



INFORMATION DOMINANCE CORPS



I. Overview: The Information Dominance Corps (IDC) effectively and collaboratively leads and manages a cadre of officers, enlisted, and civilian professionals who possess extensive skills in information-intensive fields. This corps of professionals receives extensive training, education, and work experience in information, intelligence, counterintelligence, human-derived information, networks, space, and oceanographic disciplines. This corps continually develops and delivers dominant information capabilities in support of US Navy, Joint and national war fighting requirements.

II. IDC Mission: Gain a deep understanding of the inner workings of our adversaries, develop unmatched knowledge of the battlespace, provide our operating forces with sufficient over-match in wartime command and control, and project power through and across the network.

II. IDC Background: The Information Dominance Corps was created within the U.S. Navy in 2009 to more effectively and collaboratively lead and manage a cadre of officers, enlisted, and civilian professionals who possess extensive skills in information-intensive fields. This corps of professionals will receive extensive training, education, and work experience in information, intelligence, counterintelligence, human-derived information, networks, space, and oceanographic disciplines. This corps will develop and deliver dominant information capabilities in support of U.S. Navy, Joint and national warfighting requirements.

IV. IDC Community Management: The Deputy Chief of Naval Operations for Information Dominance/Director of Naval Intelligence (OPNAV N2/N6) was designated as the leader of the IDC in 2009, representing a landmark transition in the evolution of naval warfare, designed to elevate information as a main battery of our warfighting capabilities, and firmly establish the U.S. Navy's prominence in intelligence, cyber warfare, and information management. Toward this end, the strategic objectives of OPNAV N2/N6 are to:

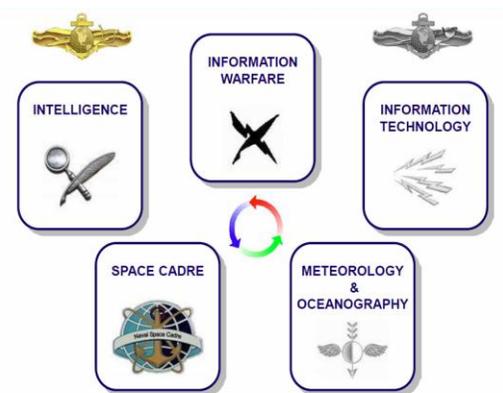
- Elevate information to a core Navy warfighting capability.
- Functionally integrate intelligence, information warfare, Information/network management, oceanography, and geospatial Information for information age operations.
- Deliver assured command and control and information access to Operational forces.

"The legacy platform-centric approach... is a way of the past. Those artificial divisions have really caused us to sub-optimize our ability to aggregate combat capability and the movement of information in ways that can maximize the effectiveness of the fleet, of the unit, for the individual."



"People who will operate in this domain will be at a premium because there will be great competition for their intellect, for their experience and for their competence. So what we have done is to take our already very proficient and experienced operators and create an "Information Dominance Corps." They will retain their individual identities, but they will be managed as a Corps, they will develop as a Corps and they will fight as a Corps. "

~ Admiral Gary Roughead



45,000 Professionals in Information-Centric Disciplines

- Boldly introduce game-changing concepts, strategies, and Capabilities.
- Coordinate resource investment to deliver information-centric Capabilities and competitive advantages.
- Aggressively accelerate experimentation and innovation with Information capabilities.
- Deliver deep multi-intelligence penetration and understanding of Potential adversaries, melded with deep multi-domain understanding of the operating environment.
- Deliver remotely piloted, unattended, and autonomous capabilities adaptively networked to extend reach, penetration and persistence in denied areas.

Information Dominance Guiding Principles:

- Every platform a sensor
- Every sensor networked
- Dynamically tasked Sensors
- A network-hosted enterprise
- Improved autonomous platforms
- Universally discoverable data
- Targeting data accessible to all shooters
- Expanded partner sharing agreements
- Federated data exploitation
- Architecture
- Service-oriented architecture
- World-class training and education

“Cyberspace will be operationalized with capabilities that span the electromagnetic spectrum – providing superior awareness and control when and where we need it.” – ADM Greenert, CNO, Sailing Directions: Vision for next 10-15 yrs

V. Operationalizing the IDC and Cyber Warfare:

A. Fleet Cyber Command/10th Fleet (FLTCYBERCOM/C10F): The United States Tenth Fleet (COMTENTHFLT or C10F) is a functional formation of the United States Navy. It was first created as an anti-submarine warfare coordinating organization during the Battle of the Atlantic in World War II. Tenth Fleet was reactivated 29 January 2010 as the US Navy Fleet Cyber Command/10th Fleet or FLTCYBERCOM/C10F, and is:

- the Navy component of United States Cyber Command (USCYBERCOM)
- the Navy authority for cyber operations
- the Navy Service Cryptologic Element (SCE), or Service Cryptologic Component (SCC)
- the operational authority and capability provider for Information Operations (IO) and cyberspace operations, in close coordination with all Navy component commanders

Fleet Cyber Command Mission: The mission of Fleet Cyber Command is to direct Navy cyberspace operations globally to deter and defeat aggression and to ensure freedom of action to achieve military objectives in and through cyberspace; to organize and direct Navy cryptologic operations worldwide and support information operations and space planning and operations, as directed; to direct, operate, maintain, secure and defend the Navy’s portion of the Global Information Grid; to deliver integrated cyber, information operations, cryptologic, and space capabilities; and to deliver global Navy cyber network common cyber operational requirements.

