10TH INTERNATIONAL COMMAND AND CONTROL RESEARCH AND TECHNOLOGY SYMPOSIUM THE FUTURE OF C2

Title: **Applying the NCW Conceptual Framework to FORCEnet: A Case Study**

Topic: Assessment, Tools and Metrics

Name of Author(s): Mr. Edgar Bates, Dr. Michael Bell

Point of Contact: Mr. Edgar Bates
Name of Organization: Office of the Chief of Naval Operations
Complete Address:
FORCEnet Innovation, Architecture and Standards
Chief of Naval Operations (OPNAV N71F)
NC-1, Suite 5471 2511 Jefferson Davis Highway
Arlington, VA 22202

Telephone: (703) 601-1405
E-mail Address *edgar.bates@navy.mil*

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
JUN 2005		**00-00-2005 to 00-00-2005**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Applying the NCW Conceptual Framework to FORCEnet: A Case Study	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Chief of Naval Operations (OPNAV N71F),Forcenet Innovation, Architecture and Standards,2511 Jefferson Davis Hwy NC-1 Suite 5471,Arlington,VA,22202**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES
The original document contains color images.

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**		**61**	

ABSTRACT

FORCEnet, the Naval implementation of network-centric warfare, in order to deliver the necessary capabilities in a timely and affordable way, requires an investment strategy that is based on objective analysis. Accordingly, a logical and comprehensive framework for FORCEnet analysis has been developed by combining a capability-based description of FORCEnet with the Conceptual Framework for Network Centric Warfare developed by the Office of the Secretary of Defense. The present paper documents the application of this analysis approach to several aspects of the FORCEnet initiative, including resource and requirement decisions in the planning, programming, budgeting and execution (PPBE) process, analysis of FORCEnet Fleet experiments, support of architecture and standards development, evaluation of tactics, techniques, and procedures (TTP), alignment of science and technology (S&T) and research, development, test, and evaluation (RDT&E) efforts with FORCEnet requirements, and evaluation and selection of modeling and simulation (M&S) tools and scenarios. The results demonstrate how the proposed metrics can be used to assess the improvement in FORCEnet capabilities over time, identify capability gaps, and guide acquisition and technology investments to close those gaps. Finally, the paper summarizes the challenges in applying the metrics.

INTRODUCTION

The evolving concept of network-centric warfare (NCW) may well revolutionize the nature of military operations in the same way as the introduction of gunpowder, armored vehicles, and aircraft into the battlespace. Information and communication technologies enable many of the new capabilities, and experts have characterized Operation Iraqi Freedom as the most technology-intensive military campaign in history, putting to the test the transformational capabilities of NCW, especially in regard to distributed command and control. NCW draws upon resources including people, platforms, systems, and organizational processes in ways that provide unprecedented flexibility and agility to warfighters and combines these resources to provide tailored "packages" of capabilities to meet transient operational requirements in complex, dynamic environments.[1] FORCEnet is the Naval implementation of NCW and the enabling capability for a fully networked naval force, connecting it to the similarly networked joint force that will be linked together by the IP-enabled, Global Information Grid. FORCEnet will facilitate increased situational awareness and enhanced decision support. It focuses on information flow throughout the battlespace, providing distributed enterprise services over advanced networks that create an information infrastructure to move information acquired by intelligence, surveillance, and reconnaissance (ISR) and fusing actionable information into common operational and tactical pictures.

