



Transforming Tomorrow's Navy

***Tomorrow's Information Advantage
Industry Day Briefing
for BAA 03-007***

28 May 2003

***Gary Toth
Program Officer,
Command and Control and Combat Systems
Office of Naval Research***



Network Centric Warfare

“ Network centric warfare is military operations that exploit information and networking technology to integrate widely dispersed human decision makers, situational and targeting sensors, and forces and weapons into a highly adaptive, comprehensive system to achieve unprecedented mission effectiveness. ”

Network-Centric Naval Forces, Naval Studies Board, National Research Council, 2000

NCW Tenets:

- A robustly networked force improves information sharing
- Information sharing enhances the quality of information and shared situational awareness
- Shared situational awareness enables collaboration and self-synchronization and enhances sustainability and speed of command
- These, in turn, dramatically increase mission effectiveness



Information Advantage

- Achieved by networking the physical, information and cognitive domains
 - Physical domain
 - Robustly networked to achieve secure, seamless connectivity
 - Information Domain
 - Capability to collect, share, access and protect information
 - Capability to correlate, fuse, and analyze data
 - Cognitive domain
 - Capability to develop and share situational awareness
 - Capability to develop a shared knowledge of the commander's intent
 - Capability to self-synchronize operations



NCW is a Major Change

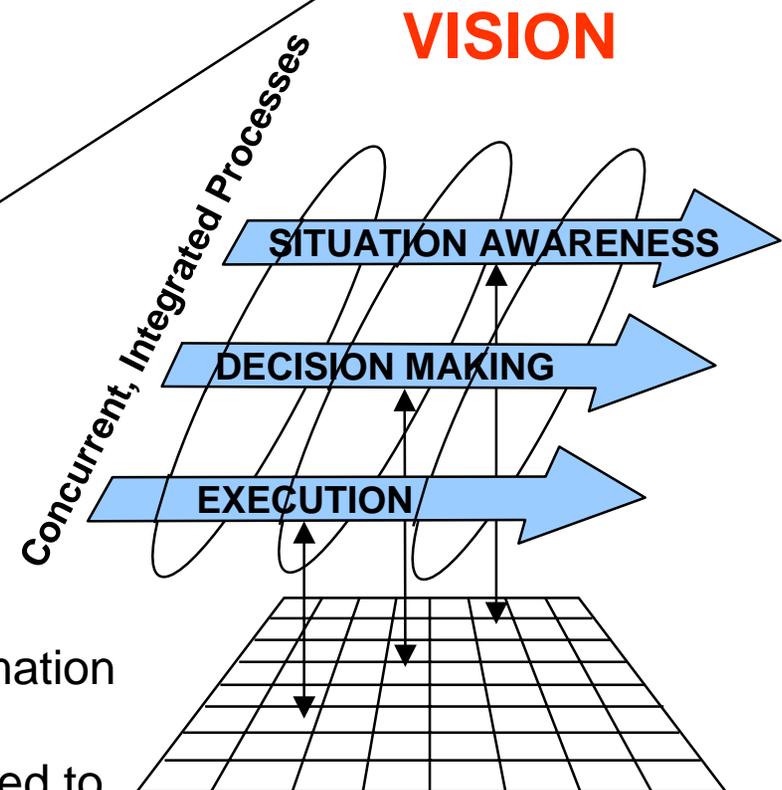
Operational Processes and Effectiveness



Sequential Processes
Information Movement via
Message Limited Awareness
of Situation Limited Cross-
Functional Awareness
Limited Ability to Adapt in
Real Time

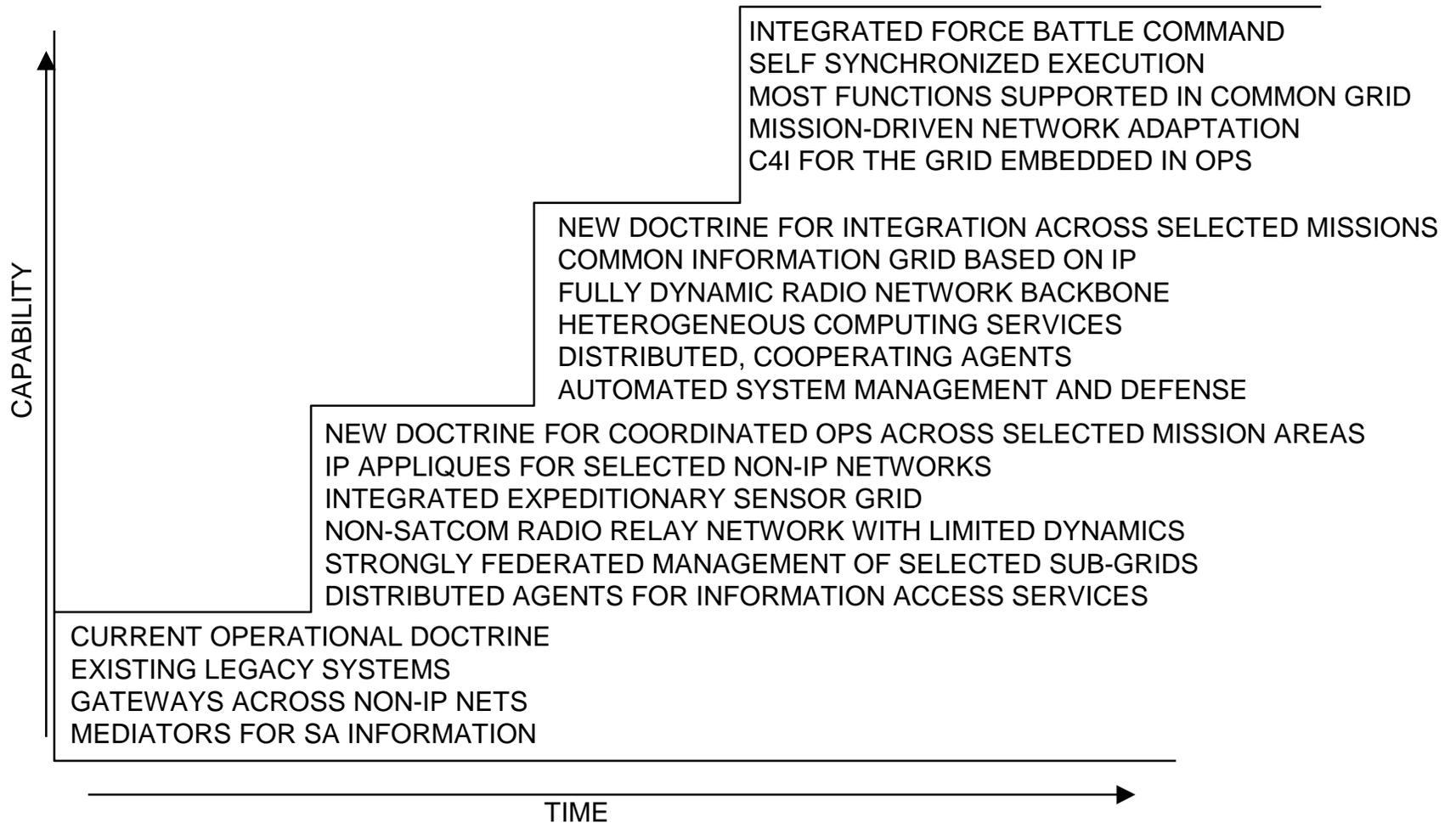
NOW

Concurrent Processes
Common, Consistent Information
via the Grid
Situation Awareness Matched to
Need
Ability to Self-Synchronize
Real Time Adaptation/Deconfliction





Requirements Anticipated





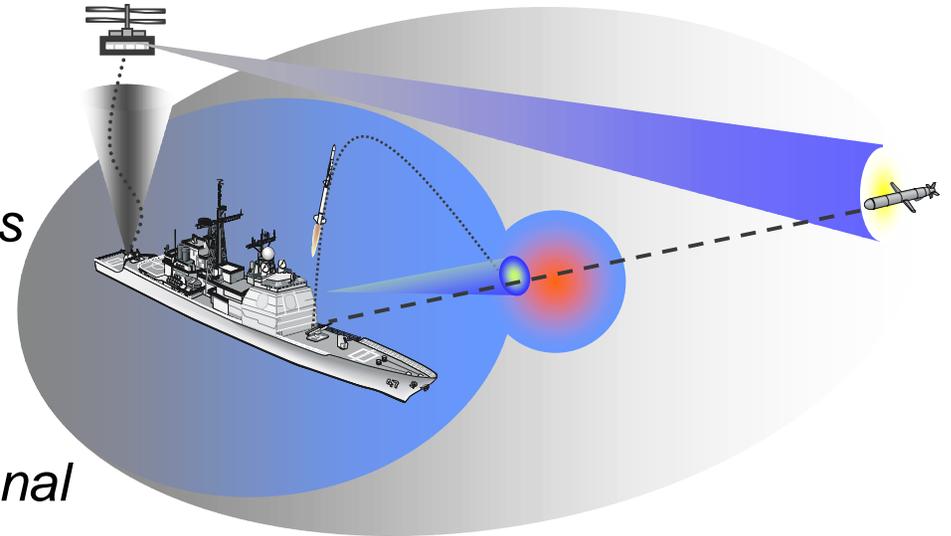
FORCEnet

*Network Centric Warfare
is the theory.*

*Net-Centric Operations
is the concept.*

*FORCEnet is the process
of making the theory
and concept a reality.*

*“FORCEnet is the operational
construct and architectural framework
for Naval Warfare in the Information
Age which integrates Warriors,
sensors, networks, command and
control, platforms and weapons into a
networked, distributed combat force,
scalable across the spectrum of conflict
from seabed to space and sea to
land.”**



*CNO's Strategic Study Group - XXI definition
from 22 July 02 CNO Briefing



What is a fully netted force?