Tenth Fleet Mission: The mission of Tenth fleet is to serve as the Numbered Fleet for Fleet Cyber Command and exercise operational control of assigned Naval forces; to coordinate with other naval, coalition and Joint Task Forces to execute the full

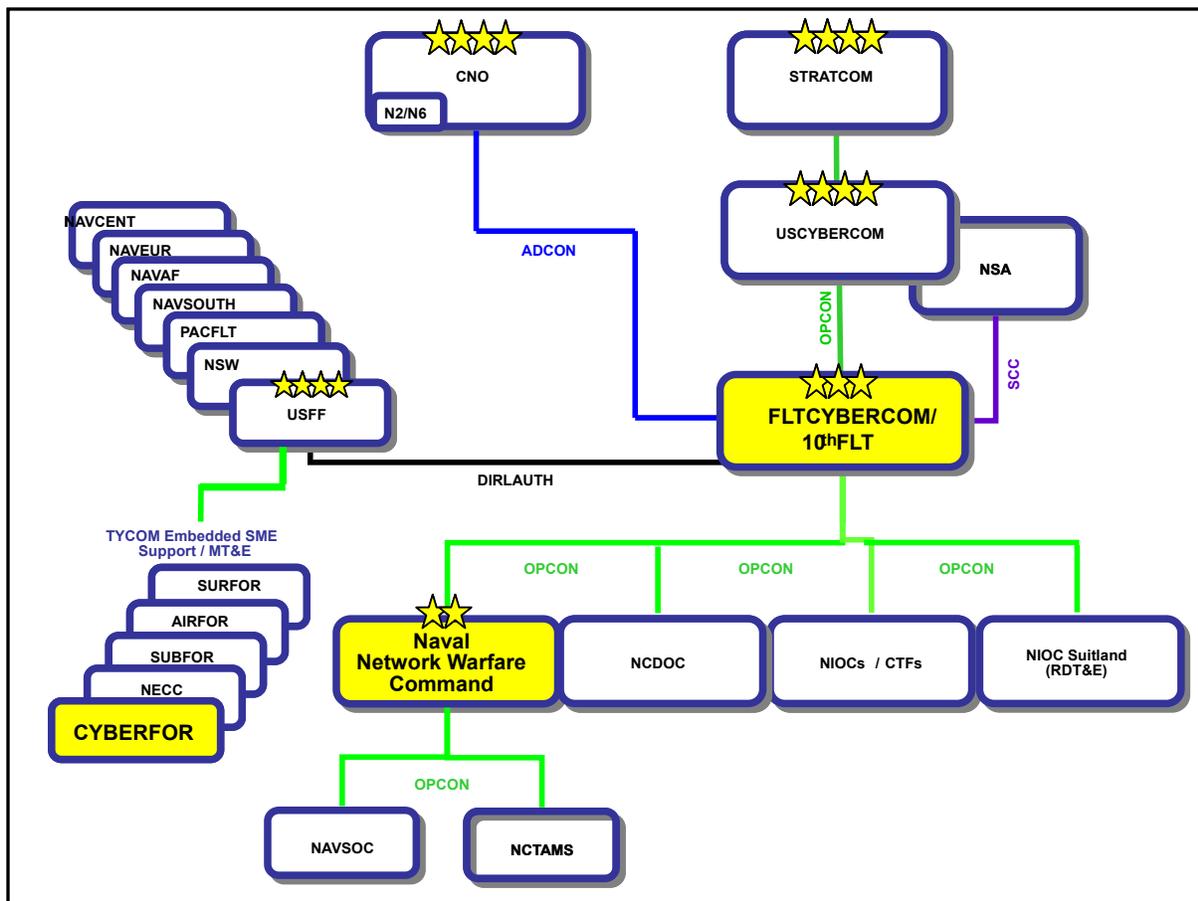


spectrum of cyber, electronic warfare, information operations and signal intelligence capabilities and missions across the cyber, electromagnetic and space domains.

B. Navy Cyber Forces (NAVCYBERFOR): Navy Cyber Forces (NAVCYBERFOR or CYBERFOR) is an Echelon III command under Commander, US Fleet Forces Command (COMUSFLTFORCOM), and is the Type Commander (TYCOM) for cryptology/SIGINT, cyber, electronic warfare, information operations, intelligence, networks, and space disciplines. Like other TYCOMs, this is the manpower, training, modernization, and maintenance component for these disciplines. Many NAVCYBERFOR personnel will be from Information Dominance Corps (IDC) communities, and much of FLTCYBERCOM's operational manpower will come from NAVCYBERFOR.



