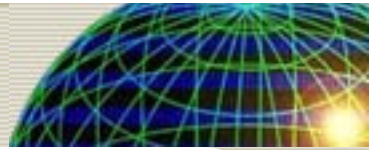
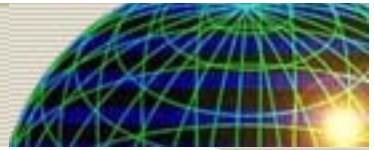


Cross-domain Information Exchange Framework (CIEF): Road Map to Web 2.0

Paul Shaw, SPAWARSYSCOM
Dr. David J. Roberts, iBaseT, Inc.
San Diego, CA

Outline…



- The Problem Being Solved… Information Exchange Across:
  - Man/Machine Boundaries
  - Diverse Information Domains and Focus Areas
  - Security Levels
- CIEF Solution is Information in a Published Context
  - Central Registries (Mission, Time, Location)
  - Publication/Subscription Model
  - Web 2.0 Recombinant Information (Pipes, Mashups, Semantic Web Services)
- Examples of CIEF Driven Scenario…

What's the Problem with the Web?…

1. You can find anything… Somewhere in 43,256 hits (e.g., Google)
2. What does it mean?... Stuff doesn't mean the same thing to all people
3. Information levels are mixed from raw to summarized, and of "varying" quality

Bottom line: Web services and Internet based systems may be fine for buying and selling shoes, but do not encompass DoD mission requirements: security, Quality of Service (QOS), semantic mediation, valued sources, etc.

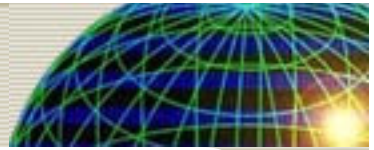
Will the Web 2.0 Fix It?…

"Web 2.0 is the business revolution in the computer industry caused by the move to the internet as platform, and an attempt to understand the rules for success on that new platform. Chief among those rules is this: Build applications that harness network effects to get better the more people use them." **Tim O'Reilly (2006-12-10). Web 2.0 Compact Definition: Trying Again**

Problem: Its (*Web 2.0*) exact meaning remains open to debate, and some technology experts, notably Tim Berners-Lee, have questioned whether the term has meaning. developerWorks Interviews

So the answer is, "No!"... Not without a defined framework

CIEF Addresses the BIG Picture…

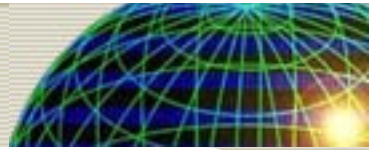


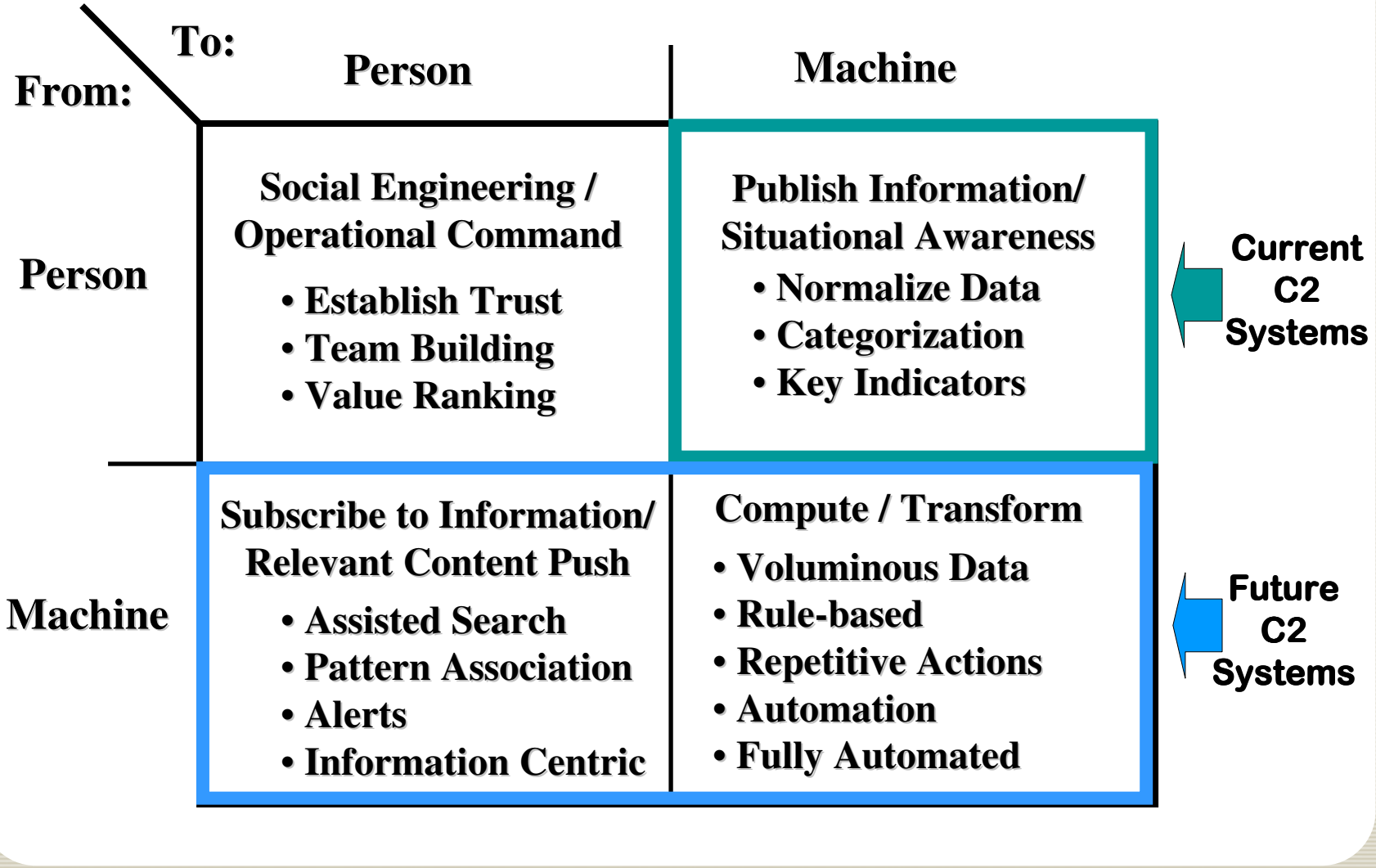
Rather than deal with bits and pieces of Web 2.0 information exchange, CIEF is a framework that addresses multiple dimensions of information exchange from the physical, to the "purposeful intent" of information request and response.

> **For example: If a planner were to request the readiness state of an asset, the response of: fuel onboard, ammunition load, and number of hours of rest of the crew, could be one set of answers… or readiness could be summarized to as a single value…**

The correct response needs to address the purposeful intent of the requestor.

CIEF Addresses Information Flow…





Information Flow Across P2P

Social Engineering / Business Rules

- Establish Trust – through certified authentication methods and published "resumes"
- Team Building – through tools to invite participation and control access and ownership of information
- Value Ranking – local and published authoritative sources, information traffic patterns, and strategies to reflect information value

The social engineering can be left to "happen" or it can be enhanced through supporting tools and processes.

