



# ISR/IO Department Overview

Greg Shaffer

SSC-Pacific ISR/IO Department Head  
SPAWAR National Competency Lead for ISR/IO

**561 – Information Operations**  
**562 - ISR**

**564 - Maritime Systems**



- **Services Oriented Architecture w/ Common Data Standards**
- **Sensors as service providers in an IP based, web-enabled, publish/subscribe environment**
- **Cross – Domain / Cross – Platform**
- **National and Tactical**
- **Ubiquitous — Strategic, Theater, Tactical, Organic**
- **User-Centric — Networked, Autonomous, Timely**

**ISR/IO from Seabed to Space - Throughout Cyberspace**

# ISR/IO Competency Definition

- ▼ The Intelligence, Surveillance and Reconnaissance (ISR) and Information Operations (IO) competency includes the scientific and engineering knowledge for the planning and conduct of research, development, system engineering, manufacturing, test and evaluation, acquisition support and in-service engineering for **ISR, IO, Meteorological and Oceanographic (METOC), Autonomous Systems, Cyberspace Operations**, and supporting infrastructure/enabling technologies which can be applied to support these areas.
  - ... **sensing, detection and collection, measurement**, mission planning, modeling and simulation, **classification and localization, fusion, object identification**, processing and **exploitation, analysis and production** ...
  - ... **influence, disrupt, corrupt, or usurp** the decision-making of adversaries...
  - ... **observation, characterization and prediction of the environment** (atmospheric and oceanographic), bathymetric data, **propagation of ocean effects** and the effects of environmental factors on **prediction of sensor performance**...
  - ... **unmanned intelligence gathering, surveillance, and reconnaissance in various physical domains** (undersea, on land, in the air, in space, and in the maritime domain) ...
  - ... **Offensive Cyber Operations (OCO), Computer Network Exploitation (CNE)**...

# Achieving CNO's Information Dominance Vision

## *Information Dominance and the U.S. Navy's Cyber Warfare Vision*

VADM Jack Dorsett  
DCNO for Information Dominance  
April 14, 2010



## CNO's Unifying Vision and Guiding Principles

*Vision – "Pioneer, field and employ game-changing capabilities to ensure Information Dominance over adversaries and Decision Superiority for commanders, operational forces and the nation."*

### First Principles include:

- ✓ Every platform is a sensor
- ✓ Every sensor is networked
- ✓ Build a little; test a lot
- ✓ Spiral development/acquisition
- ✓ Plug-n-play sensor payloads
- ✓ Reduce afloat/airborne manning
- ✓ Transition to remoted, automated
- ✓ Collectors dynamically tasked
- ✓ One operator control multiple platforms
- ✓ Data discoverable and accessible
- ✓ Missions drive requirements
- ✓ UAS's increasingly sea-based
- ✓ Commonality in interfaces, data links and control stations
- ✓ Every shooter capable of using target data derived from any sensor
- ✓ Emphasize UAS / RPV and autonomous platforms

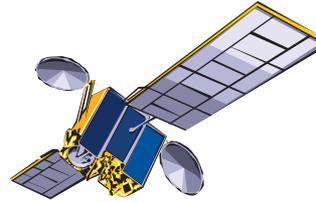
# Battlespace Awareness Portfolio

SSC PAC Portfolio Manager: Bryan Tollefson

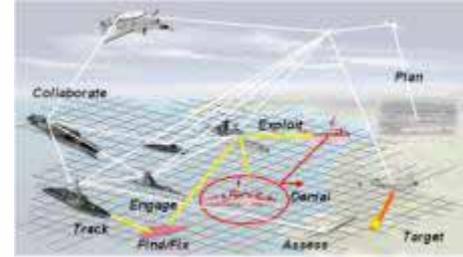


## Scope of Portfolio:

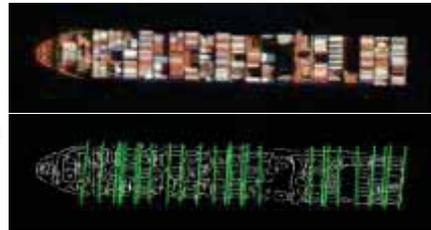
Includes engineering development and engineering services for systems and organizations that observe adversaries, collect data, and process it into information and intelligence. Includes systems that deny and deceive adversary's ability to collect data and interactions with the physical domain - data acquisition and processing - required to bring these observations into the digital world.