Navy CYBERFOR Mission: To organize and prioritize, training, modernization, and maintenance, requirements, and capabilities of command and control architecture/networks, cryptologic and space-related systems and intelligence and information operations activities, and to coordinate with Type Commanders, to deliver interoperable, relevant and ready forces at the right time at the best cost, today and in the future.



C. Organizational alignment of Navy Cyber with USCYBERCOM and IDC N2/N6:

VI. Detailed IDC Community Overviews: The IDC is made up of Information Professional Officers (IP), Information Warfare (IW) officers, Intelligence Officers (INT), Oceanography Officers (METOC), Space Cadre, Aerographers Mates (AG), Cryptologic Technicians (CT), Intelligence Specialists (IS), Information Technicians (IT) and Navy civilians.

	Information Professional (IP) 182X, 642X, 742X	Information Warfare (IW) 181X, 644X, 744X Cyber Warfare Engineer 184X, 743X	Intelligence (INTEL) 183X, 645X, 745X	Meteorology/Oceanography (METOC) 180X, 646X
	Information Systems Technician (IT) 	Cryptologic Technician (CT) (CTI, CTM, CTN, CTR, CTT) 	Intelligence Specialist (IS) 	Aerographer's Mate (AG) 
Other	IT Civilian	Space Cadre 5500x 6206x Subspecialists	Intelligence Civilian	

A. Information Professional (IP): The Information Professional (IP) community operates, maintains, secures, plans, acquires, and integrates naval networks and systems that support Navy business processes to ensure they are reliable, available, survivable, and secure. The community also seeks to aggressively foster development of the skills needed to conduct Network Centric operations, both afloat and ashore; evaluate and integrate leading edge technologies, innovative concepts, and essential information elements to maintain superior maritime operations in the information age.



1. Mission: Deliver Cyber ready systems and capabilities to the Fleet. Expertly operate the Navy networks 24/7 to support all missions to include Navy command & control and communications capabilities to support Navy, Joint and National requirements. Working with Navy stakeholders to ensure the Naval Networking Environment is aligned with mission needs. IPs develop a world-class, superior workforce and identify efficiencies while improving effectiveness.

2. Overview: The IP Community has built a culture of continuous learning within its ranks. Regardless of seniority, it is expected that all IPs stay current with the world of technology and every member of the community is encouraged to find new ways these technologies and information disciplines can be used for military benefit. Recognized for their technical expertise and experience rooted in Fleet operations, the IP Community leads the development and deployment of advanced command & control, space, cyber, and information technology capabilities within the Navy. Understanding naval operational needs, the IP Community is a key component to Navy's C4I agility.

3. Operational Elements: IPs serve both at sea and ashore. Emphasis is placed on maintaining relevancy to the operational mission, demonstrating world-class technical knowledge, developing agile thinking and innovative problem-solving skills, and staying current in this

rapidly changing field via continuous education and qualifications. The Naval environment is a complex, large-scale system of systems, and it is only expected to become more complex as new technologies emerge and more and more devices are connected to the Internet. IP officers serve in challenging billets of ever increasing scope and responsibility both afloat and ashore. IPs are assigned to sea billets on strike group staffs and ships at each grade. Shore tours include C4I/Space/Surveillance billets on major Navy and Joint staffs as well as command of key communication and surveillance facilities around the globe.

Cyber and Net-Centric Warfare Commands: Navy IPs serve as Commanding Officers of Naval Computer and Telecommunications Area Master Stations (NCTAMS), Naval Computer and Telecommunications Stations (NCTS), the Navy Communication Security (COMSEC) System, and network operations centers (NOCs). IP officers also serve in key positions on the Navy Staff, Joint Staff, Combatant Commander Staffs, major Fleet Commander staffs, Naval Network Warfare Command, and Fleet Cyber Forces Command. Senior IPs serve as the Chief Information Officers in many commands.



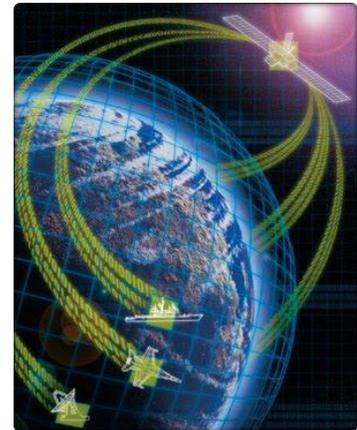
Fleet Information Dominance: Navy IPs serve as Information Management Officers, Combat Systems Officers, Carrier Strike Group C4I Directors, amphibious C5I Officers, staff Knowledge Managers, Communications Officers, Electronic Key Management System (EKMS) Custodians, Information Assurance Managers, and Information Systems Officers. IPs at sea lead enlisted Information System Technicians, Cryptologic Technician Networks, Electronics Technicians, Interior Communications Electricians and Fire Controlman ratings, and are responsible for vital shipboard functions that support everything including air operations, ship machinery control, logistics, intelligence systems, medical, and quality of life systems. IPs at sea serve as Battle Watch Captains, Tactical Action Officers, Officers of the Deck, CIC Watch Officers, and many also qualify as Surface Warfare Officers.