Information Flow Across M2P / P2M

Publish Information (P2M)

- Normalize Data – Common lexicon and formats
- Categorization – Mission oriented ontologies
- Key Indicators – Understanding of the prioritization (business rules) of data objects

Subscribe to Information (M2P)

- Assisted Search – Complexity is abstracted
- Pattern Association – Keywords in context
- Alerts – Based on objectives and limits within the mission

Supporting tools needed to support machine processing.

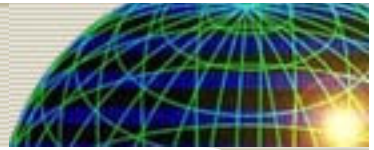
Information Flow Across M2M

Compute / Transform

- Voluminous Data – Too much information with too many attributes to be processed by humans
- Rule-based – Interactions are non-ambiguous and based on understood processes
- Repetitive Actions – Decisions and actions are deterministic and can be re-constructed.

People skills and machine processing should be view as complementary… Tools that abstract complexity (e.g., publish content to metadata registry) assist information flow.

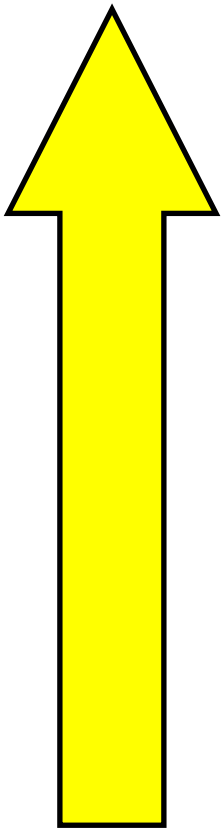
CIEF Implementation Plan…



- Start with standard set of tools to setup and manage a COI / Domain
- Build a centralized method to register and search for information publication/subscription
  - Profile registry (provides context of the request)
  - Content registry (ontological categorization of information)
  - Admin registry (usage stats, queuing, routing)
- Develop tools to assist in the publication and subscription to information…
  - Refactoring and customer involvement are key
  - Based on mission threads/processes

The Goal: To Published Context…

Published Context



Negotiated Context

Information Pipes – Structured content that is published and registered in a content registry (associated with mission ontology)

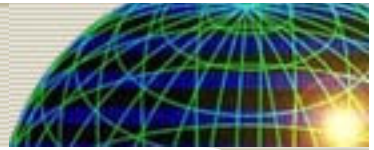
News Feeds – Structured content in information domains (channels)

Web Services/UDDI – Shared data and methods

Reports – Structured content publication

Documents – Free form or structured content

Info Pipes: Adaptations of RSS v2.0…



Channel elements:

Language	DTIC DAC / Encryption level
Managing Editor	CIEF COI Manager
WebMaster	CIEF Domain Manager
Category	Access control group
Docs	DTIC DAC
Cloud	Registration information

Items:

Category	Mission ontology classification
Guid	Unique CIEF identifier

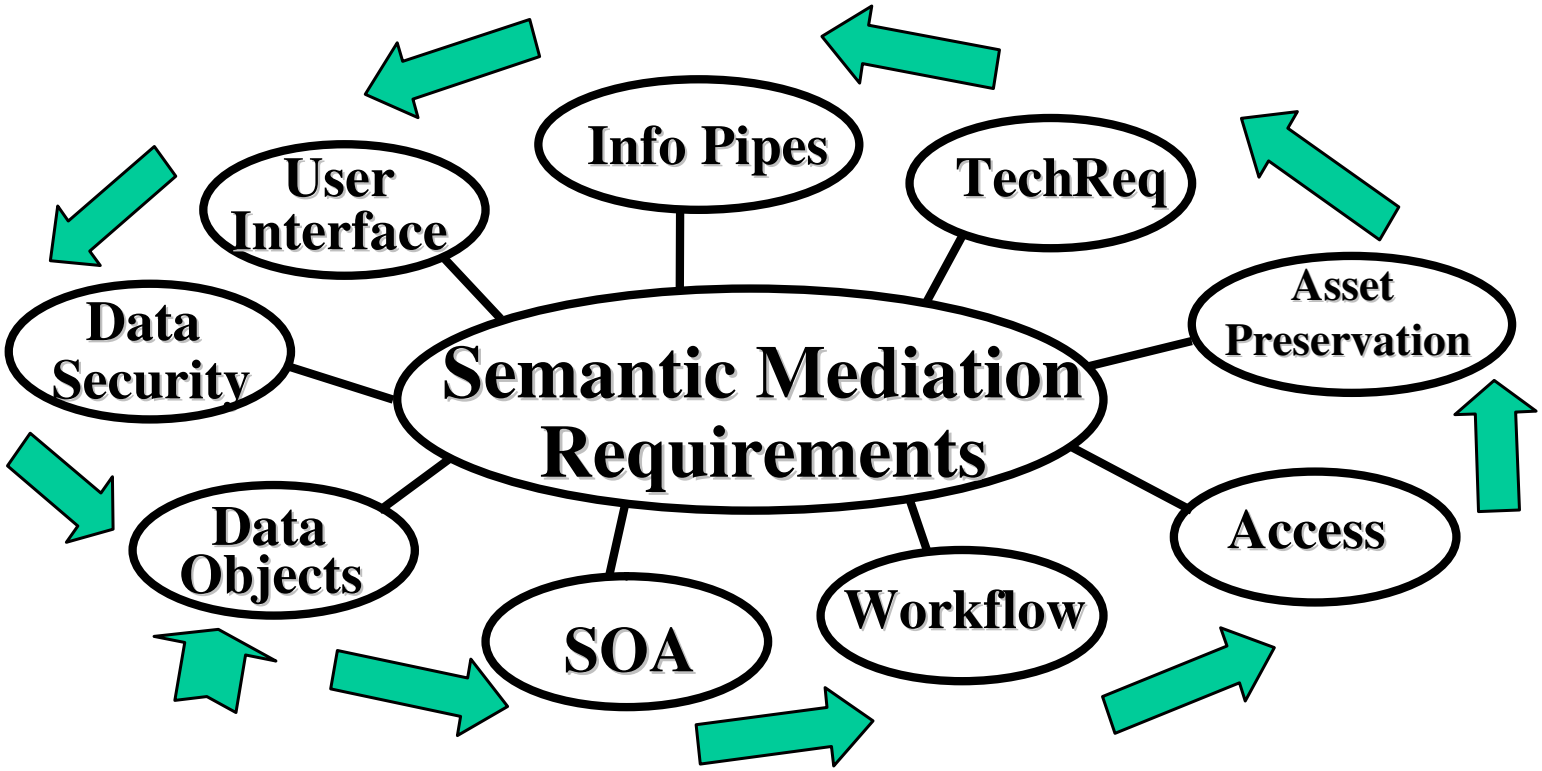
RSS Extensions:

Priority	Importance of information
Geo-location	Location specific indicator

RSS vs. CIEF Information Pipes…

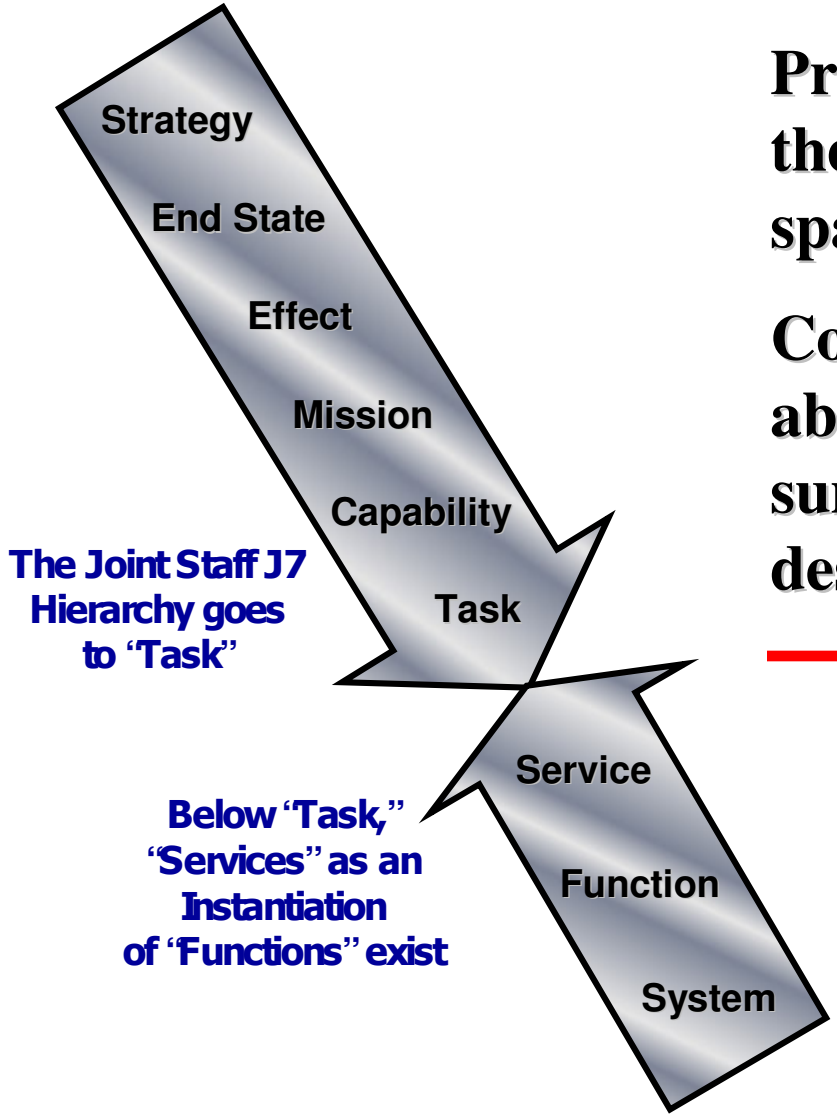
	RSS News Feed	Information Stream
XML/RDF Based…	Yes	Yes
Semantic Orientation…	Yes	Yes
Centralized Registry…	Partial	Yes
Public Format…	Yes	Partial
Commercial Reader…	Yes	No
Analysis Tools…	Partial	Yes
Re-publication Tools…	No	Yes
DoD Oriented Schema…	No	Yes
- Mission Context…	No	Yes
- Time Context…	No	Yes
- Geo-location Context…	No	Yes
DoD Authentication…	No	Yes
DoD Encryption…	No	Yes
DoD Access Control…	No	Yes

CIEF Data Strategy…



Data exchange strategy is built around core data elements/processes

CIEF Address SOA at the Task Level…

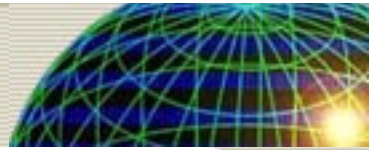


Profile Registry… Establishes the mission, temporal, and spatial contexts

Content Registry… Processes, abstraction level (raw to summarized), metadata descriptors, and URL

- **Web Services**
- **Information Pipes**
- **Databases**
- **Documents/Reports**

CIEF Core Registries…



Profile… Contextual Constraints

Authenticated Name
Access Rights (COI, SIG, Individual)
Mission (Type, Temporal, Spatial)

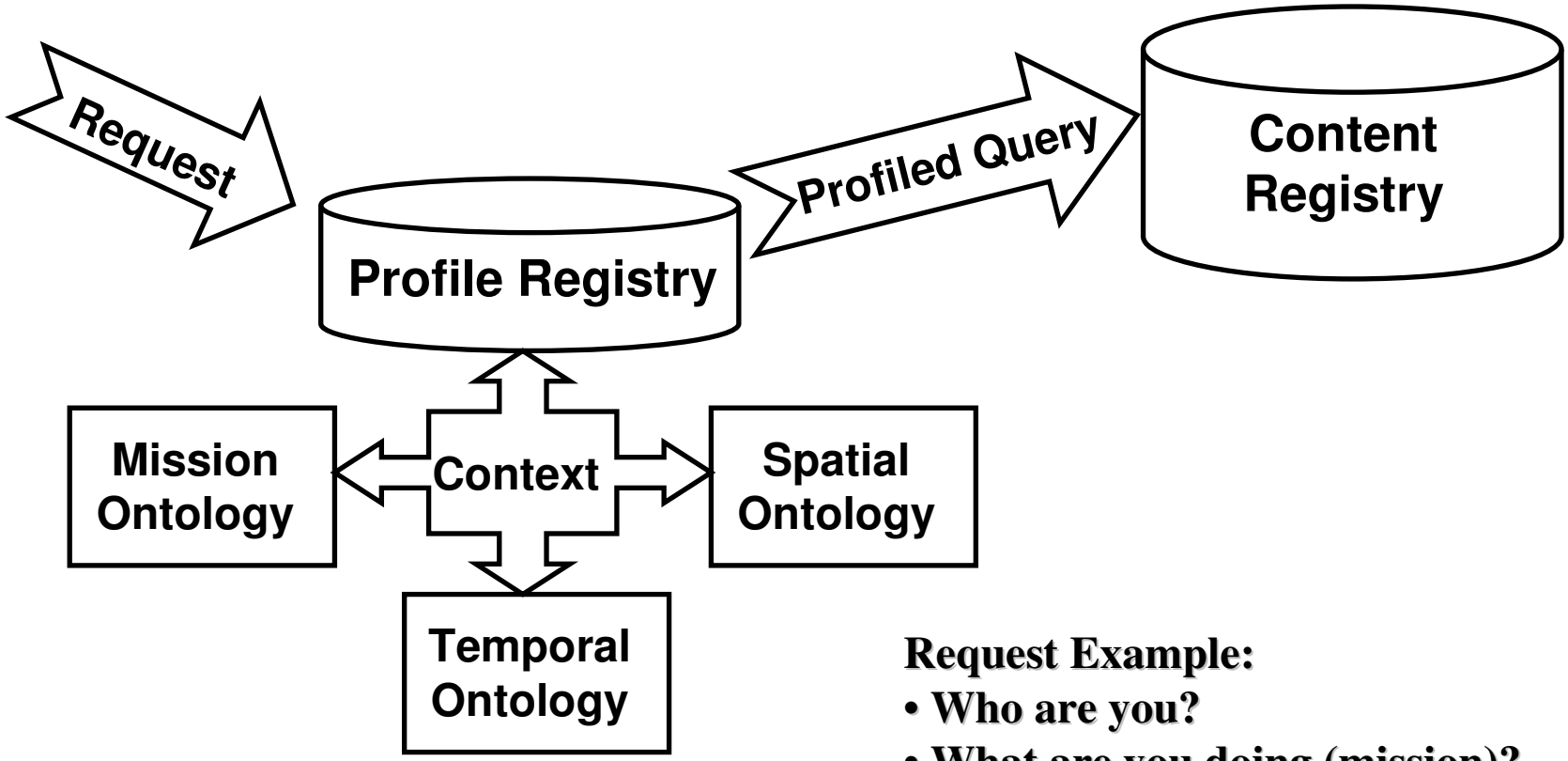
Content… Metadata Descriptors

Access Level, Functional Level, Element (context), Resource Location

Admin… Operational Constraints

Resource, Priority (value), Availability (responsiveness), Reliability (historical)