“The right info to the right place at the right time.”

- Enabling Sea Strike, Sea Shield and Sea Base warfighters
- Building a path to Joint network centric warfare
- Maximizing Joint network capability & battlespace awareness
- Minimizing stand-alone, redundant systems by end of FYDP



What will FORCEnet Provide?

FORCEnet benefits are:

- Increased speed and precision of command
- Distributed self-synchronization
- Flexibility and adaptability to operational situations
- Decision superiority

Maximize Combat Capabilities



Building FORCEnet Capability

Expeditionary,
multi-tiered
sensor and weapon
information

Dynamic, multi-path
and survivable
networks

Human-centric
Integration

FORCEnet

*Working
Towards
Information
Weapons*

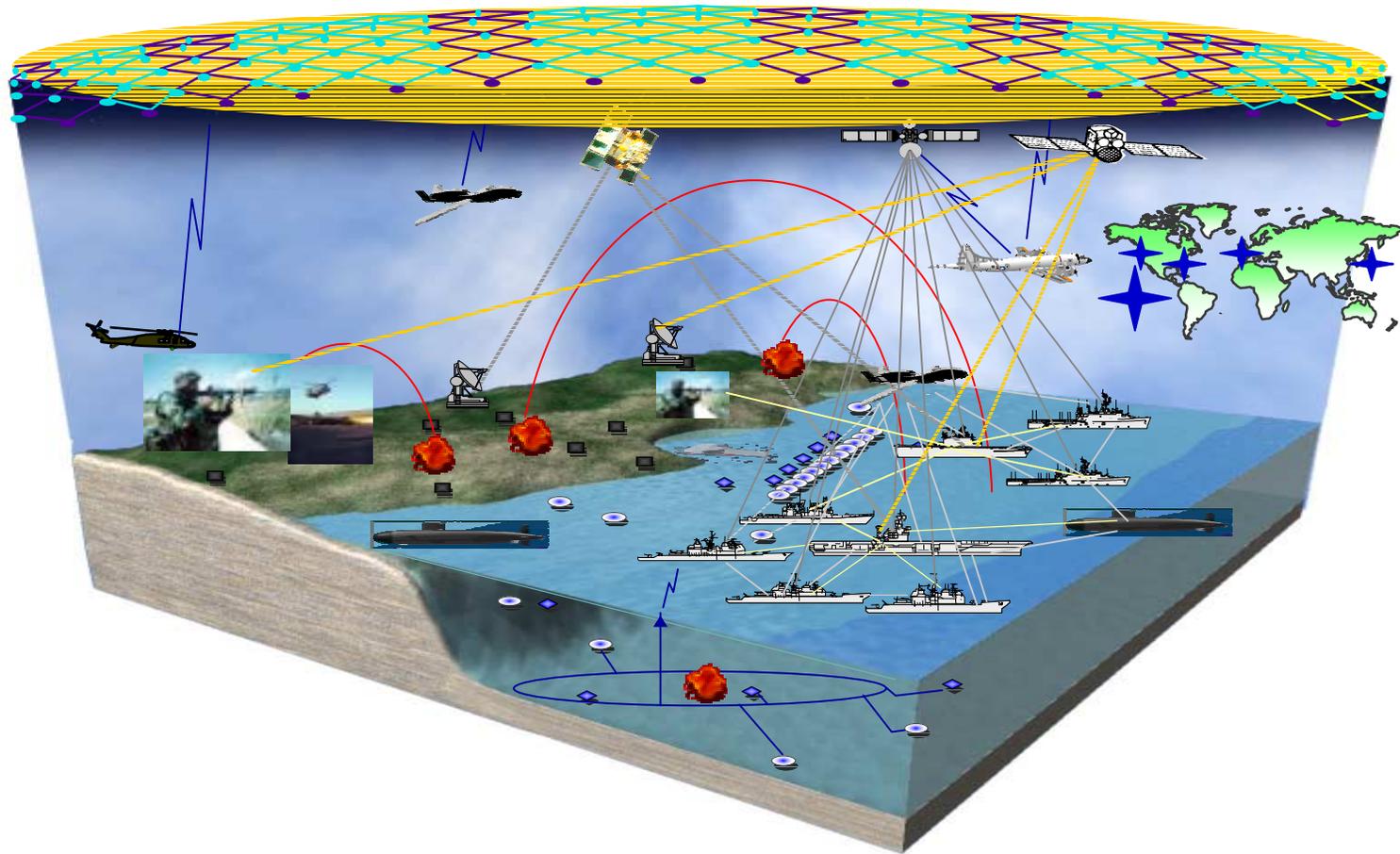
Distributed,
collaborative
command &
control

Adaptive /
automated
decision aids



C2 & CS Program Goals

Develop the science and technology enablers for decision making and mission execution to achieve battlespace superiority





Goal

- Achieving a high level of situation awareness at all levels of warfare
 - Strategic
 - Operational
 - Tactical
- For all forces
 - Joint
 - Naval
 - Coalition
 - Combined



Focus

- Advanced approaches for processing and integrating information from disparate sources
- Optimal decision aids incorporating
 - Rigorous decision theory
 - Automated inference and reasoning
- Assuring information integrity and availability



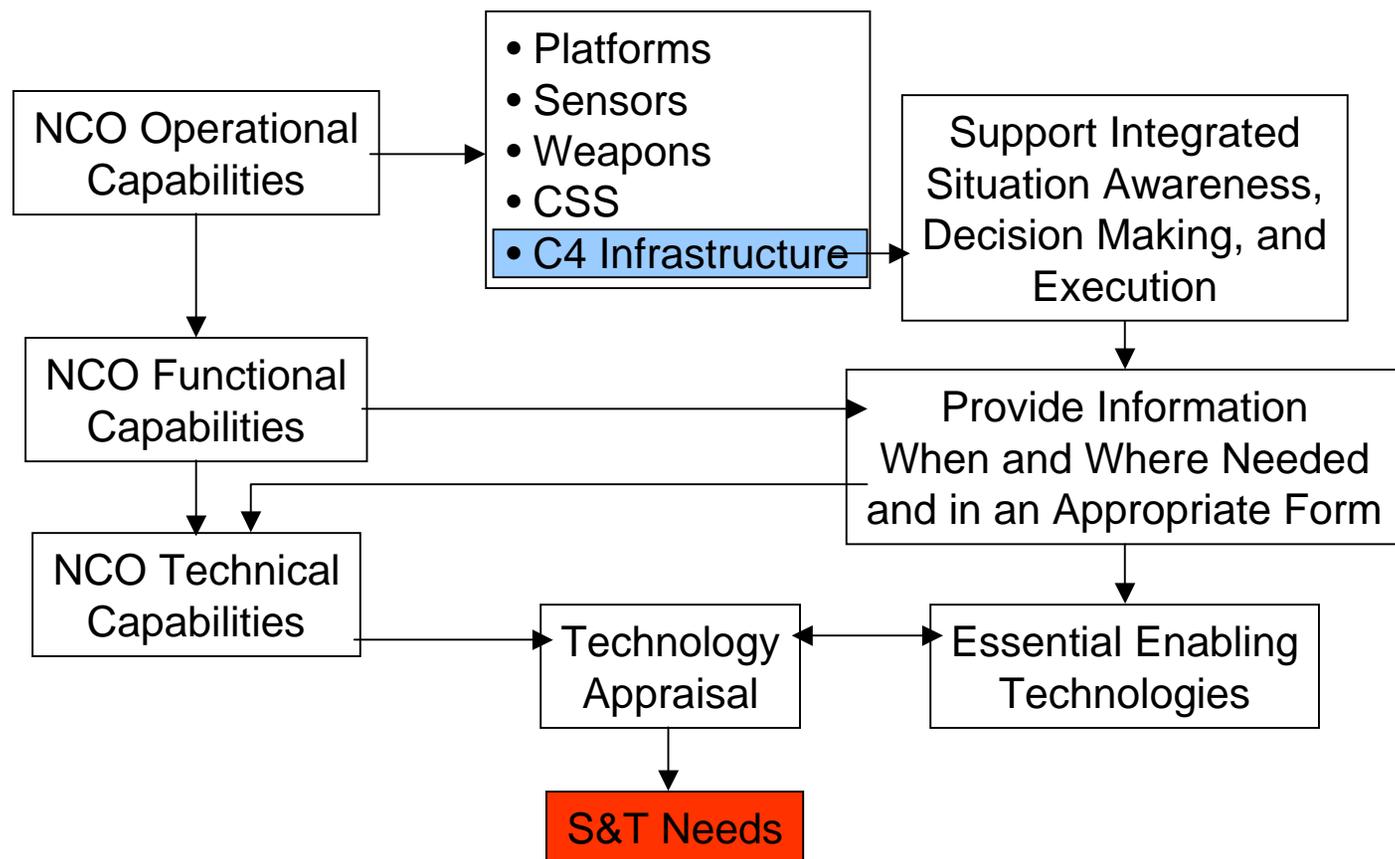
Three Thrust Areas

- **Increased Speed and Precision Decision Making**
 - Automated Image Understanding
 - Automated integration of disparate sensors and sources of information
 - Presentation for rapid understanding
 - Automated Reasoning to develop alternate Courses of Action
- **Information Assurance**
 - Network Protection (Insider Threats)
 - Information Integrity
 - Information Availability
- **Mission Focused Quality of Service**
 - Latency and priority for tactical tasks/activities
 - Contention in a complex multi-objective environment