Joint and Combined Operations: Navy IPs serve today in Afghanistan, Iraq, Horn of Africa and in other hazardous duty areas supporting Joint and Combined operations. IPs serve as J6 Directors, Knowledge Managers, Network Systems Engineers, and in other communications positions. The IP Community also serves in Special Warfare and Navy Expeditionary Combat assignments to provide essential C2, communications, and networking capabilities.

- 4. The Navy's Networks:** The Navy IP Community manages the Navy's networks including:
- NIPRNet** – The Non-Classified Internet Protocol Router Network for unclassified but sensitive information exchange.
 - SIPRNet** – The Secret Internet Protocol Router Network for classified (up to and including Secret) information exchange.

- c. **JWICS** – The Joint Worldwide Intelligence Communications System for classified (up to and including Top Secret (TS) and Special Compartment Information (SCI) information exchange.
- d. **CANES** – Consolidated Afloat Networks and Enterprise Services provides the common shipboard computing environment infrastructure for command, control, communications, computers, and intelligence (C4I) applications.
- e. **ONE-NET** – The OCONUS (outside the Continental United States) Navy Enterprise Network provides information exchange and telecommunication services to OCONUS Navy shore commands.
- f. **CENTRIXS** – Combined Enterprise Regional Information Exchange System for multi-national information sharing in support of planning and executing military operations. Supports intelligence and classified information exchange up to Secret Releasable.



B. Information Warfare (IW): The Information Warfare Community employs specific tools and processes to provide the Commander with kinetic and non-kinetic means of achieving key objectives at all levels of operations by effecting adversary, and protecting friendly, decision making-capabilities. Often first on the scene, Navy assets bring great reach and flexibility to the joint Information Operations campaign. Navy platforms deliver the commander's message to maritime, littoral, and leadership audiences, as well as audiences in denied areas. They affect vital networks, protecting friendly assets and impeding adversary Command and Control (C2).

1. Mission: Execute the full spectrum of cyber, cryptology, SIGINT, information operations, computer network operations and electronic warfare missions. This occurs across the cyber, electromagnetic and space domains to deter and defeat aggression, to provide warning of intent, and to ensure freedom of action while achieving military objectives in and through cyberspace.

2. Overview: The IW Community delivers information superiority. This is achieved through the application of Signals Intelligence (SIGINT), Computer Network Operations (CNO) and Electronic Warfare (EW) expertise. Other responsibilities of the Navy IW Community typically include:

- Leading Information Dominance personnel across the spectrum of military operations
- Developing and operating cutting-edge network exploitation and defense systems
- Planning and delivering information warfare effects during exercises and operations

3. Operational Elements:

IW Community members are typically assigned to one of the four National Cryptologic Centers (Hawaii, Texas, Georgia, Maryland). At each one of these Cryptologic Centers the Navy's presence is significant, and identified as a **Navy Information Operations Command (NIOC)**. As the Navy's Center of Excellence for Information Operations (IO), Navy Information Operations Command advances Information Operations war fighting capabilities for Naval and Joint Forces by providing operationally focused training and planning support, developing doctrine, tactics, techniques, and procedures, advocating requirements in support of future effects-based warfare, and managing functional data for Information Operations. NIOCs are organized under Commander, US Tenth Fleet. Within each NIOC is the Fleet Information

Operations Center (FIOC) responsible for support to fleet needs as directed by operational fleet commanders and as specified in the NIOC's mission.

Navy Cyber Defense Operations Center (NCDOC) located in Little Creek, VA, coordinates, monitors, and oversees the defense of Navy computer networks and systems and is responsible for accomplishing Computer Network Defense (CND) missions as assigned by Commander, U.S. Tenth Fleet and Commander, U.S. Cyber Command.

Expeditionary Tactical Information Operations Support (ETIOS) teams are deployable, three-man enlisted teams capable of task organizing to conduct tactical SIGINT electronic warfare (EW)/electronic warfare support (ES) collection, processing, and analysis in direct support of JFMCC or NCC requirements. ETIOS provides EW/SIGINT-derived FP/I&W intelligence to the supported commanders and staffs. Specifically, ETIOS personnel conduct real-time or near-real-time collection operations that include, but are not limited to, search, intercept, identify, exploit, and direction-find communications and non-communications transmissions support to deployed expeditionary forces.

In composite warfare, the **Information Operations Warfare Commander (IWC)** is responsible to shape and assess the information environment, achieve and maintain information superiority, develop and execute IO plans in support of Composite Warfare Commander (CWC) objectives while supporting other warfare commanders.