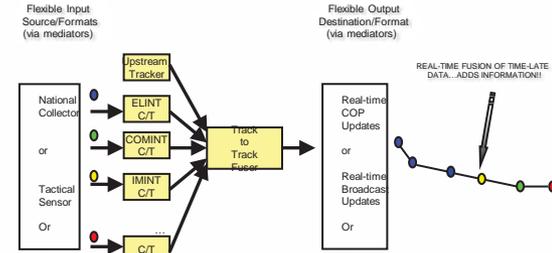
Space & National Systems



SSEE Inc F



Automated Imagery Analysis



Multi-Int Data Fusion/ Integration

## Unique Capabilities:

- ✓ Maritime Domain Awareness
- ✓ ISR
- ✓ IO
- ✓ Autonomous Systems ; UxVs
- ✓ SIGINT
- ✓ Multi-Int Data Fusion / Integration
- ✓ Automated Threat Detection



ISR for Unmanned Systems for All Warfare Domains

Information Is the Weapon

# Integrated Cyber Operations

SSC PAC Portfolio Manager: Josh Caplan



## Scope of Portfolio:

Cyber involves a close coupling of computer network defense, computer network exploitation, and computer network attack development and engineering. Enables U.S. forces to maneuver in the cyber domain while denying adversary's ability to do the same and simultaneously protecting U.S. critical infrastructure and information. Includes network security, red teaming, and exploit/attack tool development.



Computer Network Defense Afloat (CND-A)



Convergence of Networks & Technology

## Unique Capabilities:

- ✓ Managing Security Risks
  - IA requirements analyses
  - Risk mitigation strategies
- ✓ Security Architecture Engineering
- ✓ Afloat CND/IA assessments
- ✓ PKI support for non-NMCI networks
- ✓ MLS/CDS Solutions
- ✓ SIGINT/IO Engineering



High Assurance Internet Protocol Encryptor (HAIZE)



Tactical Key Loader (TKL)