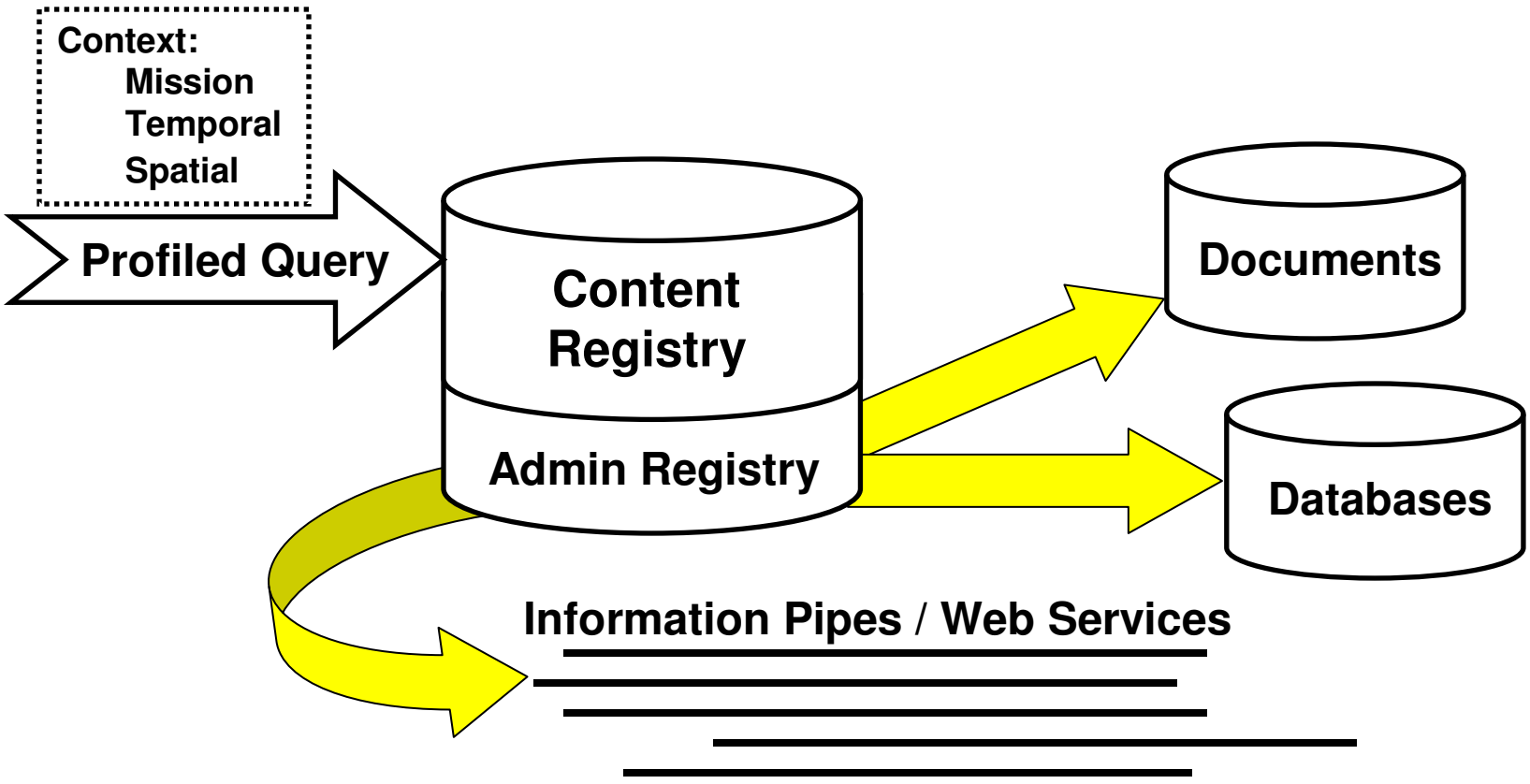
CIEF Profiled Query…



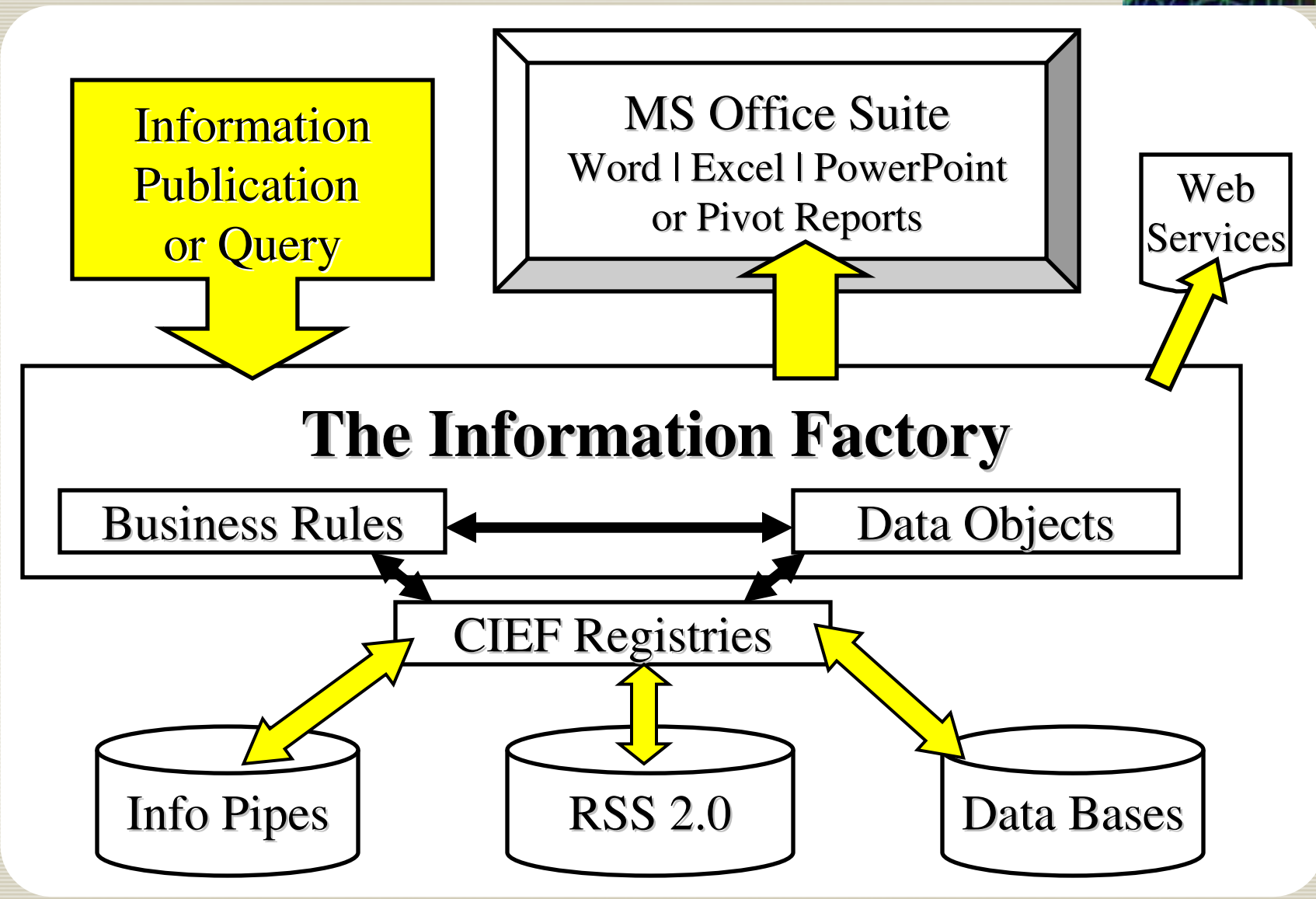
Request Example:

- **Who are you?**
- **What are you doing (mission)?**
- **When (urgency of information)?**
- **Where are you (geo-location)?**

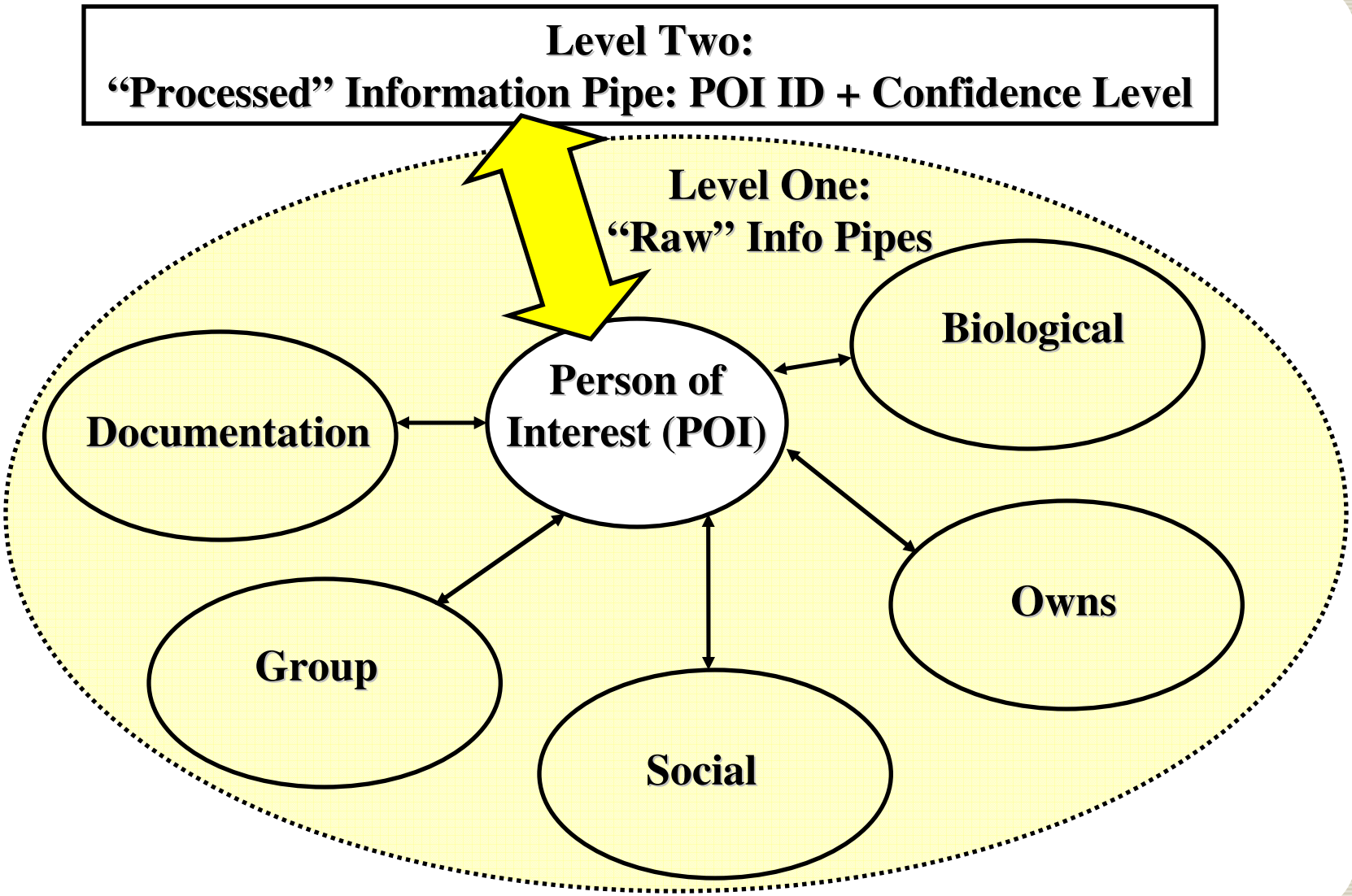
CIEF Profiled Response…



Example of a CIEF Publication Tool…



Example of Recombinant Info Pipes…



Example of CIEF Driven Scenario…

Person of Interest (POI) processing…

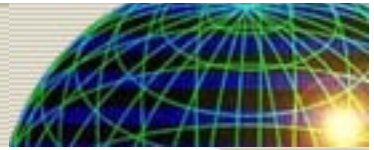
1. Gather all Level One information on POI past and present.
2. Publish all Level Two information on POI with priority rating (the POI's recent travel and other associations are "flagged" for a Level Two further analysis).
3. Level Two COI "patterns" POI information and requests backsweep (all additional Level One information on POI).
4. Level Two COI published POI information with action plan and request Level One information for:
    - Additional database access of: Visa, carrier manifest, etc.
    - Human intelligence reports
    - Time/location updates of prior information
5. Action plan results in pick up of POI's associate and additional Level One biological descriptors to "fill in" information patterns.
6. POI is located through biological identification at US port of entry (POI documentation was false but would have passed screening).