The **Cryptologic Resource Coordinator (CRC)** is the officer assigned some or the entire Officer in Tactical Command (OTC) detailed responsibilities for management of cryptologic assets, cryptologic coverage and tasking plans, personnel and augmentation requirements, cryptologic direct support operations, signal security operations, direct service interfaces, cryptologic sanitation, and correlation procedures. The CRC should be collocated with the OTC staff and should have representatives in the CWC's SUPPLOT watch area. The alternate CRC should be located on the ship with the best cryptologic resources.

Typically, a senior enlisted Sailor from one of the NIOCs is assigned to the CRC as an assistant CRC. Together, they coordinate the cryptologic effort of the group to which they are attached while receiving support from each unit's SSES Division Officer/SIGWO. Additionally, each sensor platform is assigned an Electronic Warfare Officer to serve as the principal EW planner who develops operation plans (OPLANs) and concept plans (CONPLANs), plans and monitors routine EW operations and activities, and coordinates joint EW training and exercises.

4. IW Components

Electronic Warfare (EW) refers to any military action involving the use of electromagnetic (EM) and directed energy to control the EM spectrum or to attack the adversary. EW includes three major subdivisions: electronic attack (EA), electronic protection (EP), and electronic warfare support (ES). EA involves the use of EM energy, directed energy, or antiradiation weapons to attack personnel, facilities, or equipment with the intent of degrading, neutralizing, or destroying adversary combat capability. EP ensures the friendly use of the EM spectrum. ES consists of actions tasked by, or under direct control of, an operational commander to search for, intercept, identify, and locate or localize sources of intentional and unintentional radiated EM

energy for the purpose of immediate threat recognition, targeting, planning, and conduct of future operations. ES provides information required for decisions involving EW operations and other tactical actions such as threat avoidance, targeting, and homing. ES data can be used to produce SIGINT, provide targeting for electronic or other forms of attack, and produce measurement and signature intelligence (MASINT). SIGINT and MASINT can also provide battle damage assessment (BDA) and feedback on the effectiveness of the overall operational plan.

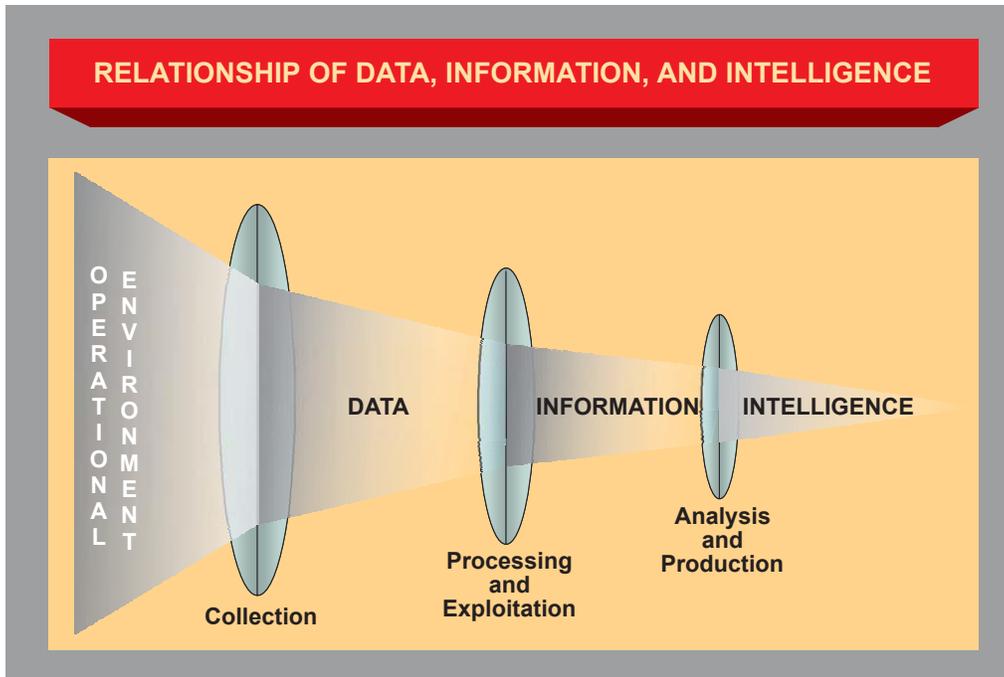
Computer Network Operations (CNO) is one of the latest capabilities developed in support of military operations. CNO, along with EW, is used to attack, deceive, degrade, disrupt, deny, exploit, and defend electronic information and infrastructure. For the purpose of military operations, CNO are divided into Computer Network Attack (CNA), Computer Network Defense (CND), and related computer network exploitation (CNE) enabling operations. CNA consists of actions taken through the use of computer networks to disrupt, deny, degrade, or destroy information resident in computers and computer networks, or the computers and networks themselves. CND involves actions taken through the use of computer networks to protect, monitor, analyze, detect, and respond to unauthorized activity within DOD information systems and computer networks. CND actions not only protect DOD systems from an external adversary but also from exploitation from within, and are now a necessary function in all military operations. CNE is enabling operations and intelligence collection capabilities conducted through the use of computer networks to gather data from target or adversary automated information systems or networks.