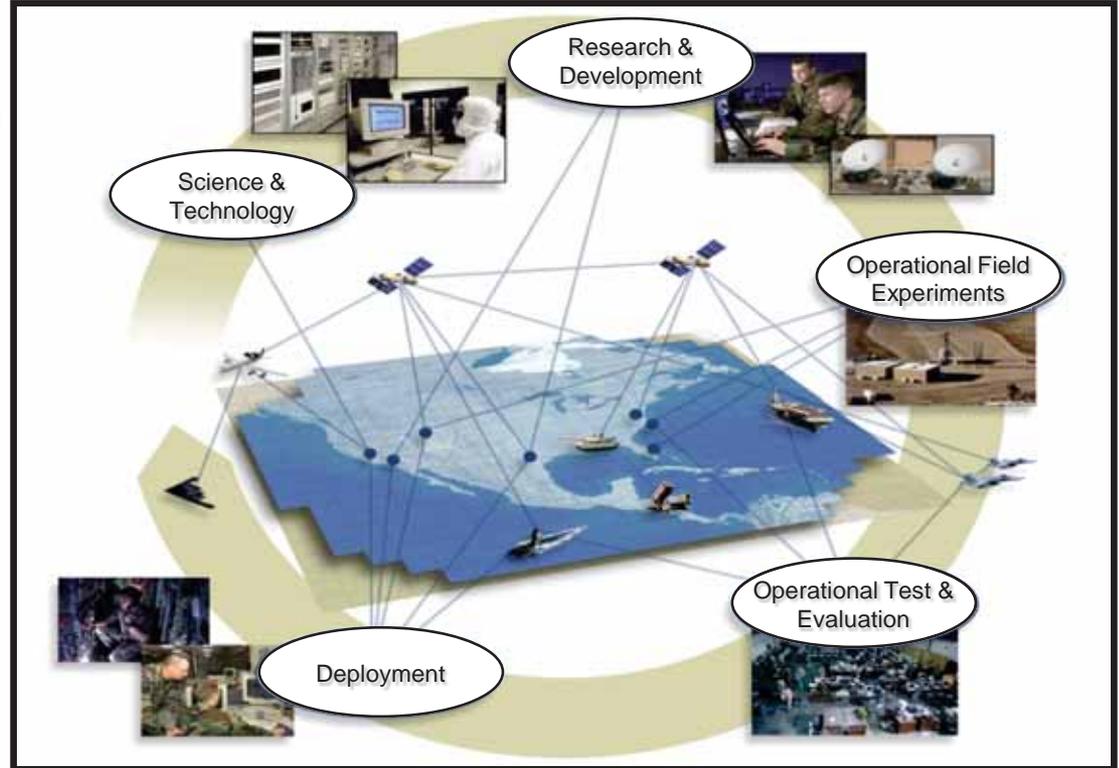


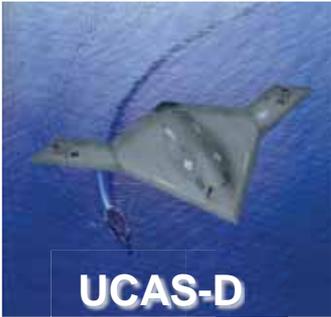
Compact Encryption And Line-Interconnect Circuitry for Information Assurance in Networking (CEALICIAN)

*Alignment with OPNAV N2/N6 and FCC/C10F Priorities*

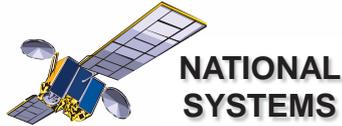
### “Leveraging the Information Environment”

- **EW / ES (SIGINT)**
  - Tactical Cryptologic Systems (TCS)
- **Cyber**
  - Bringing SIGINT to the Fight
  - CNO / CNE
- **Military Deception / Military Information Support Operations**
- **Service Based Environment**
  - Ozone Widget Framework (OWF)
  - APPS for the Warfighter
- **Science & Technology (S&T)**
  - Cognitive IO
  - Network exploitation
- **Information Technology**
  - System Engineering Support
  - Analysis
  - Data Fusion
  - Modeling and Simulation
- **Dept of Homeland Security (DHS)**

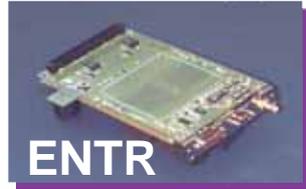




**UCAS-D**



**NATIONAL SYSTEMS**



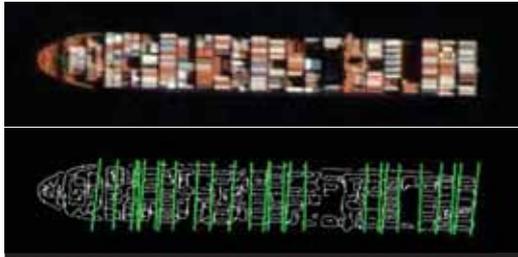
**ENTR**



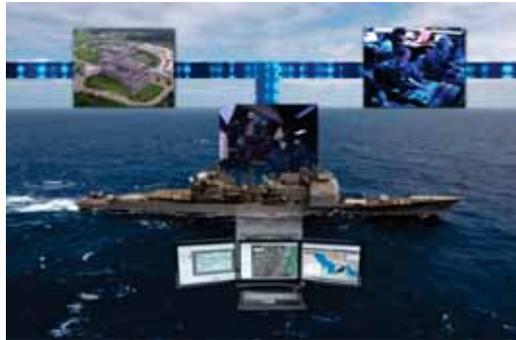
**MASINT/ Unattended Ground Sensors**



**BAMS UAS Interoperability**



**Automated Imagery Analysis**



**Intelligence Carry-On Program (ICOP)**



**Special Tracking systems**

- Developing and fielding innovative sensor networks, collection management, knowledge discovery, and ISR dissemination systems
- Focused on providing the warfighter with the right info, in the right format, of the right bandwidth, on a tactically relevant timeline
- Extracting all of the meaning from the data
- Dissemination that supports Speed of Decision
- Governance, Standards, and Design to ensure Net-Centricity