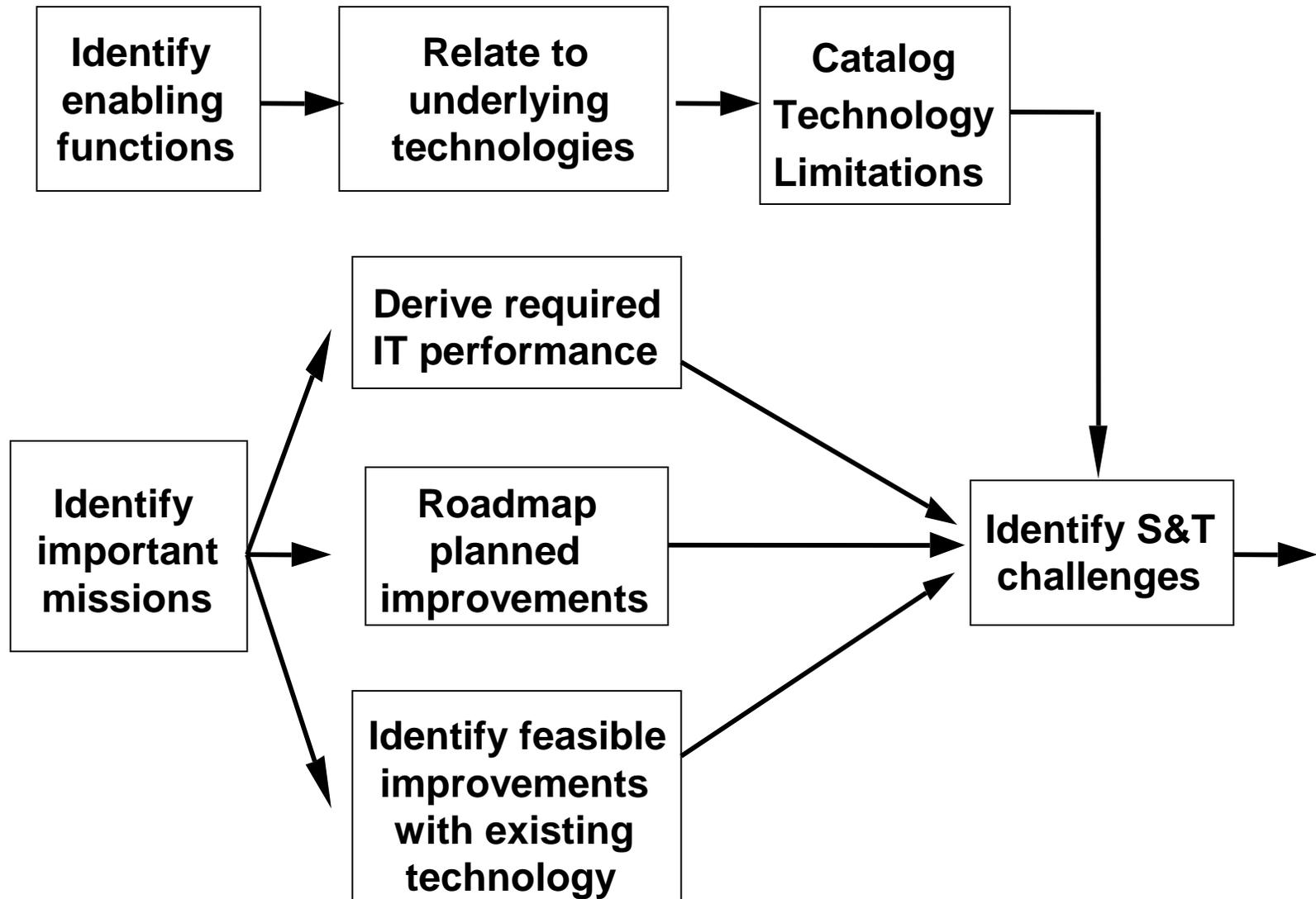
NCO Infrastructure Objectives and Required S&T

- The process for definition:





NCW Taxonomy Methodology





Increased Speed and Decision Making (1)

- Automated Image Understanding
 - Current imagery analysis
 - Primarily manual
 - Time consuming
 - Time critical operations and autonomous operations require automated approaches

- Candidate projects
 - Automatic feature and object recognition
 - Automatic image registration for single and multimodal images, maps
 - Imagery supported navigation
 - Feature/object based compression to maximize bandwidth utilization



Acquired Data

Registration is Key





Multichannel Registration

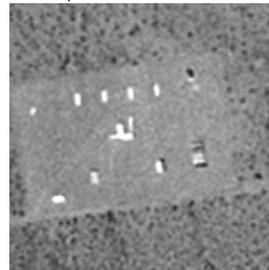
Color Image (Spring 1997)



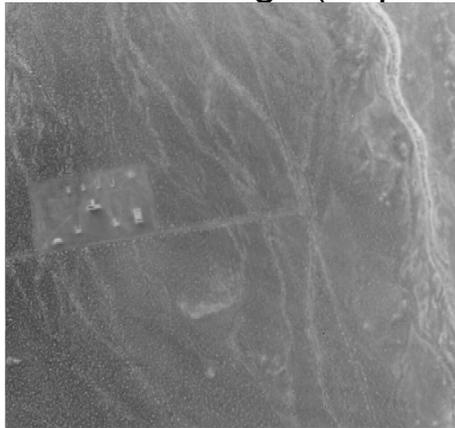
Extracted Regions of Interest



Color to Grayscale



Mid-Wave IR Image (Sep. 1997)



- Automated Registration
- No pre-designated control points
- Additional refinement needed
 - Offsets evident
 - Affine transformations not planar projective

Registered Visible & IR Images





Registered Mosaic

UAV Video : Constrained Looks

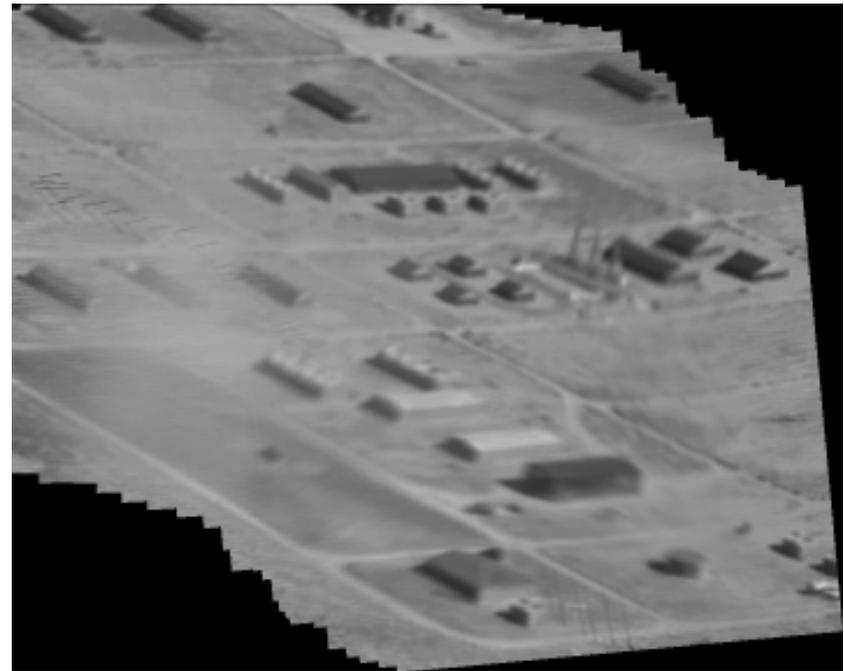
Frame 3

Frame 20

Frame 45

Frame 58

To a Global View



Registered 58 Frame Mosaic

- Shape (Level Sets)
- Velocities
- Affine Transformations

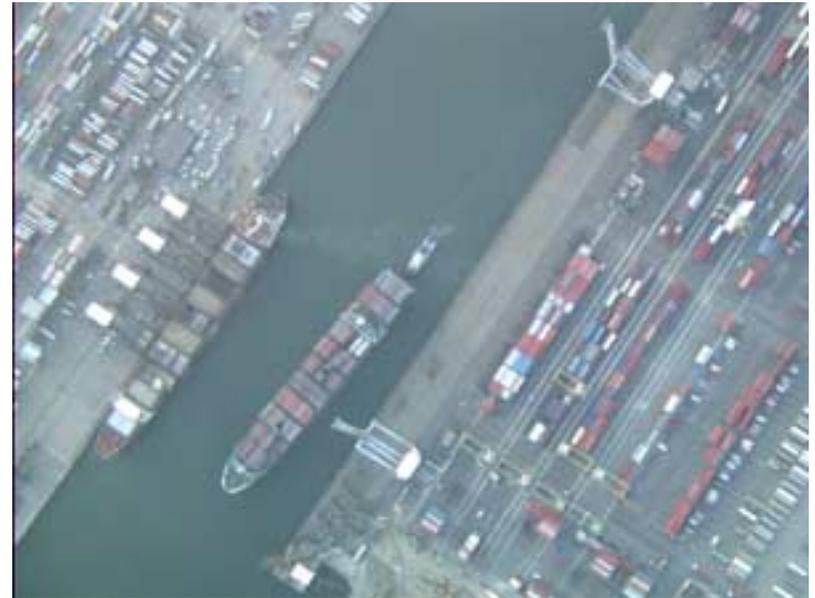


Two Passes over Same Area

First Pass



Return Pass



This shows two passes over the same area. This ship has moved. When first seen it is opposite a docked ship loaded with containers. In the second view it has moved and is now across from the nearly empty container ship that was only coming into the field of view during the first pass.