Signals Intelligence (SIGINT) is intelligence derived from electronic signals and systems used by foreign targets, such as communications systems, radars, and weapons systems. SIGINT provides a vital window for our nation into foreign adversaries' capabilities, actions, and intentions.

C. Intelligence (INTEL): Naval Intelligence provides evaluated intelligence on an adversary's capabilities and intentions to support planning and operations at all levels of warfare. Intelligence allows anticipation or prediction of future situations and circumstances, and it informs decisions by illuminating the differences in available courses of action. Naval Intelligence provides tactical, operational and strategic intelligence support to U.S. naval forces, joint services, multi-national forces, and executive level decision-makers.

It is important to understand the distinction between *information* and *intelligence*. *Information* is an assimilation of data that has been gathered, but not fully correlated, analyzed, or interpreted. While not fully analyzed or correlated, information still has significant value to the tactical commander and plays a key role in threat warning and target acquisition.

Intelligence, on the other hand, is the product resulting from the collection, exploitation, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. Integration and analysis, combined with a thorough understanding of mission requirements, convert information into usable intelligence. Thus, intelligence is the product we derive from analyzing all available and relevant information.



Today’s technology enables commanders and their staffs to access in near-real-time, very large amounts of information relating to every aspect of the operational environment — the composite of the conditions, circumstances, and influences that affect the employment of capabilities and bear on the decisions of the commander. Information will be available throughout the joint force covering an extremely wide range of matters relating to friendly, neutral, and enemy forces and the civilian populace. There will also be an equally large volume of information concerning weather, terrain, cultural influences, and other aspects of the operational environment. This mass of information, when subjected to an analytical process, can be distilled into intelligence to support a predictive estimate of adversary capabilities and intentions. It is this predictive nature of intelligence that distinguishes it from the mass of other information available to the commander.

1. Levels of Intelligence:

- a. Strategic Intelligence
- b. Operational Intelligence
- c. Tactical Intelligence

STRATEGIC
Senior Military and Civilian Leaders
Combatant Commanders

- Assist in developing national strategy and policy
- Monitor the international situation
- Assist in developing military plans
- Assist in determining major weapon systems and force structure requirements
- Support the conduct of strategic operations

OPERATIONAL
Combatant and Subordinate Joint Force
Commanders and Component Commanders

- Focus on military capabilities and intentions of enemies and adversaries
- Monitor events in the Joint Force Commander’s area of interest
- Support the planning and conduct of joint campaigns
- Identify adversary centers of gravity

TACTICAL
Commanders

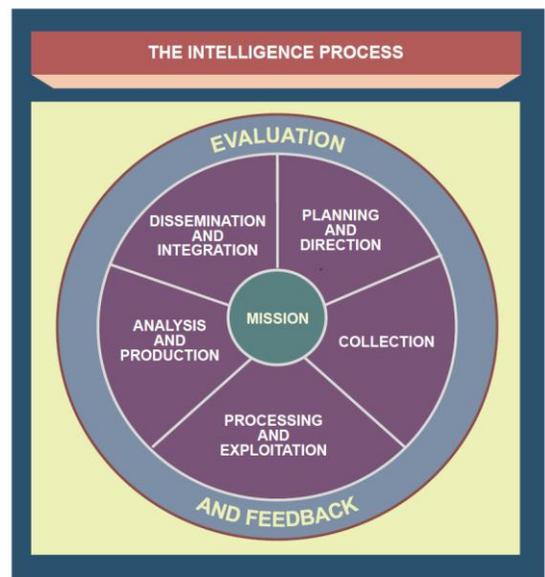
- Support planning and conducting battles and engagements
- Provide commanders with information on imminent threats to their forces
- Provide commanders with obstacle intelligence

GEOINT -- Geospatial Intelligence	
-- Imagery	
-- IMINT - Imagery Intelligence	
-- Geospatial Information	
HUMINT -- Human Intelligence	
-- Debriefings	-- Source Operations
-- Interrogation Operations	-- Document and Media Exploitation
SIGINT -- Signals Intelligence	
-- COMINT - Communications Intelligence	
-- ELINT - Electronic Intelligence	
** Technical ELINT	
** Operational ELINT	
-- FISINT - Foreign Instrumentation Signals Intelligence	
MASINT -- Measurement and Signature Intelligence	
-- Electromagnetic Data	-- Radio Frequency Data
-- Geophysical Data	-- Radar Data
-- Materials Data	-- Nuclear Radiation Data
OSINT -- Open-Source Intelligence	
-- Academia	-- Media Broadcasts
-- Interagency	-- Internet
-- Newspapers/Periodicals	
TECHINT -- Technical Intelligence	
CI -- Counterintelligence	

- 2. Intelligence Sources, i.e., the “INTs”:**
- Geospatial Intelligence (GEOINT)
 - Human Intelligence (HUMINT)
 - Signals Intelligence (SIGINT)
 - Measurement and Signature Intelligence(MASINT)
 - Open-Source Intelligence (OSINT)
 - Technical Intelligence (TECHINT)
 - Counter Intelligence (CI)

3. The Intelligence Process/Cycle: The intelligence process is comprised of a wide variety of interrelated intelligence operations which must focus on the commander’s mission and concept of operations.

