commands.

Define new Essential Elements of Information to enhance critical support to Navy IW development and targeting objectives.

Identify intelligence support shortfalls and emergent requirements for Navy IW. While IW is highly technical and SIGINT dependent, it also requires all source intelligence to support perception management, PSYOP, and deception.

Examine technology developments and trends in information, automation, and networking. Ensure that they are characterized in intelligence products and databases.

Develop a cohesive approach to intelligence requirements, databases, and reporting to satisfy needs of operational commanders.





# *Vision for the Future*

*"The IW Vision: A Navy that will dominate the battle space by achieving total information superiority using Offensive and Defensive Information Operations to preserve the peace, deter or resolve crisis, and fight and win in combat operations."*

**T**his document attempts to capture the vision of a Navy guided by Information Warfare doctrine, manned by IW proficient sailors, and armed with an array of precision offensive and defensive IW weapons which enjoys a decisive ability to support the National Strategy across a spectrum of requirements. Advanced technologies, combined with smart targeting and the historic advantages of maneuver from the sea, will provide the Navy with unprecedented opportunities in its role as the premier forward deployed American military force. The growth and innovative application of technology will improve combat effectiveness, at the same time avoiding the vulnerabilities associated with increased information dependence.

The information revolution, driven by technology, is transforming society, reorienting economies and transforming military operations. Navy recognized the potential of information in warfighting in the late 1980's, developed the Copernicus Strategy, and has never looked back. The key to continued development and progress will depend upon our ability to create an efficient organizational structure, energized by innovation and linked to technology, to realize the benefits of Information Operations. This strategic plan is intended to provide a comprehensive concept for the conduct of Information Operations/Information Warfare to enable Navy to support National Security objectives and to meet the requirements of Joint Combat Operations.



# Glossary of

*Information Warfare, as with other disciplines, has a set of terms be confused with other applications. This Glossary of Terms*

## **BATTLE SPACE —**

Information Warfare Battle Space refers to the medium in which IW activities are conducted. The IW Battle Space addresses physical aspects, human factors, information systems, and networks, and electronic or digital media. The various levels in the IW Battle Space are interdependent and can be affected by IW activities conducted at other levels. For example, managing digital transfer standards in the electronic media to control access to information will provide a degree of protection to information residing in information dependent weapons systems at the physical level of the Battle Space. A characteristic of the IW Battle Space is that the traditional factors of time, distance, and location are dramatically compressed. The IW Battle Space is rapidly growing and evolving; it requires continuing study to enable information dominance.

## **COMPUTER NETWORK ATTACK —**

Operations to disrupt, deny, degrade, or destroy information resident in computers and computer networks or the computers and networks themselves.

## **DEFENSIVE IW —**

Defensive Information Warfare is an element of IW and is defined as actions taken to protect friendly information from exploitation and attack by unauthorized entities or adversaries. Defensive IW includes traditional information systems security products and services to achieve the objective of Information Assurance. Defensive IW is a requisite capability for achieving Information Superiority.

## **“DUAL USE” —**

“Dual-use” in IW refers to a philosophy of using the resources of one activity to achieve the objectives of another. For example, IW systems acquired for and used in Exploitation and also used to Attack an adversary’s information systems are considered “Dual-use.” “Dual-use” is intended to result in economy and cost effectiveness.

## **INFORMATION —**

Facts, data, or instructions in any medium or form.

## **INFORMATION ASSURANCE —**

Information Operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.

## **INFORMATION SUPERIORITY —**

The capability to collect, process, and disseminate an uninterrupted flow of information while exploiting or denying an adversary’s ability to do the same.

# Key Terms

*that relate to specific meanings within the discipline and may provides a short explanation of terms used in this IW Strategic Plan.*

## **INFORMATION SYSTEMS —**

The entire infrastructure, organization, personnel, and components that collect, process, store, transmit, display, disseminate, and act on information.

## **INFORMATION WARFARE —**

Information Operations conducted during time of crisis or conflict to achieve or promote specific objectives over a specific adversary or adversaries.

## **OFFENSIVE IW —**

An element of IW that refers to actions taken to manipulate, deny, deceive, delay, and destroy an adversary's information, systems, and networks. Offensive IW is a requisite capability for achieving Information Superiority.

## **OPERATIONAL ASSESSMENT —**

A vulnerability assessment targeted at determining susceptibility to exploitation and attack of fielded Information Systems in the fleet and shore communities. Generally, applies to networked systems.

## **RED TEAM —**

A vulnerability assessment conducted in connection with exercises and operations that simulates an intruder or attacker's capabilities to attack friendly information systems. (continued)

Vulnerability assessment results will be used short term to strengthen the defensive IW posture of individual commands. Longer term, red team assessment results will be fed back into the system development and acquisition process for systemic improvements.

## **SPECIAL INFORMATION OPERATIONS —**

Information Operations that by their sensitive nature, due to their potential effect or impact, security requirements, or risk to the national security of the U. S., require a special review and approval process.

## **TECHNICAL CONTROL —**

The authoritative prescription of all processes by which naval automated information systems are monitored to include those uniform techniques, standards and support mechanisms by which information is collected, processed and reported.

## **VULNERABILITY ASSESSMENTS —**

Activities taken to determine the vulnerability for unauthorized exploitation of, or attack upon friendly information and information systems.