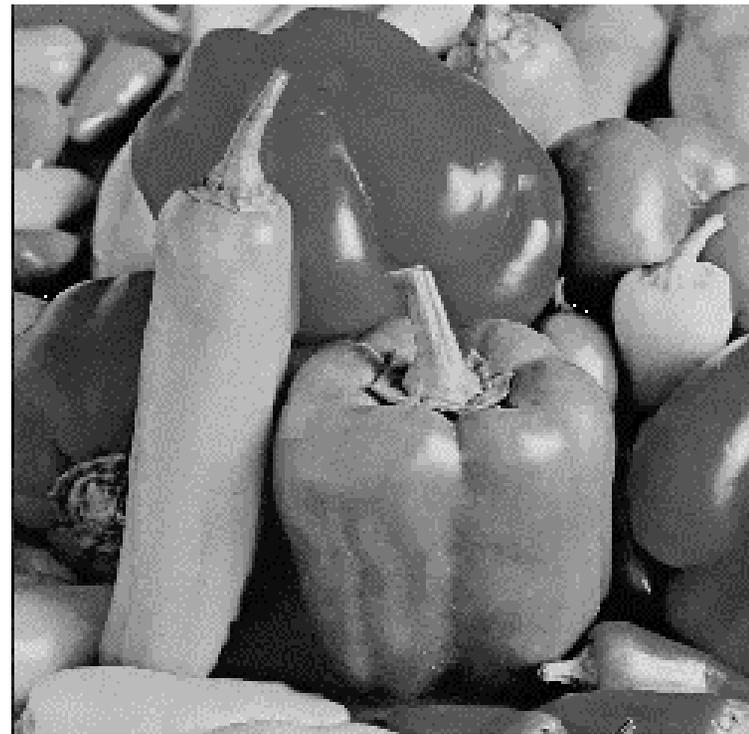
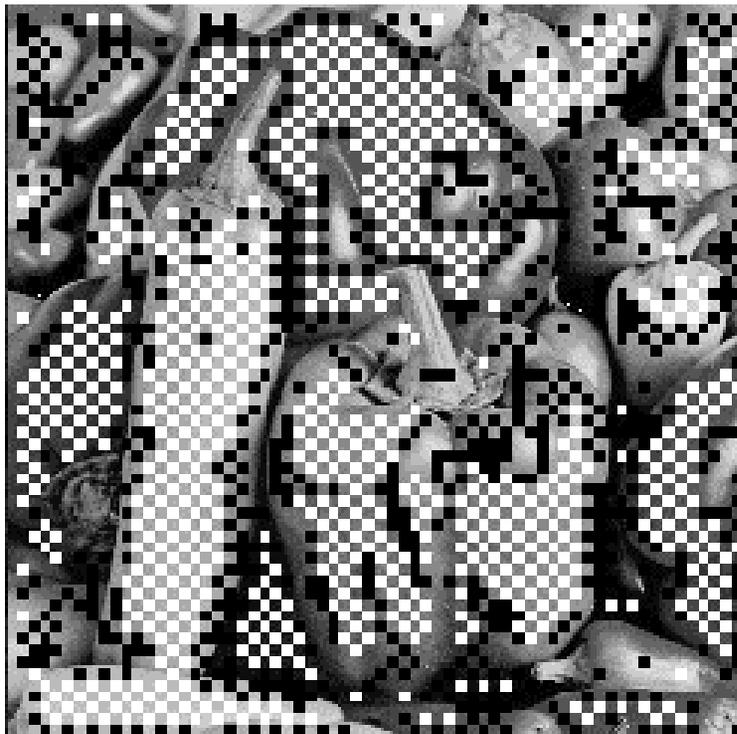


Video Frame Registration to Reference Image





Image Coding Using Structure and Texture Inpainting





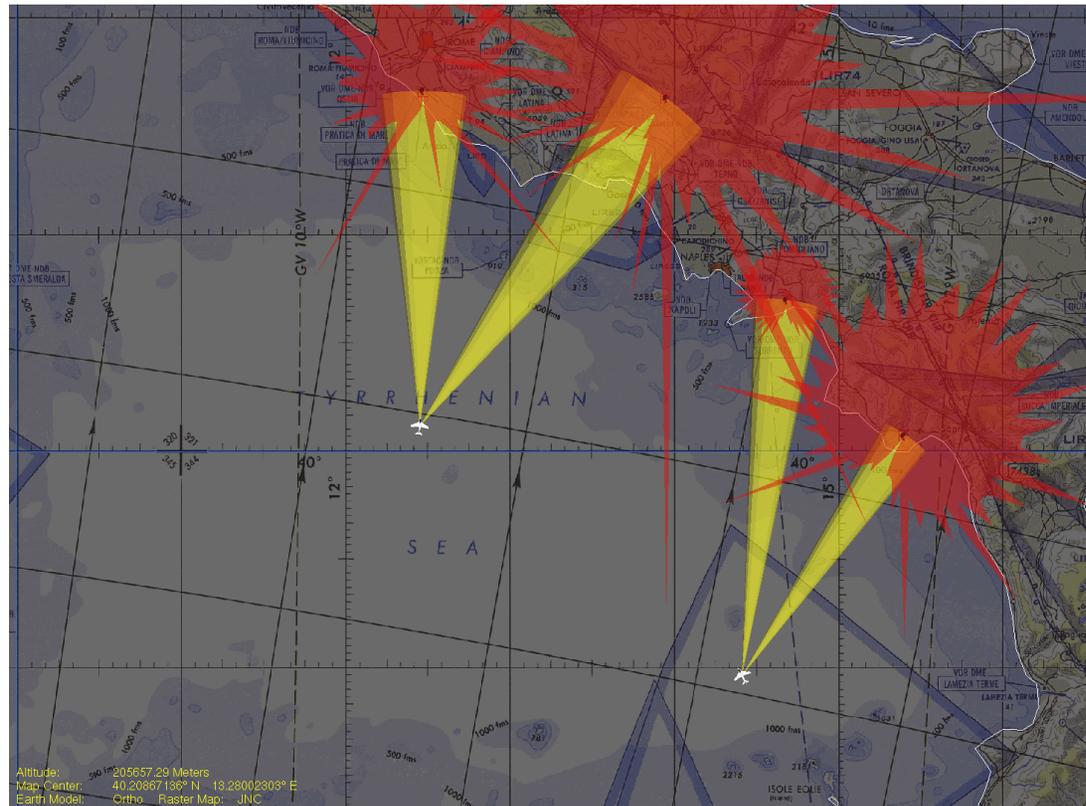
Increased Speed and Decision Making (2)

- Automated integration of disparate sensors and sources of information
 - In future conflicts, the amount of information will be overwhelming
 - Warfighters require IT-based decision tools that integrate and transform information into actionable knowledge

- Desired tools include
 - Decision Aids
 - To evaluate options, select “best” option, present option in understandable manner
 - To assess uncertainty and its impact
 - Sensor related tools
 - Optimally allocate sensors
 - Integrate information from disparate sensors
 - Transform data into knowledge



Asset Optimization: Example



- Optimally position & configure assets so as to maximize coverage
 - Sensors
 - Jammers
 - Shooters



Increased Speed and Decision Making (3)

- Presentation for rapid understanding by the warfighter
 - New technology has created new issues in data understanding
 - Increasing numbers of sensors in the battlespace
 - Demand is to provide information locally rather than sending it a command center for integration

- Target capabilities
 - Self-adaptive algorithms for sensor systems
 - Data aggregation using embedded computers
 - Interpretation of and interaction with aggregated by human operators
 - Automated cognition tools



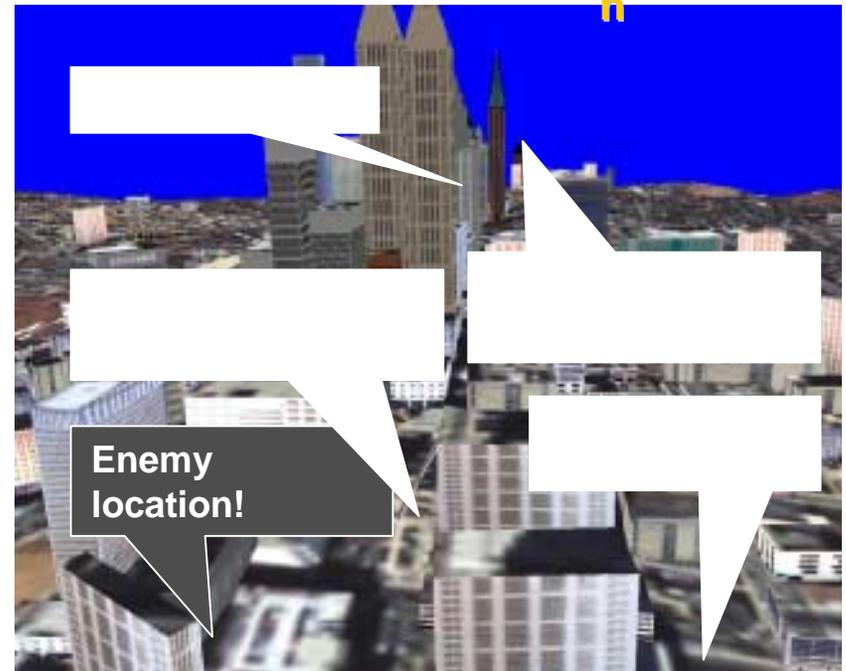
Research Challenges in Developing a Mobile AR System

- User Interface
 - Clearly display information to user
 - Information Filtering
 - Multi-modal interactions
- Tracking and Registration
 - Align graphics with real world
- Collaboration
 - Coordinate multiple mobile users and command center
- Rapid 3D Database Construction
 - Full geometry accurately georegistered with the real world
- Power Consumption
- Display Hardware
- Small and Rugged Computation Power
 - Capable of driving stereo displays
 - Capable of working in harsh environments
- System Integration
- Wireless Networking