Summary…

CIEF is a developmental framework that will allow:

- **Multiple information exchange functional areas to be developed by specialized teams but still "plug into" an operational framework.**
- **Allow direct participation by mission subject matter experts in the definition of information patterns, data objects, and information processing.**
- **Metrics that address increases in mission efficiency (net-centricity) and related Return on Investment (ROI).**

Points of Contact…



Program Manager:

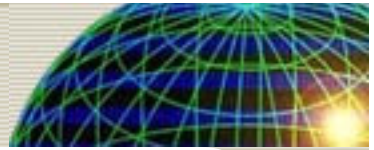
Paul Shaw, Paul.Shaw@navy.mil

Chief Scientist:

Dr. David J. Roberts, droberts@ibaset.com

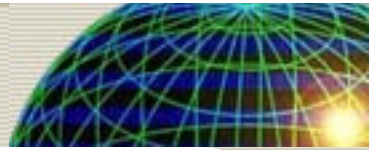
Backup Detail
and Supporting Research

CIEF Operational Definitions…



- Class (association of semantic objects)
- Pattern (class and attribute model)
- Type (delineates pattern features)
- Context (delimits pattern scope)
- Attribute (descriptor of class)
- Instance (value of attribute)
- Action (modification of attribute instance)
- State (instance with context)
- Goal (desired state of attribute(s))
- Plan (sequence of attribute changes, with contingencies)
- Level (degree of abstraction of object)

Semantic Object Levels…



Level One… Assimilation (fuse, correlate, pattern recognition)

- Sensor Information
- Primary information sources

Level Two… Application (plan, execution, assessment, and adjustment)

- Resource assessment
- Decision making… applied strategies
- Initiate actions
- Monitor for effect
- Modifications based on effect

Examples of Semantic Objects by Level…

Level One… Assimilation

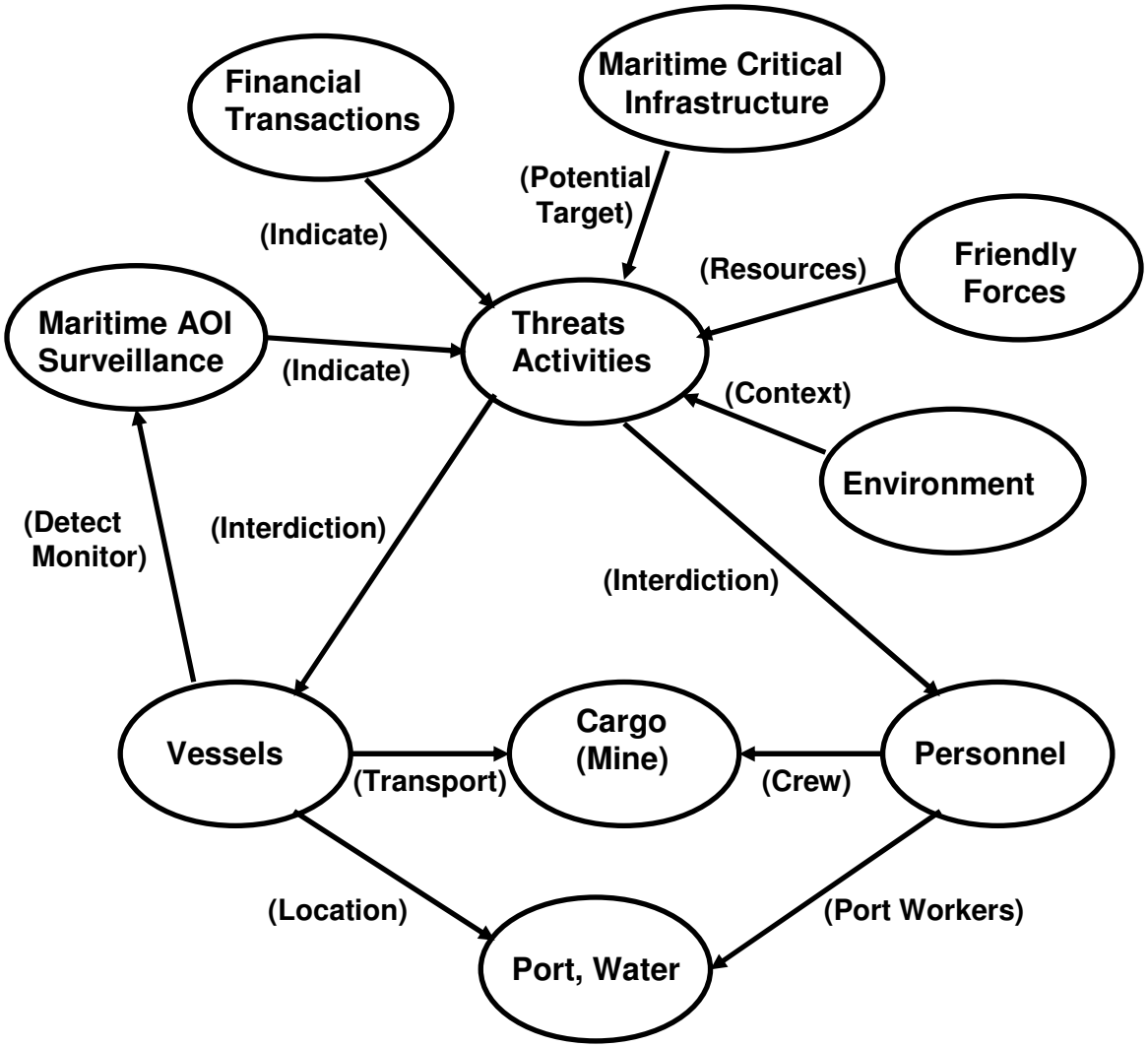
Element (type, context)
Context (temporal, spatial)

Level Two… Application

Threat (type, temporal, spatial)
Resource (type, temporal, spatial)
Policy (type, temporal, spatial)
Value (type, temporal, spatial)
Intent (type, temporal, spatial)

Two Scenarios Based on National Strategic Maritime Security (NSMS) Mission Areas that Initiated CIEF Research

Scenario Threat Model for Both Scenarios…



Scenario #1:
Radiological Dispersal Device (RDD)

Based on the "White Paper on the Applicability of the NATO Generic Hub, Version 5 (GH5) for an Information Exchange Data Model (IEDM) to Support National Strategy for Maritime Security (NSMS) Mission Areas and Joint Capability Areas (JCA)," by Paul Shaw and Dr. David Roberts, SPAWARSYSCOM, June 6, 2006. (Note: This paper is available to authorized agencies upon request.)

Radiological Dispersal Device (RDD) …

The RDD scenario was developed that addressed the following National Strategic Maritime Security (NSMS) mission areas:

- **Prevent transport of WMD by merchant or cruise ship for detonation in port.**
- **Prevent transport of WMD, weapons, and or critical system technology.**
- **Prevent transport of conventional explosives alongside offshore or port facility.**
- **Prevent intentional (catastrophic) pollution of oceans or ports**

An analysis of the applicability of current Information Exchange Data Models (IEDM) to support detection, interdiction, and post detonation events was conducted.

RDD Scenario Overview…

Goal: Disrupt global shipping

Objective: Detonation of one or more RDD in three destination ports (Two US, one Asian)

Perpetrators: Elements of a foreign government

Radiological Source: "Orphaned" material use in oil surveying, and cold pasteurization

Devices: Device #1 and #2 detectable through normal screening processes. Device #3 designed to circumvent detection.