- Planning and Direction - the identification of a need for intelligence regarding all relevant aspects of the battlespace, especially the adversary.
- Collection - tasking appropriate collection assets and/or resources to acquire the data and information required to satisfy collection objectives.
- Processing and Exploitation - the collected raw data is transformed into information that can be readily disseminated and used by intelligence analysts to produce multidiscipline intelligence products.
- Analysis and Production - integrating, evaluating, analyzing, and interpreting information from single or multiple sources into a finished intelligence product.
- Dissemination and Integration - properly formatted intelligence products are disseminated to the requester, who integrates the intelligence into the decision-making and planning processes.



4. Functions of Naval Intelligence: Naval intelligence reduces risk to operations by identifying adversary capabilities, vulnerabilities, and intentions. It attempts to impart thorough knowledge of the situation through the application of the following basic intelligence functions that form the foundation of required analytical support to the commander.

a. Intelligence Preparation of the Battlespace. Intelligence Preparation of the Battlespace (IPB), sometimes also referred to as the **Intelligence Preparation of the Operating Environment (IPOE or Joint: JIPOE)**, is the systematic and continuous analysis of the adversary, terrain, and weather in the assigned or potential battlespace. Its goals include understanding the adversary's forces, doctrine, tactics, and probable courses of action, together with the physical and environmental characteristics of the target area. IPB identifies gaps in knowledge that require intelligence collection efforts. It consists of five elements:

- *Define the Battlespace/Operating Environment:* Defines the area of operations and focuses intelligence assets on the battlespace.
- *Describe the Battlespace's Effects:* Evaluates physical characteristics of the battlespace and their effects on friendly and adversary capabilities to maneuver, attack, employ sensors, and communicate.
- *Evaluate the threat:* Encompasses a detailed study of the threat, identifying adversary capabilities and vulnerabilities.
- *Determine Threat Courses of Action:* Ties the previous steps together providing a predictive analysis of probable adversary courses of action and friendly force survivability in each case.

IPB is of great importance to all aspects of combat planning. We use IPB to plan action and manage the risk to friendly forces. Risk will always be inherent in military operations, but IPB seeks to reduce that risk. We assess risk by weighing adversary capabilities and intentions against friendly forces and assigned missions. This risk is then analyzed to determine whether additional information or intelligence could alleviate it. Our management of risk thus depends on a clear understanding of both what is known and what is not known.

b. Indications and Warning. The goal of Indications and Warning (I&W) is to provide early warning of potential hostile action. To accomplish this goal, intelligence must convey understanding of the adversary. This understanding is gained through IPB and allows us to interpret indications, thus allowing adequate warning. I&W prevents surprise and reduces risk by detecting adversary actions that may threaten friendly forces. It can support strategic, operational, or tactical levels of warfare. By focusing on reduction of surprise and threat avoidance, I&W supports operational and tactical commanders.

c. Targeting. Targeting is a function of intelligence and operations, by which an adversary's critical vulnerabilities are identified for possible attack or disruption. The primary goal of targeting is to enable us to use resources effectively in defeating the adversary. Targeting is more than a function of planning the physical destruction of enemy facilities. Targeting is an analysis process in which the components of a target, or target system and their vulnerabilities and relative importance are assessed to determine what effect their loss or impairment would have on the adversary. Intelligence can indicate where selective employment of force can have a major effect.

D. Meteorology/Oceanography (METOC) – Both the terms “OCEANO” and “METOC” are used to refer to the Oceanography community which provides actionable information to include meteorological, climatological, oceanographic, and space environment observations, analyses, prognostic data or products and meteorological and oceanographic effects.

1. Community Overview

Naval Oceanography is about generating competitive advantage across the warfighting and shaping spectrum through **Battlespace on Demand (BonD)**. BonD, is a strategic concept that consists of three tiers, each of which builds on the previous tier to ultimately produce enhanced decision-making capabilities for the warfighter. It is the framework used to inform our operational and technical domains, drives our investment strategy and enables us to keep the Fleet safe, and enhance warfighting effectiveness by achieving decision superiority.



Tier 0: Data from various sources are collected, assimilated and fused to provide initial and boundary conditions that accurately describe the current ocean and atmosphere environment, as well as the celestial and temporal reference frames.

Tier 1: Data from satellites, altimetry, gliders, buoys and other collection methods are incorporated to initialize computations. Then, our high performance supercomputers run complex models to continually forecast and verify the future state of the ocean and atmosphere.