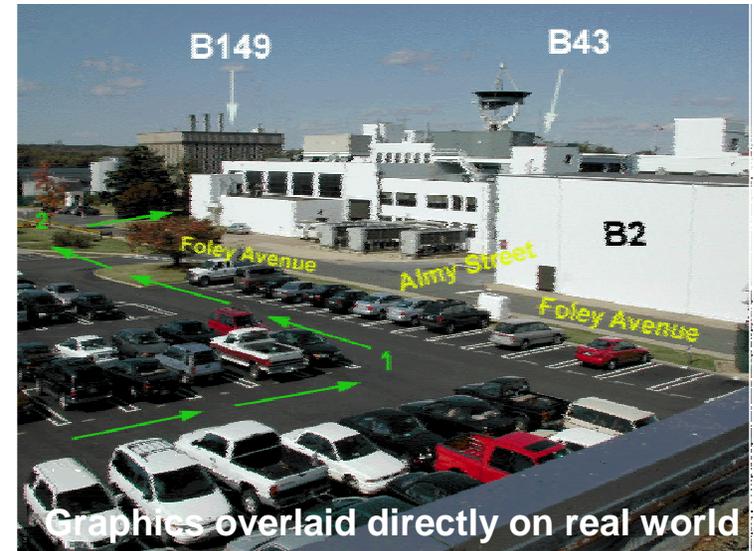
Military Operations in Urban Terrain (MOUT)

- **Changing nature of military operations**
 - Counter-terrorism; Disaster relief; Peacekeeping; Surgical strikes
- **Operating in *Urban Terrain***
 - Identify roads, buildings
 - Avoid hidden risks
 - Maintain knowledge of position, routes, ...
 - Coordinate with team members
 - Avoid fratricide
 - Visualize chemical sensor data, ground penetrating radar, ...
- **Examples**
 - Somalia, Haiti, Bosnia, Afghanistan, Panama, Lebanon, Grenada, Bagdad, Grozny, Leningrad, Berlin, Jenin





Mobile Augmented Reality

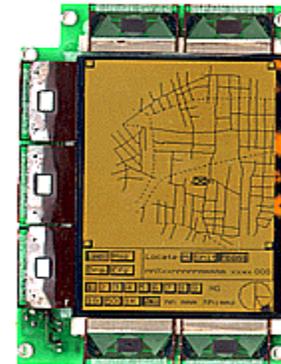
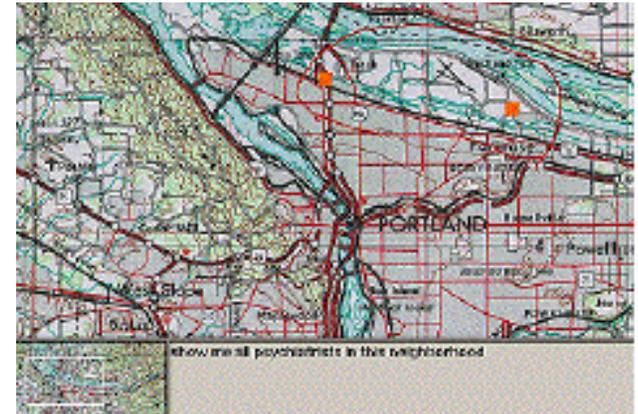


- | | | |
|-----------------------------|---|--|
| <i>Wearable</i> | → | Support users in the field |
| <i>See-through</i> | → | Provide unobscured view of surroundings |
| <i>AR</i> | → | Integrate information with surroundings |
| <i>Collaborative</i> | → | Coordinate multiple interacting users |
| <i>Networked</i> | → | Interoperate with other systems |
| <i>3D</i> | → | Objects behave like objects, not pictures |
| <i>Interactive</i> | → | Acquire/transmit information easily & effectively |



Shortcomings of Existing Methods

- Radioed instructions are hard
 - **To visualize**
 - **To integrate into tactical picture**
- Paper / electronic maps
 - **Force user to correlate map with environment, even if map automatically updates / orients**
 - **Do not represent 3D nature of urban infrastructure**
- Handheld displays
 - **Divert attention from surrounding environment**
- Monocular displays
 - **Obscure environment**





Increased Speed and Decision Making (4)

- Automated reasoning on information towards developing alternate Courses of Action (COA) with associated risks and uncertainties and drill down
 - Focus is on automated reasoning
 - Intelligent plan authoring for wargaming simulation systems
 - Reduction of time to create COAs
 - Ability to represent uncertainties and risks in MOEs

- Enabling technologies
 - Machine learning methods
 - Scalable learning
 - Integration of domain knowledge
 - Statistical learning to build and maintain dynamic knowledge bases
 - Case-based reasoning
 - Qualitative reasoning to handle incomplete/uncertain information
 - Reasoning methods to deal with contradictory information
 - Active logic to handle facts/situations that change in time



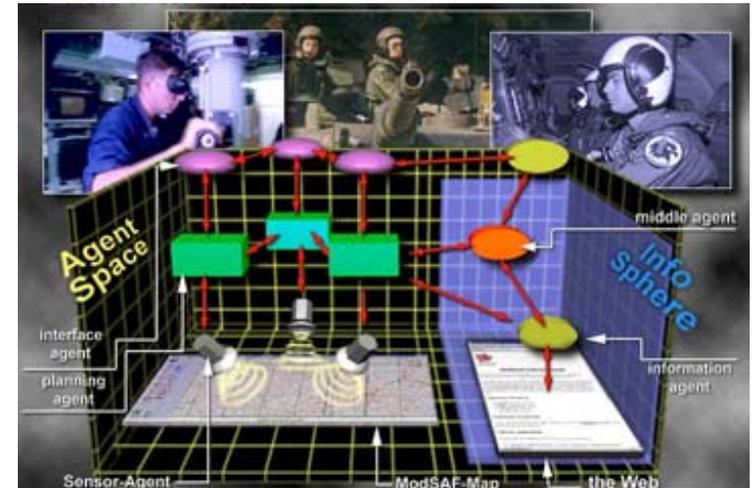
Automated Reasoning in Network-Centric Environments

- To perform a variety of tasks better, in less time, with less cost
 - **For use in**
 - Decision Support Systems
 - Autonomous Systems
 - **Develop enabling technologies to**
 - Find data (from sensors, databases, reports, etc.)
 - Process and integrate data, extract relevant information
 - Send the right information, to the right person/agent/system, at the right time, in the right form



Focus Areas in Machine Learning & Reasoning

- Scalable learning to handle multitudes of data
- Hybrid learning (e.g. statistical and domain knowledge)
- Qualitative reasoning for dealing with uncertain, imprecise, incomplete information
- Perception-based reasoning to properly handle human reports
- Active logic for reasoning in a changing world
- Reasoning with contradictory information
- Methods for integration of diverse, heterogeneous data



- **Intelligent Agents:**
 - Interface, Information, Task, Middle
- **Data Mining**
- **Knowledge Management**



Automated Plan-Authoring

- Wargaming simulation systems (e.g., JICM, JWARS)
 - Inputs:
 - World State (WS): Database of initial state of the scenario
 - Plan:COA to be simulated
 - Output:
 - Measure of effectiveness (MOE)
 - Select best plans based on MOEs
- Problems:
 - Analysts take weeks (modify WS) or months (start a scenario) to develop non-trivial wargaming scenarios
- Need automated plan-authoring tools to reduce the time to create plans
 - Efficient interfaces for preparing the World State
 - Automated methods for intelligently exploring a vast number of promising alternatives



Information Assurance (1)

■ Information Integrity

- Warfighters must be able to trust information received and performance of information systems
- Information integrity is easily challenged
- Current mechanisms
 - Reduce overall operational system performance
 - Impose additional operational constraints
- Goal is to rapidly detect and counter malicious acts

■ Interest areas include:

- Steganography to protect against insider threat
- Cryptographic protocol design and analysis to ensure trust across networks
- Real-time/fault tolerant multi-level secure group communications
- Certification technology
- Certification of embedded software and information systems



Information Assurance (2)

- Information Availability
 - Malicious and unintentional acts may deny access to information and information systems
 - System-wide information availability is dependent on approaches that protect all the links in the system
 - Current networks are extremely heterogeneous

- Target areas include:
 - Technologies to ensure timely/rapid availability of information across disparate networks
 - Access control and identification
 - Automation
 - Hardening to support recovery and reconstitution
 - Secure operations in a degraded mode



Information Assurance (3)

- Information Confidentiality
 - As systems become increasingly connected, the risk to data confidentiality increases
 - Malicious or unintentional acts may disclose information to unauthorized persons, processes or devices

- Areas of interest include:
 - Technologies to protect
 - Data
 - Other parameters critical to system security (e.g., biometric data)