---

[1] See Alberts, David S., *Information Age Transformation: Getting to a 21st Century Military*, Washington, DC: CCRP. 2002

FORCEnet requires an investment strategy based on objective analysis that delivers the necessary capabilities in a timely and affordable way. In response to this demonstrated analysis requirement, a comprehensive framework has been developed by combining a capability-based description of FORCEnet with the Conceptual Framework for Network Centric Warfare developed by the Office of the Secretary of Defense. The framework and associated attributes, measures and metrics were described in a previous paper, "How Much is a Pound of C4ISR Worth? An Assessment Methodology to Evolve Network Centric Measures and Metrics: FORCEnet Case Study," presented at the 8th ICCRTS. The present paper documents the application of this analysis approach to several aspects of the FORCEnet initiative, including resource and requirement decisions in the planning, programming, budgeting and execution (PPBE) process, analysis of FORCEnet Fleet experiments, support of architecture and standards development, evaluation of tactics, techniques, and procedures (TTP), alignment of science and technology (S&T) and research, development, test, and evaluation (RDT&E) efforts with FORCEnet requirements, and evaluation and selection of modeling and simulation (M&S) tools and scenarios.

Framework for Assessment

The notion that objective, quantitative analysis is required in shaping an investment strategy is particularly true for FORCEnet, which is not a system or program but a set of capabilities that will enable network centric operations and warfare. A framework for analysis for FORCEnet has been created that is consistent with the Conceptual Framework (CF) for Network Centric Warfare (NCW) being developed by the Assistant Secretary of Defense for Networks, and Information Integration (ASD/NII) and the Office of Force Transformation (OFT).[2] The NCW CF has been combined with a capability-based description of FORCEnet to yield a set of attributes and corresponding quantitative measures for each capability. These attributes and measures have been applied as broadly and consistently as possible in assessing every aspect of FORCEnet development. The framework has been successfully applied to modeling and simulation, experimentation, program assessment, experimentation, human systems integration (HSI), and science and technology (S&T) planning.

A net-centric measurement scheme evaluating the performance of the infospaces and the underlying infrastructure is based on how well the information demands are being met, as opposed to simple technical measurements (bandwidth, processing speed, etc.). In such a scheme, the core of data interoperability is whether the various infospace members are being supplied with the information they need to complete their missions successfully. In particular, one evaluates whether the quality of the provided information is sufficient to create the required knowledge, which in turn creates the required understanding needed

---

[2] The NCW Conceptual Framework is an ongoing initiative co-sponsored by the Office of Force Transformation and NII's Command and Control Research Program. The most recent briefing on the Framework is: Signori, David, et al, "A Conceptual Framework for Network Centric Warfare," Proceedings of the Network Centric Warfare / Network Enabled Capabilities Workshop, December 17-19, 2002. Available from http://www.dodccrp.org.

to execute missions in desirable ways. The Network Centric Warfare (NCW) Conceptual Framework describes measures and metrics to evaluate the quality of information. The Framework identifies both *objective* metrics, which provide context-free measurements of an attribute, and *fitness for use* metrics, which evaluate the measurements with respect to mission requirements. In the case of FORCEnet, a hierarchical capability taxonomy has been developed and refined over the past two years to articulate aspects of what comprises "FORCEnet." This hierarchy consists of six capabilities at the top level as described in Appendix A. These six capabilities are:

- Provide expeditionary, multi-tiered sensor and weapon information
- Conduct distributed, collaborative command and control
- Provide dynamic, multi-path and survivable networks
- Provide adaptive/automated decision aids
- Provide human-centric integration
- Provide information effects

For our purposes, we define a capability as that combination of human, technological, organizational, process, and cognitive elements that provides the means to achieve a clearly articulated outcome in a defined context. While the measures and metrics described in Appendix A provide a set of potentially useful types or templates, measures applied in a specific case can be drawn from the growing body of existing and evolving activities in the naval and joint communities. In particular, recent guidance from Joint Chiefs of Staff defines a top down capabilities identification methodology that provides a method to identify gaps in warfighting capabilities and assess associated risk(s). [3] The hierarchy is also valuable as a method for quantifying the benefits of FORCEnet. Thus, on the "radar graph" (Kiviat diagram) shown in Figure 1, the dotted line should move outward as each of the capabilities matures toward the desired end-state. Furthermore, each of the capabilities can be analyzed to see which experimental treatments or other changes were responsible for an improvement.