Transport Mode: Marine shipping container

Timeline: None for assembly, but coordinated arrivals based on shipping schedules

Detonation: Designed to detonate during off-loading

Post Detonation: Device #1 and #2, six by three mile contamination plume; Device #3, twenty city blocks

RDD Analysis…

Assessments were made with regard applicability of the current IEDM to meet the scenario requirements to:

- **Gather initial intelligence (intent, warning levels)**
- **Detecting threats**
- **Monitor and assess threats**
- **Distribute situation updates**
- **Coordinate actionable tasks to appropriate agencies, to include publish information to the media**
- **Collect historical information for after action reviews**

Analysis Detail per RDD Scenario…

NSMS Tasking Areas	Score
Gather Initial Intelligence	3
Detecting Threats	3.5
Monitor and Assess Threats	4
Distribute situation updates	5
Coordinate Actionable Tasks to Appropriate Agencies	3.5
Collect Historical Information for After Action Reviews	4

Scale is:

5 = Meets current requirements
4 = Meets most requirements
3 = Can be adapted to meet requirements
2 = Substantial effort to meet requirements
1 = Will not meet requirements (conflicting, not compatible)

Conclusions:

- Many areas of applicability of the current IEDM
- Also capability shortfalls in NSMS tasking areas
- Adequate information in post-detonation / after action reviews
- Needs domain content and additional reporting formats

Applicability per Global Maritime Req…

Area	Global Maritime Mission	Score
1	Vessel Characteristics	4.8
2	Cargo (Vessel's Manifest)	3.5
3	Vessel Crews and Passengers	3
4	Maritime Areas of Interest	4.3
5	Ports, Waterways, and Facilities	3
6	Environment	3.5
7	Maritime Critical Infrastructure	3.6
8	Threats and Activities	4
9	Friendly Forces Operational Info	3.8
10	Financial Transactions	3

Scale is:

5 = Meets current requirements
4 = Meets most requirements
3 = Can be adapted to meet requirements
2 = Substantial effort to meet requirements
1 = Will not meet requirements (conflicting, not compatible)

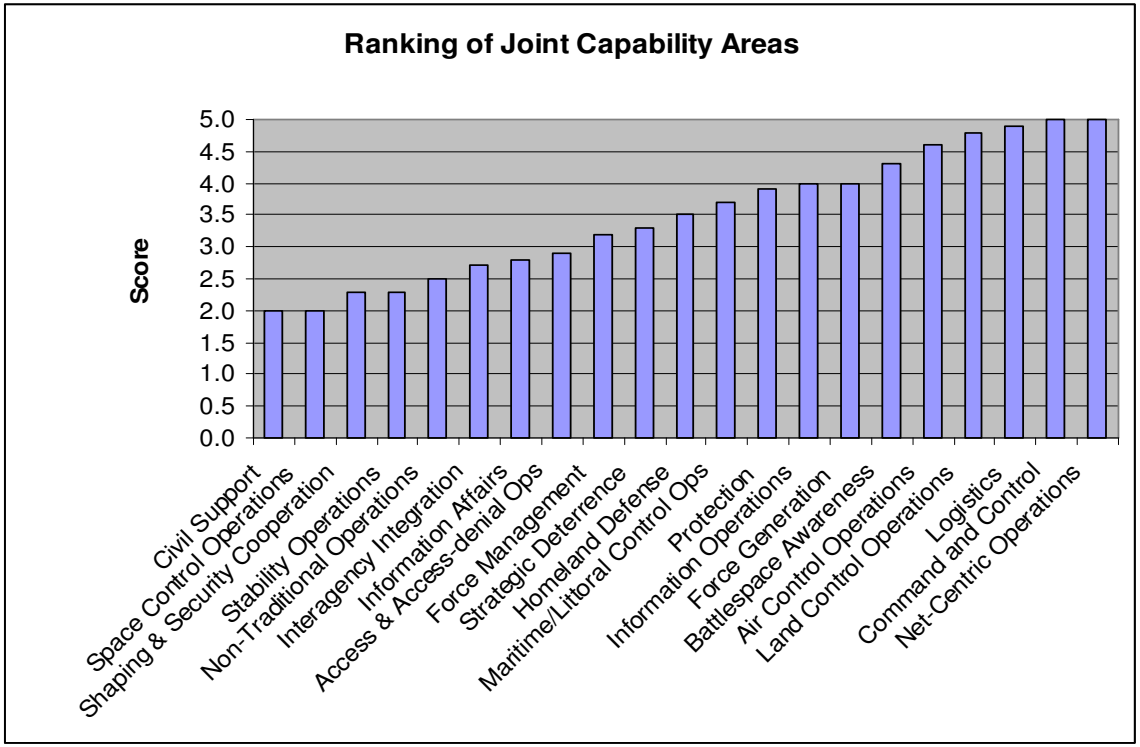
Applicability per JCA Requirements…

Acronym	Joint Capability Areas (JCA)	Score
BA	Battlespace Awareness	4.3
C2	Command and Control	5
NC	Net-Centric Operations	5
II	Interagency Integration	2.7
IA	Information Affairs	2.8
IO	Information Operations	4
FP	Protection	3.9
FL	Logistics	4.9
FG	Force Generation	4
FM	Force Management	3.2
HD	Homeland Defense	3.5
SD	Strategic Deterrence	3.3
SS	Shaping & Security Cooperation	2.3
SO	Stability Operations	2.3
CS	Civil Support	2
NT	Non-Traditional Operations	2.5
AO	Access & Access-denial Ops	2.9
LC	Land Control Operations	4.8
MC	Maritime/Littoral Control Ops	3.7
AC	Air Control Operations	4.6
SC	Space Control Operations	2

Scale is:

- **5 = Meets current requirements**
- **4 = Meets most requirements**
- **3 = Can be adapted to meet requirements**
- **2 = Substantial effort to meet requirements**
- **1 = Will not meet requirements (conflicting, not compatible)**

Applicability per JCA Requirements…



Scale is:

- **5 = Meets current requirements**
- **4 = Meets most requirements**
- **3 = Can be adapted to meet requirements**
- **2 = Substantial effort to meet requirements**
- **1 = Will not meet requirements (conflicting, not compatible)**

Applicability Summary…

Composite scores of all mission areas:

Coverage	Tasking Area	Score
National	NSMS (RDD Scenario)	3.8
Global	Global Maritime Community of Interest	3.7
Joint	Joint Capability Area	3.5

Scale is:

5 = Meets current requirements
4 = Meets most requirements
3 = Can be adapted to meet requirements
2 = Substantial effort to meet requirements
1 = Will not meet requirements (conflicting, not compatible)

- **Failings of the current IEDM were a lack of domain and report information focus, rather than any architectural short comings.**
- **Based on the shortfalls indicated in this research, further efforts were recommended to develop a light-weight framework to address IEDM shortcomings (e.g., CIEF).**

Scenario #2:
Mine Warfare (MIW)

Based on the "White Paper on the Applicability of the NATO Generic Hub, Version 5 (GH5) for an Information Exchange Data Model (IEDM) to Support National Strategy for Maritime Security (NSMS), Mission Areas and Joint Capability Areas (JCA) and Specifically, Mine Warfare (MIW) Missions," by Paul Shaw and Dr. David Roberts, SPAWARSYSCOM, June 22, 2006. (Note: This paper is available to authorized agencies upon request.)

Mine Warfare (MIW) Scenario…

A MIW scenario was developed that addressed the following NSMS mission areas:

- **Prevent transport of conventional explosives alongside offshore or port facility.**
- **Prevent mining of harbors and sea lanes by commercial vessels.**
- **Prevent control of critical choke points on sea lanes by terrorists.**
- **Prevent intentional (catastrophic) pollution of oceans or ports.**

An analysis of the applicability of the current IEDM to support detection, interdiction, and post detonation events will be conducted.