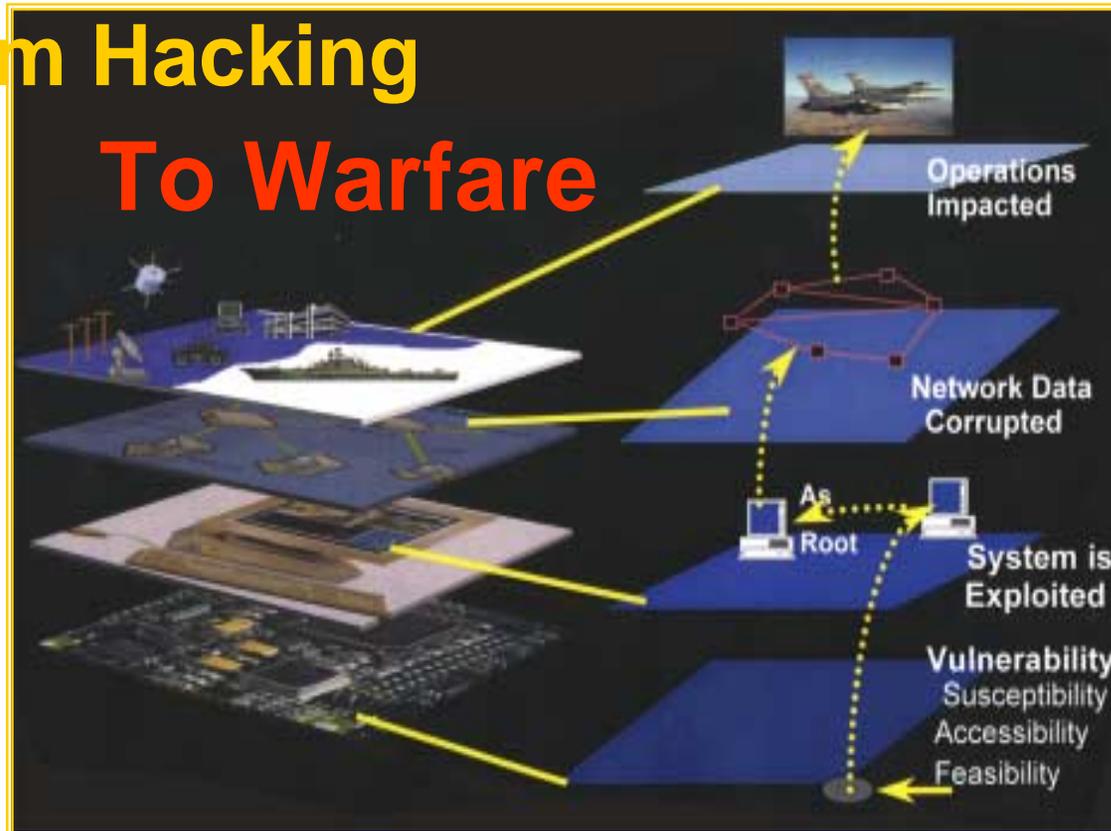
Information Network Situational Awareness

- Required to protect information infrastructure of joint, coalition and naval tactical commands.
- Important research areas include:
 - Network sensors to analyze, filter, coordinate, and communicate relevant data
 - Portrayal of network health and status appropriate for command in real-time
 - Exploration of alternatives for rapid coordinated assessment and response
 - Coordination with traditional C2 in the physical battle-space
 - Shared situation awareness of information networks in coalition operations



Why are we concerned

From Hacking To Warfare



**Information is the foundation on which we fight, yet...
Currently, we have real vulnerabilities at all echelons**



C² for Networks is Different

Traditional C2 Domain

Network C2 Domain

- Geographical 3D mission space

- Multi-dimensional mission space

- Physical effects are well understood
(e.g., kinetics, energetics, scattering)

- Non-physical effects ill-understood
(e.g., scope of influence, rationality)

- Interdependencies generally understood

- Complexities of information use and software dependencies ill-understood

- Most attacks at a perceptible speed
(with obvious exceptions)

- Network environment lends itself to wide imperceptibly rapid attacks

- Most attacks have physical manifestations

- Often no perceptible signs until too late

- Overrun / compromise easily detectable

- Compromise may not be detected at all

- Often war of "destruction"

- Usually war of "disruption"



Information Network Situational Awareness

- Network sensors to analyze, filter, coordinate, and communicate relevant data

Network Sensor Software Agent Community



Crypto Assistant
AGENTS



Host Monitoring
AGENTS



Authorization
AGENTS



Intrusion Detection AGENTS

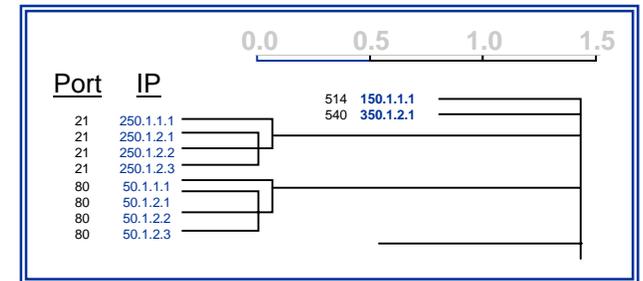
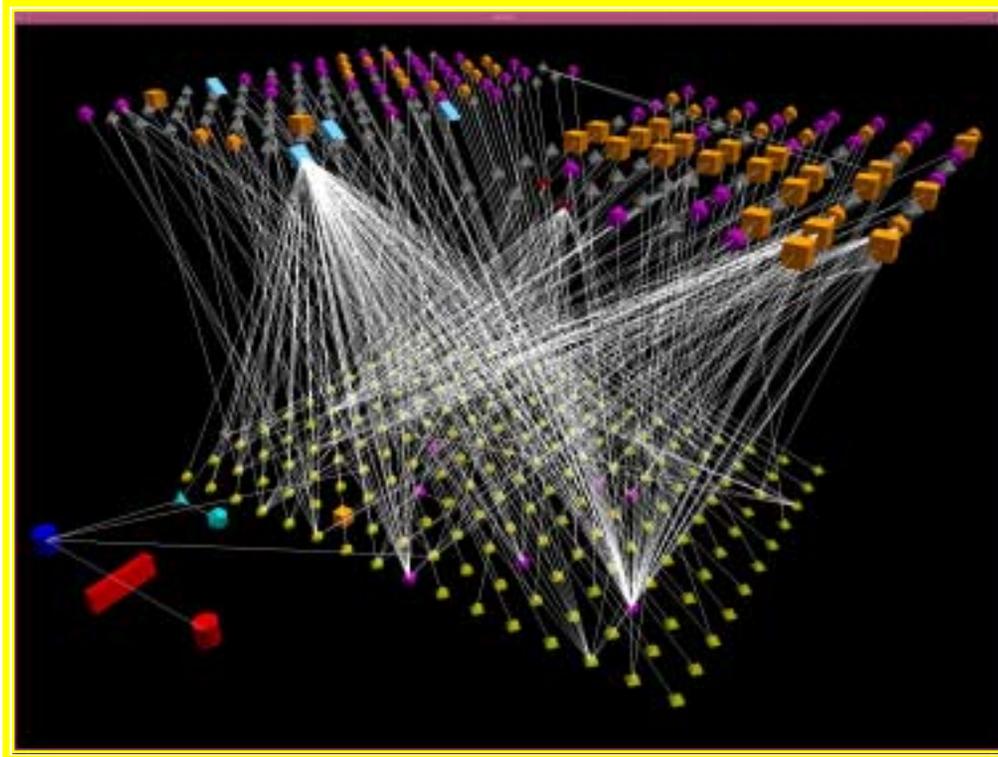


Policy Enforcement AGENTS

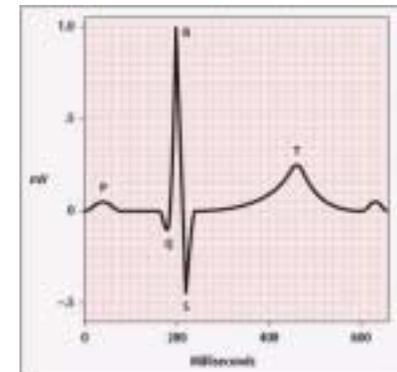


Information Network Situational Awareness

- Portrayal of network health and status appropriate for command in real-time



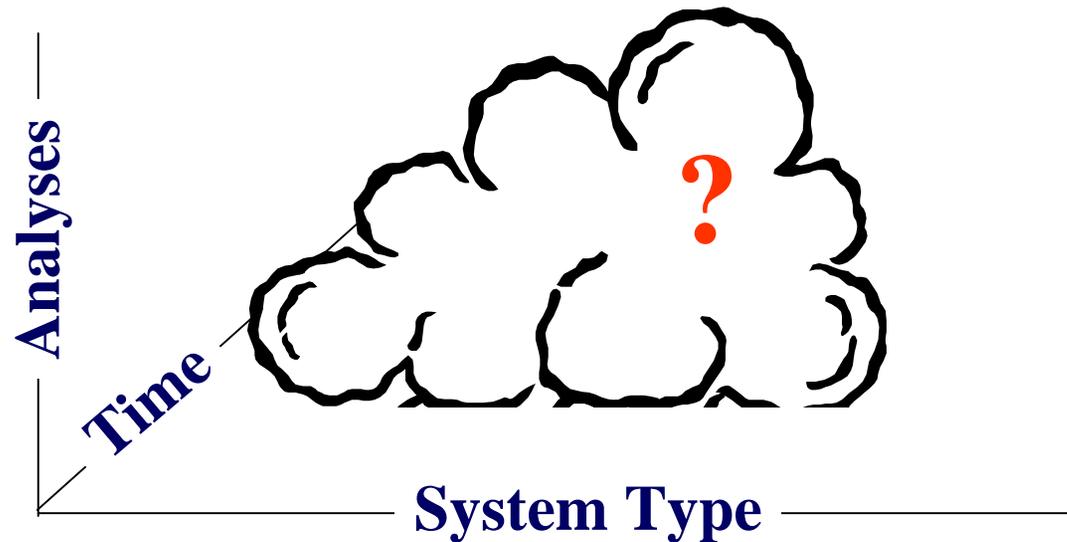
Dendrogram of Activity Clustering





Information Network Situational Awareness

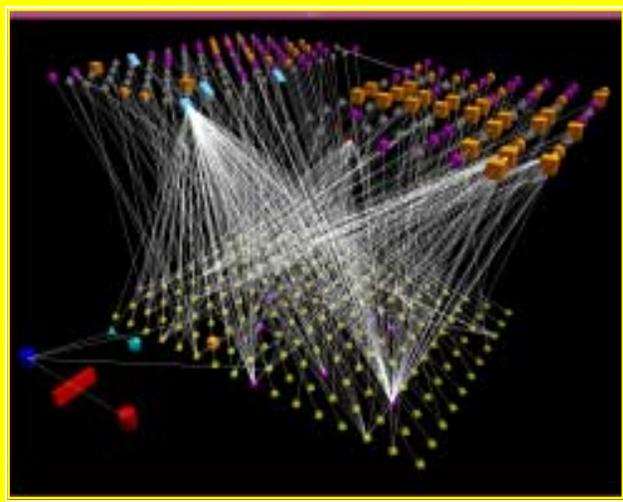
- Exploration of alternatives for rapid coordinated assessment and response