[3] CJCSI 3170.01C states: "(1) Capability definitions must contain the following elements: key characteristics(attributes) with appropriate parameters and metrics, e.g., time, distance, effect (including scale), obstacles to be overcome, and supportability. (2) Capability definitions should be general enough so as not to prejudice decisions in favor of a particular means of implementation, but specific enough to evaluate alternative approaches to implement the capability."

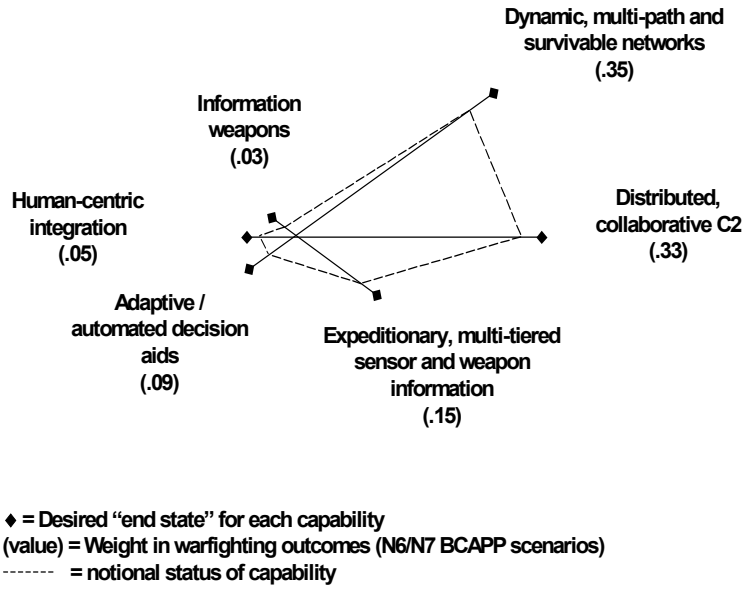


Figure 1 Measuring FORCEnet Capability

Normally, the axes of a Kiviat diagram are of equal length. In Figure 1, however, the axes have been scaled according to the weight given to the capability it represents by a group of senior warfighters who were asked to assess the contribution of FORCEnet capabilities to the outcome of the campaign scenario used in developing the PR-05 submission. (These weights are shown in parentheses in Figure 1.) As a result of this scaling, equal distances on the axes (representing capability changes or differences) correspond to equal impacts on warfighting outcomes.

The framework when coupled with the analysis associated with the budget process provides a start at understanding the FORCEnet return on investment.

Joint Capabilities Development Process

The Joint Capabilities Integration and Development System (JCIDS), CJCSI 3170.01C, is based on the need for a joint concepts-centric capabilities identification process. JCIDS can be used to assess FORCEnet capabilities in light of their contribution to future joint concepts The procedures established in the JCIDS support the Chairman of the Joint Chiefs of Staff (CJCS) and the Joint Requirements Oversight Council (JROC) Additionally, JCIDS considers the full range of joint resources which include doctrine, organization, training, materiel, leadership and education, personnel, and facilities (DOTMLPF). Functional Capability Boards (FCBs) provide oversight and assessment as appropriate to ensure the sponsor's analyses are taking into account joint capabilities, concerns, and approaches to solutions. The FCBs provide the JROC a context briefing to explain where a given capability proposal fits within a functional area, and make recommendations on validation and approval. The following FCBs: C2, Battlespace Awareness, and Net Centric are aligned with FORCE net capabilities. In particular, the C2 FCB which is responsible for the organization, analysis, and prioritization of joint

warfighting capability needs within the assigned command and control functional area is also tasked with developing a network centric conceptual framework, including capabilities, attributes, measures and metrics that apply to all other functional areas. Also, it must enforce net centric standards (e.g. the Net-Ready Key Performance Parameter, the Network Centric Data Strategy, and the Net Centric Operations and Warfare Reference Model) that cut across all of the FCBs. The Functional Concepts focus primarily on the operational level of war and describes activities will be performed to achieve success when executing missions and operations described in the Joint Operating Concepts.[4] These concepts also provide the measurement framework for evaluating the command and control investment options needed to implement the functional capabilities, and for assessing those investment decisions.