Tier 2: The environment modeled in Tier 1 will impact sensors, weapons, platforms and people, providing opportunities and restrictions for operations and warfighting. We define the influences on planning, force structure, targeting, timing, maneuver, tactics, techniques and procedures. The result is a “performance surface” that accounts for both the predicted environment and the capabilities and behaviors of the force – both allies and adversaries.

Tier 3: Performance surfaces are applied to specific decision-making processes to quantify risk and opportunity at strategic, operational and tactical levels. We provide actionable recommendations on force allocation and employment that directly enhance safety and warfighting effectiveness.

2. Organization

a) Commander, Naval Meteorology and Oceanography Command

Mission: Commander, Naval Meteorology and Oceanography Command (CNMOC) provides critical information from the ocean depths to the most distant reaches of space, meeting the needs of our military, scientific, and civilian communities.

Functions: Naval Meteorology and Oceanography Command is the Type Commander for the Navy's oceanographic forces worldwide to include 340 officers, 950 Aeroographer's Mates, 1300 civilians, 6 oceanographic survey ships, and various survey aircraft, hydrographic survey craft, and autonomous underwater vehicles.

b) Production Centers

The **Fleet Numerical Meteorology and Oceanography Center** (FNMOC) uses high performance computing to provide high quality, relevant and timely worldwide meteorology and oceanography support to U.S. and coalition forces from its Operations Center in Monterey, California.

The **Naval Oceanographic Office** (NAVO) maximizes seapower by applying relevant oceanographic knowledge in support of U.S. National Security. NAVO leverages a wide range of collection assets deployed globally to accomplish its mission. NAVO is located at Stennis Space Center, Mississippi.

c) Other Fleet Supporting Components

The **U.S. Naval Observatory** (USNO) provides a wide range of astronomical data and products and serves as the official source of precise time for the U.S. Department of Defense and a standard of time for the entire United States. USNO is located in Washington, DC and Flagstaff, AZ.

The **Joint Typhoon Warning Center** (JTWC), located at Pearl Harbor, Hawaii, is the U.S. Department of Defense agency responsible for issuing tropical cyclone warnings for all forces operating in the Pacific and Indian Oceans.

The **Naval Oceanography Operations Command** (NOOC) advises Navy operations on the impact of ocean and atmospheric conditions in for every operation in every theater of operations. NOOC products include those from the **Fleet Weather Centers** in Norfolk, Virginia and San Diego, California and the Naval Oceanography ASW Center – Yokosuka, Japan.

3. Warfare Directorates

Four Warfare Directorates have been established to support the warfighter across eight warfare areas. The directorates include:

- Undersea Warfare:
 - Anti-Submarine Warfare: Focused on forward presence with reachback support, personnel in the ASW Directorate are using state of the art technology to capture the characteristics of the water column and turn that data into usable information for the warfighter. Billets are worldwide, both ashore and afloat.
 - Mine Warfare: Focused on all facets of MIW. METOC officers are expected to learn a myriad of skills including UUV employment, side scan sonar interpretation, and advanced MIW planning. Billets are worldwide, both ashore and afloat.
- Expeditionary Warfare: Focused on providing Naval Special Warfare with sea, air and land (SEAL) high ground information by defining the physical environment to optimize mission

planning for tactical advantage. Deployments with SEAL teams are common, requiring outstanding physical fitness and an ability to conduct METOC support operations in remote locations.

- Weather Services:
 - Fleet Operations: Focused on METOC support for afloat units. Officers are generally attached to a specific ship (LHD/LHA/CVN), Strike Group and Numbered Fleets and will conduct normal deployments. Opportunities exist for deployments to joint task forces or similar staffs.
 - Maritime Operations: Responsible for providing enroute weather (WEAX) and Optimum Track Ship Routing, a service designed to keep ships safely away from hazardous weather, to afloat units. Officers in this directorate initially qualify as maritime forecasters enroute to final qualification as a "Ship Router". These positions are located in Norfolk and San Diego.
 - Aviation Operations: Focused on flight weather support to air forces around the world to support safety of flight. Billets are worldwide to include two joint USAF/USN weather centers in Sembach, Germany and Pearl Harbor, HI.
- Precise Time and Astrometry:
 - Navigation: Focused on providing hydrographic surveys supporting real world operations, as identified by Combatant Commanders and other DOD customers. Consisting primarily of USNS hydrographic survey vessels and the Fleet Survey team, their combined objective is to deliver digital and/or paper navigation products within a single deployment (45-60 day turnaround). They operate state of the art side-scan and multi-beam sonar technologies, GPS, and modern hydrographic survey launches (HSLs). Officers in this directorate are trained in the art and science of hydrography and deploy around the world as coastal and harbor survey units.
 - Positioning and Timing: The Naval Observatory and is the preeminent authority in the areas of Precise Time and Astrometry, and distributes Earth Orientation parameters and other Astronomical Data required for accurate navigation and fundamental astronomy.