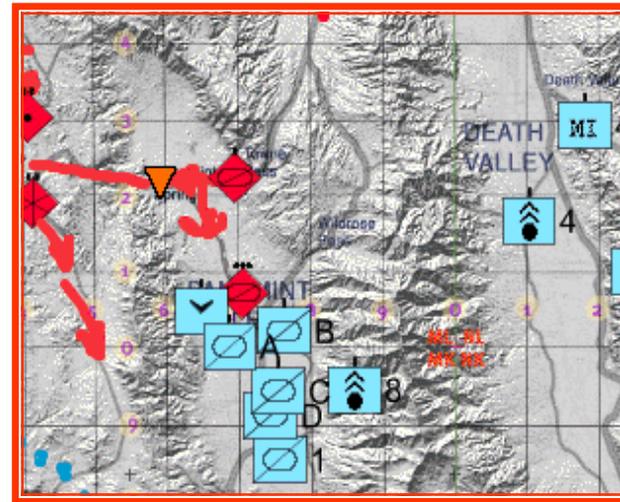


Information Network Situational Awareness

- Coordination with traditional C2 in the physical battle space



+

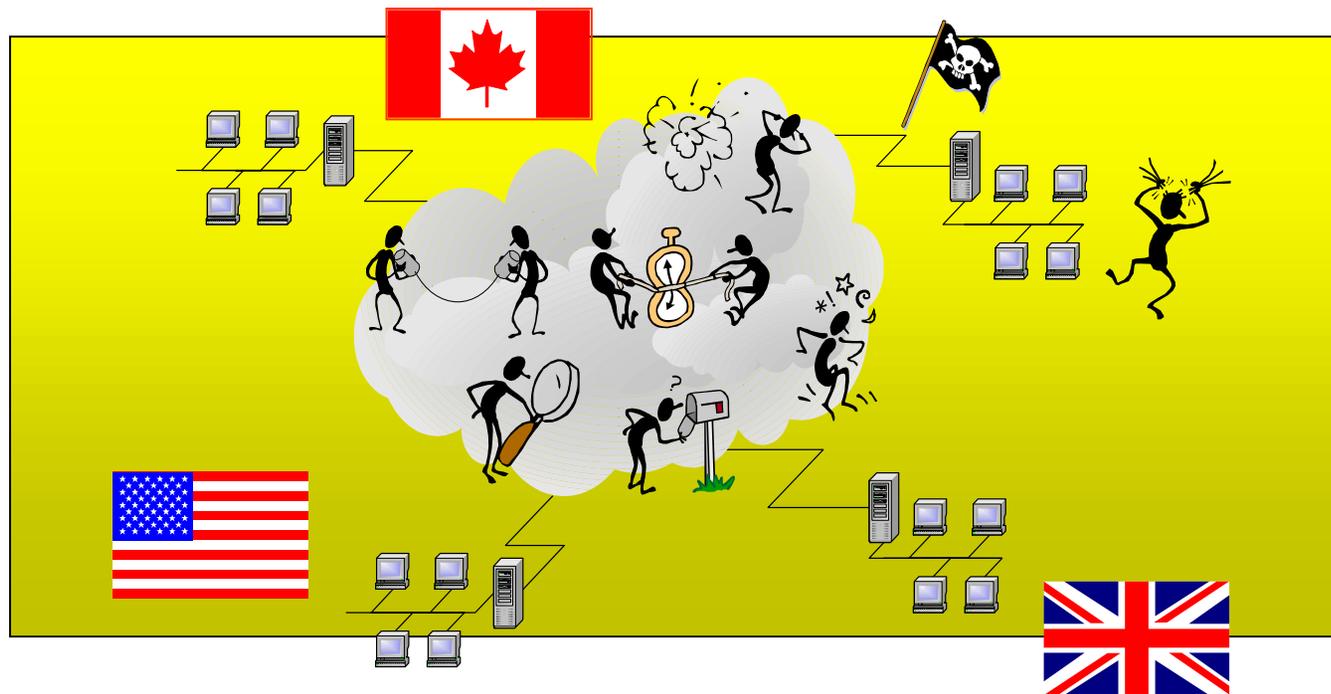


= ?



Information Network Situational Awareness

- Shared situation awareness of information networks in coalition operations





INSA in FY03 looked for:

- **A Cross-section of INSA topic areas**
 - Multi-disciplinary projects encouraged
 - Multi-investigator teams efforts encouraged
- **Strong IA component**
 - No award without a major IA focus
- **Transition Planning**
 - Leverage connections and contacts
 - Plan for downstream transitions
- **Applied Research effort**
 - Search for new utility and usefulness



IA in FY04 differs in emphasis

- Integrity, Availability, and Confidentiality
 - Higher priority on these information qualities
 - Situational Awareness of information quality
- Technology
 - Must promote both interoperability and QoS
- Heterogeneity
 - Must facilitate technological change
 - Protocol-centric approach encouraged



There's lots of room for innovation

Fault-Tolerance	Systems of Systems	Mission Context
Self-Organizing	Interoperability	Hybrid Systems
Real-Time	Operationalize Situational Awareness Defense-in-Depth	Hierarchies
Speed	Operational Detection Tools Vulnerability Analysis Tools	Decentralized
Options	Rapid Adaptation System Configuration and Analysis Tools	Coalitions
Sensor Grid	Network-Centric Concepts Data Fusion, Correlation, Classification Tools	Organizations
Monitoring	Theory and Principles of IA design Engineering Knowledge Base on Assurance	Ontologies
Survivability	Scalability and Trust Management Security Economics	Abstractions
Agents		Interfaces

Security, Integrity, Confidentiality, Availability, Non-Repudiation



Mission Focused Quality of Service (1)

- Current distributed information demands consume tactical network resources
 - Network congestion impacts operations
 - Information related to mission must be identifiable and given top priority

- Interest areas include:
 - Information prioritization
 - Real time data replication
 - Information delivery to reduce latency



Mission Focused Quality of Service (2)

- Contention in a complex multi-objective environment
 - Noise and retransmissions reduce available bandwidth

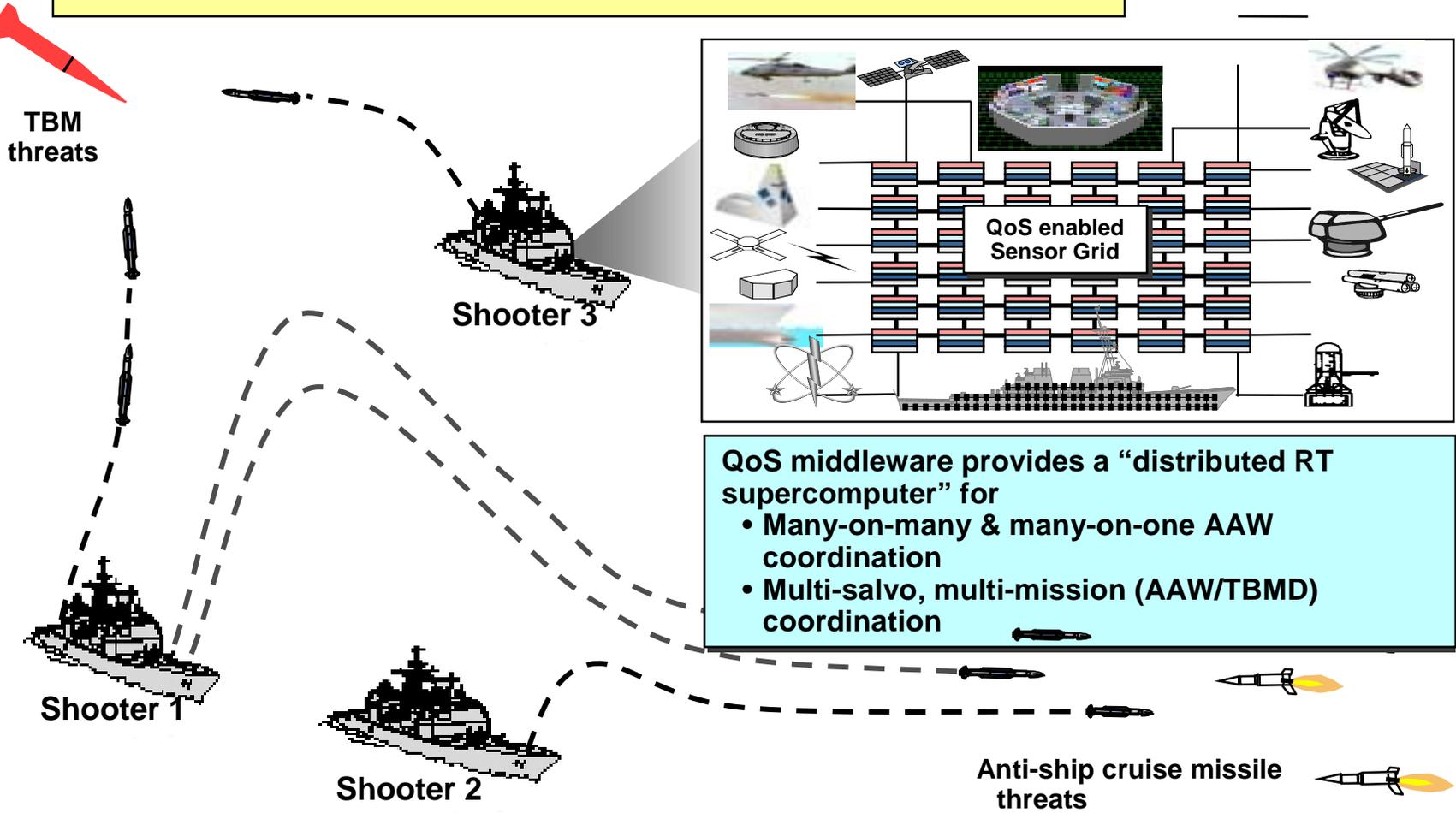
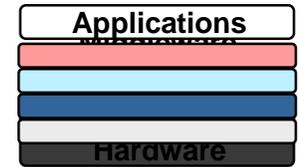
- Target areas include technologies that:
 - Support rapid establishment/disestablishment of networks
 - Using airborne relay to build and automate CVBG/ARG intranet
 - Extending networks to USMC/Joint forces
 - Dynamic dissemination of multi-media products to disadvantaged users