For example, of primary importance in defining C2 capabilities will be the Joint Command and Control Functional Concept. The current draft of the Joint C2 Functional Concept (revision date 31 October 2003), identifies the current capabilities and attributes being supported. The Joint Battle Management Command and Control (JBMC2) initiative clusters programs that support the joint mission threads.

Naval Capabilities Development Process

The Deputy Chief of Naval Operations for Warfare Requirements and Assessments (N6/N7) is the executive agent and lead for focusing capability-driven warfighting requirements to enhance the ability to communicate a long-term warfighting vision that shapes research and development, procurement, force structure, and capabilities to counter threats and achieve mission success. High level guidance and a variety of more focused concepts allows the Services to identify the capabilities that will be required to succeed against a wide variety of threats. As separate Services, the Navy and Marine Corps each then have distinct force development methods that allow them to maximize the value of the core competencies brought to joint force development. The Navy's Naval Capability Development Process (NCDP) includes extensive participation by Navy and Marine Corps warfighters to identify, validate, and prioritize Navy capabilities required by the joint force. The NCDP establishes Warfare Sponsors for four Naval Capability Pillars who are responsible for developing Mission Capabilities Packages (MCPs) within specific mission-area domains (e.g., Homeland Security), which cross and link platform-specific communities (e.g., Naval Aviation), and coordinating the MCPs with resource sponsors, Fleet, and the acquisition community. The MCPs serve as the primary mechanism to identify the current baselines of capabilities and to forecast capability evolution, thus contributing to comprehensive planning and programming for integrated systems capabilities identified in Navy and Joint Service strategies.

Each Warfare Sponsor is responsible for the identification of capability gaps, issues and program priorities in their assigned Naval Capability Pillar, and for recommending alignment of programs to optimize overall performance in that pillar in an output brief called the Naval Capability Plan (NCP). The FORCEnet Warfare Sponsor who is the Director of Network Centric Warfare (N71) is supported in this role by an analytic staff,

[4] See **http://www.dtic.mil/jointvision/jointfc.htm** for the latest version of the Functional Concepts

elements of the Office of Naval Research, and the Commander Space and Warfare Systems Command, and such other warfare centers as necessary. Tasks associated with NCDP include establishing the baseline assumptions, threats and scenarios and the scope of capabilities and programs encompassed by each MCP. OPNAV N6/N7 establishes procedures with ASN(RDA) for PEOs to provide the technical and program data that the Systems Commanders and Warfare Sponsors require to conduct the analysis for each MCP. Furthermore, OPNAV N6/N7 provides guidance concerning the capability requirements and their priorities, force structure, fiscal constraints etc. that the Systems Commanders and PEOs should use in their analysis and inputs. The Systems Command Commanders evaluate their respective major acquisition programs and legacy systems on the basis of a set of characteristics (redundancy, interoperability, cost, schedule, performance etc.) and provide the warfare sponsor a prioritized list of programs on that basis.

The process strives to establish an affordable long-range Integrated Strategic Capability Plan (ISCP) and an Integrated Sponsor's Program Proposal (ISPP) for warfare systems that will meet the operational needs of the fleet. The Integrated Strategic Capability Plan comprises all MCPs and becomes the Navy's "warfare investment", and when consolidated with resource sponsor programming inputs, becomes the Integrated Sponsor's Program Proposal which is then forwarded to N8.