MIW Scenario Overview…

Goal: Disrupt local (San Diego) and world shipping

Objective: Sinking a commercial cruise ship to block the main shipping channel

Perpetrators: Elements of a foreign government

Material Sources: COTS and smuggled explosives for booster charges and detonators

Mining Devices: COTS material, 55 gallon drum

Delivery Craft: Modified sports fishing craft (28')

Timeline: None for assembly, but coordinated arrivals based on cruise ship departure schedule

Detonation: Magnetic anomaly detection (16' distance)

Post Detonation: Compromised hull of cruise ship that cannot be re-floated blocking the main channel

MIW Analysis…

Assessments were made with regard applicability of the current IEDM to meet the MIW scenario to:

- **Gather initial intelligence (intent, warning levels)**
- **Detecting threats**
- **Monitor and assess threats**
- **Distribute situation updates**
- **Coordinate actionable tasks to appropriate agencies, to include publish information to the media**
- **Collect historical information for after action reviews**

Analysis of Applicability per RDD Scenario…

NSMS Tasking Areas	Score
Gather Initial Intelligence	3
Detecting Threats	3.5
Monitor and Assess Threats	4
Distribute situation updates	5
Coordinate Actionable Tasks to Appropriate Agencies	3.5
Collect Historical Information for After Action Reviews	4

Scale is:

5 = Meets current requirements
4 = Meets most requirements
3 = Can be adapted to meet requirements
2 = Substantial effort to meet requirements
1 = Will not meet requirements (conflicting, not compatible)

Conclusions:

- **Many areas of applicability of the current IEDM**
- **Also capability shortfalls in NSMS tasking areas**
- **Adequate information in post-detonation / after action reviews**
- **Needs domain content and additional reporting formats**

Applicability per Global Maritime Req…

Area	Global Maritime Mission	Score
1	Vessel Characteristics	4.8
2	Cargo (Vessel's Manifest)	3.5
3	Vessel Crews and Passengers	3
4	Maritime Areas of Interest	4.3
5	Ports, Waterways, and Facilities	3
6	Environment	3.5
7	Maritime Critical Infrastructure	3.6
8	Threats and Activities	4
9	Friendly Forces Operational Info	3.8
10	Financial Transactions	3

Scale is:

5 = Meets current requirements
4 = Meets most requirements
3 = Can be adapted to meet requirements
2 = Substantial effort to meet requirements
1 = Will not meet requirements (conflicting, not compatible)

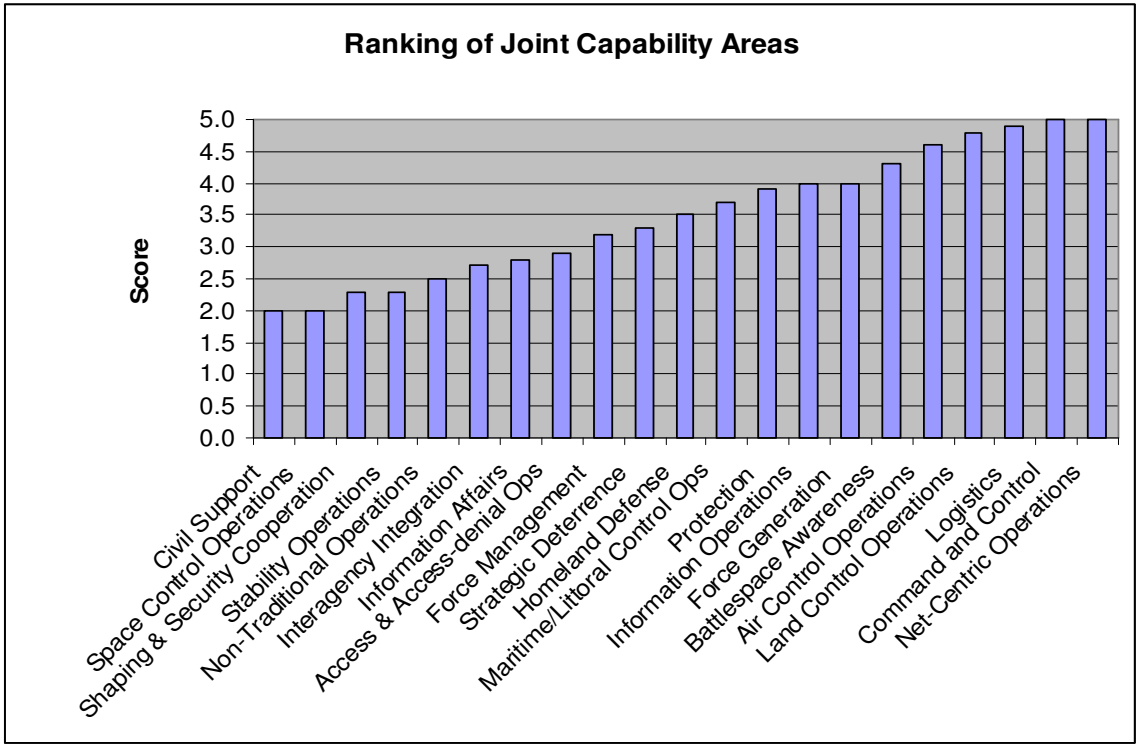
Applicability per JCA Requirements…

Acronym	Joint Capability Areas (JCA)	Score
BA	Battlespace Awareness	4.3
C2	Command and Control	5
NC	Net-Centric Operations	5
II	Interagency Integration	2.7
IA	Information Affairs	2.8
IO	Information Operations	4
FP	Protection	3.9
FL	Logistics	4.9
FG	Force Generation	4
FM	Force Management	3.2
HD	Homeland Defense	3.5
SD	Strategic Deterrence	3.3
SS	Shaping & Security Cooperation	2.3
SO	Stability Operations	2.3
CS	Civil Support	2
NT	Non-Traditional Operations	2.5
AO	Access & Access-denial Ops	2.9
LC	Land Control Operations	4.8
MC	Maritime/Littoral Control Ops	3.7
AC	Air Control Operations	4.6
SC	Space Control Operations	2

Scale is:

- **5 = Meets current requirements**
- **4 = Meets most requirements**
- **3 = Can be adapted to meet requirements**
- **2 = Substantial effort to meet requirements**
- **1 = Will not meet requirements (conflicting, not compatible)**

Applicability per JCA Requirements…



Scale is:

- **5 = Meets current requirements**
- **4 = Meets most requirements**
- **3 = Can be adapted to meet requirements**
- **2 = Substantial effort to meet requirements**
- **1 = Will not meet requirements (conflicting, not compatible)**

Applicability Summary…

Composite scores of all mission areas:

Coverage	Tasking Area	Score
National	NSMS (RDD Scenario)	3.8
Global	Global Maritime Community of Interest	3.7
Joint	Joint Capability Area	3.5

Scale is:

5 = Meets current requirements
4 = Meets most requirements
3 = Can be adapted to meet requirements
2 = Substantial effort to meet requirements
1 = Will not meet requirements (conflicting, not compatible)

- **Failings of the GH5 IEDM were a lack of domain and report information focus, rather than any architectural short comings.**
- **Based on the shortfalls indicated in this research, further efforts were recommended to develop a light-weight framework to address IEDM shortcomings (e.g., CIEF).**