QoS Research Goals

Create the new generation of **middleware** technologies for distributed real-time & embedded (DRE) systems that enable

1. Simultaneous control of **multiple QoS properties** &
2. Customizable combat system **common technology bases**





Requirements: Network Centric Sensor to Shooter QoS

- Network centric sensor to shooter applications traverse many levels of computing and encounter stringent requirements at all levels:
 - **Accuracy** – sensor information must be accurate with tolerance limits
 - **Real-Time**
 - Weapons systems have stringent timing constraints on when execution must be performed
 - Sensor information must meet timing constraints:
 - Absolute temporal validity - not “stale” data
 - Relative temporal validity – a piece of sensor data must be within time of other sensor data that are used for a common tactical picture.
 - **Security** – sensor data has various security levels (intra ship crew rank, coalition forces access, etc)
 - **Reliability** – sensor data must meet availability and trust requirements.
- These and other requirements that pervade all levels of computing are called Quality of Service (QoS) requirements.



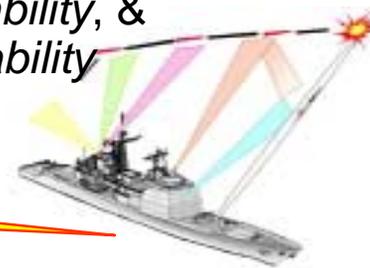
Problems with Current Approaches

- Dynamic RT combat system QoS requirements historically not supported by COTS
 - *i.e.*, COTS is too big, slow, buggy, incapable, & inflexible

- Likewise, the proprietary **multiple technology bases** in RT combat systems today limit effectiveness by impeding
 - **Assurability** (of QoS),
 - **Adaptability**, &
 - **Affordability**

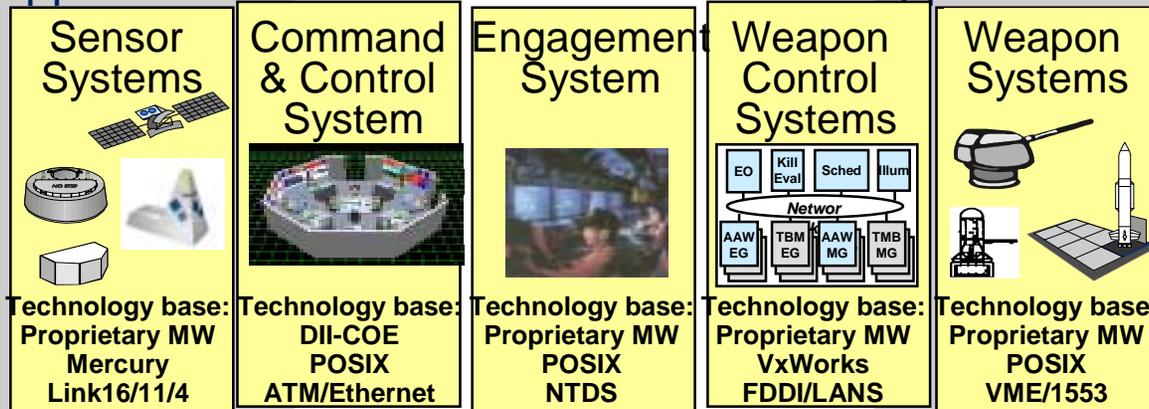
Today, each combat system brings its own:

networks
computers
displays
software
people



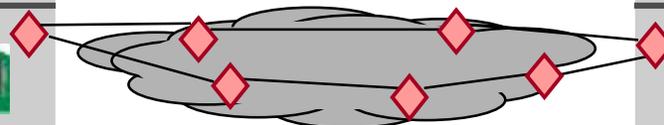
Applications

Applications



Operating System

Endsystem



Wireless/Wireline Networks

Operating System

Endsystem

Problems

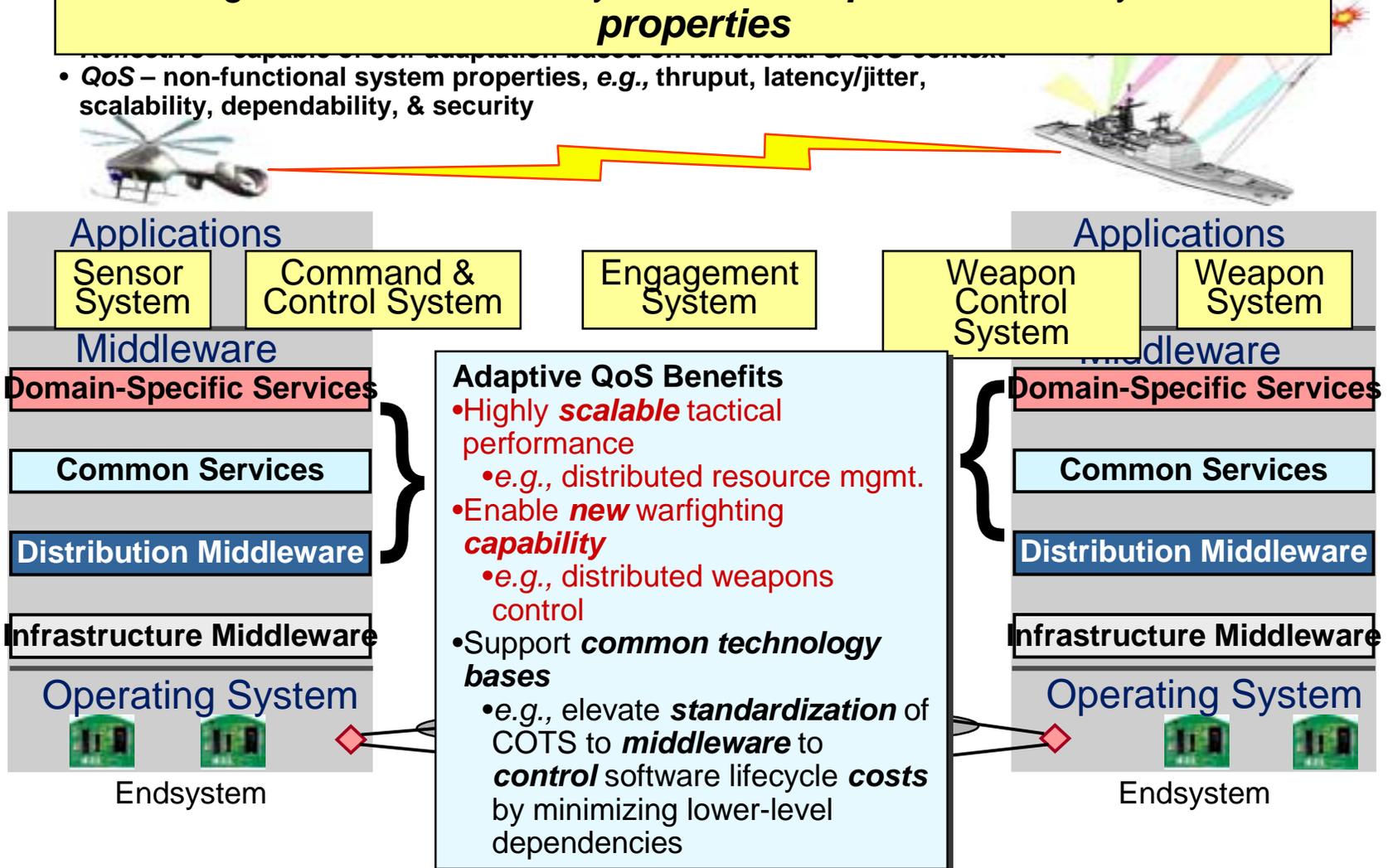
- **Non-scalable** tactical performance
- **Inadequate QoS** control for joint operations
 - *e.g.*, distributed weapons control
- **High** software lifecycle **costs**
 - *e.g.*, many “accidental complexities” & low-level platform dependencies



QoS Enables Sensor to Shooter

Create the new generation of **adaptive & reflective middleware** technologies to simultaneously control **multiple** Real-time system **QoS properties**

- QoS – non-functional system properties, e.g., thrupt, latency/jitter, scalability, dependability, & security





Research Needs

- Design QoS real-time model which enables the expression of time critical concepts and level of QoS.
- Develop a multi-layered QoS negotiation schema which will provide a mathematical basis for synthesizing the parameters (real-time, accuracy, reliability & security).
- Develop a scheduling & analysis capability which provide metrics with respect to the synthesis of the parameters.
- Design a modular framework to support the system design and enable the insertion of custom solutions.
- Focus on the middleware layer for support since this is the emerging layer for network centric sensor-to-shooter systems.



Summary: Where are we going?

- We are moving from platform-centric to net-centricity by applying
 - Commercial emerging technology
 - Emergent technology
- The S&T community is key to tomorrow's transformation
 - Sea Trial puts the Fleet at the heart of innovation
 - Exploiting innovation for operational excellence
 - Rapidly delivery technology to support doctrine and capabilities
- Projects **must** relate to Navy needs and objectives



Schedule for BAA

- Full Proposals Due Date 23 JUN 2003
- Notification of Award 23 AUG 2003
- Contract Awards October 2003

- For complete information: visit the ONR website, contracts and grants, BAAs