The Naval Transformation Roadmap identified four Naval Capability Pillars (NCP): Sea Strike, Sea Shield, Sea Basing and FORCEnet.[5] For POM development, the FORCEnet NCP was further broken down into three Mission Capability Packages (MCP): Communication & Data Networks, Intelligence, Surveillance & Reconnaissance, and Common Operational & Tactical Picture. The FORCEnet analytic framework in general maps to these areas as follows:

- Intelligence, Surveillance & Reconnaissance
  - Provide expeditionary, multi-tiered sensor and weapon information
- Common Operational & Tactical Picture
  - Conduct distributed, collaborative command and control
  - Provide dynamic, multi-path and adaptive/automated decision aids
  - Provide human-centric integration
- Communication & Data Networks
  - Provide dynamic, multi-path and survivable networks
  - Provide information effects

Modeling and Simulation (Campaign Analysis)

The annual Navy budget proposal is supported by simulation-based analysis of one or more theater-level campaigns. Prior to work on POM-06, these campaign analyses were based on the assumption of "perfect" C4ISR. That is, models were used in which the behavior of entities in the simulation was determined by ground truth, not by the commander's perception of the battlespace. This greatly limited the ability of the analyst

[5] http://www.dtic.mil/jointvision/naval_trans_roadmap.pdf

to assess the impact on campaign outcomes of C4ISR system performance in general, and the capabilities of FORCEnet in particular. This difficulty was mitigated somewhat by the use of an ISR systems simulation, the C4ISR Space and Missile Operations Simulator (COSMOS), to generate target detections. These detections were then fed to the campaign-level simulations, the Integrated Theater Engagement Model (ITEM) for the air-land battle or the General Campaign Analysis Model (GCAM) for the maritime campaign.

For the POM-06 campaign analysis, the Naval Simulation System (NSS) [6] was used to model maritime and expeditionary warfare missions. NSS provides a fairly detailed description of sensor performance and communications behavior. More important, it explicitly accounts for the information available to commanders in determining how their units will act. This provided, for the first time, an analytically sound basis for examining the tradeoffs between investments in platforms and weapons on the one hand and C4ISR systems on the other. The level of fidelity that NSS offers in communications modeling has been gradually improved. In addition to point-to-point communications, options for broadcast and multicast communication were added, providing a means to describe IP-based networks. For PR-07 and following campaign analyses, NSS was further enhanced with the addition of dynamic routing capability and both real-time and non-real-time federations with a DoD standard network-modeling tool, the Network Warfare Simulation (NETWARS) [7]. The level of detail that NSS provides in sensing and communications processes makes it impractical to use the model to simulate the entire campaign. Instead, a limited vignette, confined to a restricted geographical area and time period, was used. This vignette was selected on the basis that it would be the most stressing on C4ISR systems.

In summary, the C4ISR modeling capability provided by NSS (when combined with NETWARS, COSMOS, and the other models) permitted the addressing of high-level, generic questions regarding specific areas of interest within the FORCEnet analytic framework.

Science and Technology (S&T)

The FORCEnet S&T program is a formal process led by OPNAV. The OPNAV FORCEnet Pillar lead directs the ONR Future Naval Capability and Discovery & Invention process to assist ONR in crafting an S&T investment strategy responsive to desired Fleet capabilities.

To provide the greatest capability for the Navy given limited funding, the Future Naval Capabilities (FNC) S&T development program are focused on naval warfighting gaps as identified by the Naval Capabilities Development Process (NCDP). In coordination with the FNC IPTs, ONR analyzes the proposed gaps and develops Enabling Capabilities (ECs) or recommends adjustments to existing ECs to close Naval gaps. ONR and the FNC IPTs work closely together to ensure that EC proposals properly

[6] http://www.metsci.com/pages/ssd.html
[7] http://www.opnet.com/products/library/netwars_models.html

address the gap and that the products are aligned and developed to support transition. These proposals identify a series of ECs that will fill the gap. ECs are a collection of S&T projects that complete in three to five years and deliver a measurable increment of improved capability to the Fleet. ONR may recommend available commercial or non-S&T alternatives in lieu of developing or adjusting an EC.

FORCEnet S&T is coordinated closely with operational, requirements, experimentation, and acquisition communities to ensure technology projects meet critical warfighter needs, have superior transition potential, and are co-evolved with doctrine, organization, training, materiel, leadership, personnel, and facilities (DOTMLPF).

For POM 06, the S&T gaps that were derived from the MCP/NCDP gaps and the relationship to the FORCEnet capabilities are as follows:

- Intelligence, Surveillance & Reconnaissance
  - Provide expeditionary, multi-tiered sensor and weapon information
    - Persistent Intelligence, Surveillance, Reconnaissance, and Targeting (ISRT) for Accurate Target Discrimination and Location
    - Optimal Mix of Naval Sensors to Complement Joint and National Capabilities to Meet Naval Mission Requirements
- Common Operational & Tactical Picture
  - Conduct distributed, collaborative command and control
    - Common and Persistent Maritime Picture on/below the Surface (i.e. capability to network ISR data)
  - Provide dynamic, multi-path and adaptive/automated decision aids
    - Joint Combat ID (i.e. capability to automate, merge, and display the full range of Blue force tracking capability)
  - Provide human-centric integration (Note: Separate ONR effort)
- Communication & Data Networks
  - Provide dynamic, multi-path and survivable networks
    - Ubiquitous, Secure Communications and Network Infrastructure
    - Link Management and Architecture
    - Computer Network Defense and Information Assurance
  - Provide information effects (Note: Not considered by S&T in FORCEnet Pillar)

Although Existing FNC projects are oriented toward filling the gaps and can generally be regarded as incremental steps toward net-centric capability as opposed to transformational leaps, the full range of S&T within the context of the analytic framework includes: [8]

- Intelligence, Surveillance & Reconnaissance
  - Provide expeditionary, multi-tiered sensor and weapon information

[8] ONR Working Papers

        - Advanced light-weight, small, efficient sensors for variety of platforms (video, IR, SAR, chem/bio, etc)
            - Flexibility in search / ID
            - Multi-modal
        - Automated processing at sensors and sensor networks (triage, assessment, and control)
        - Integrated modules including on-board processing and control
        - Automated control and tasking of sensors and sensor networks including optimization of resources and COTP development
        - Four-dimensional navigation data across network with and without GPS

- Common Operational & Tactical Picture
    - Conduct distributed, collaborative command and control
        - Joint Service Oriented Architectures for rapid, interoperable sharing and discovery of mission relevant sensor data and information and joint command and control
    - Provide dynamic, multi-path and adaptive/automated decision aids
        - Automated integration of disparate sensors and sources of information including metadata (eg information source, quality, validity, integrity, priority, degradation) to produce actionable knowledge
        - Automated Courses Of Action with insight into uncertainty and risk particularly for specific scenarios such as urban, guerilla, and terrorist activities and port / force / base protection
    - Provide human-centric integration
        - Highly flexible means of presenting, to warfighter, complex information including uncertainty, geo-spatial, etc from multiple relevant data sources for aiding in assessing intent as well as situation awareness while performing mission

- Communication & Data Networks
    - Provide dynamic, multi-path and survivable networks
        - Develop tools for verifying validity of software functionality both with respect to what it is suppose to do as well as ensure it does not have hidden functionality
        - Develop technologies to enable real-time systems for assured access to information–Where necessary, develop protocols and architectures for dynamic, mobile naval forces
        - Within this architecture, develop mission-driven, quality of service capability
        - Develop tools for automation network which account for battle-space situation, battle-space environment, and commander's intent
        - Enable robust over-the-horizon connectivity
        - Develop necessary aperture technology to ensure continuous platform participation in the network

- Investigate concepts for enhancing underwater communications and for rapidly moving underwater sensor information and data into overall common picture database
- Develop technologies to enable real-time systems for assured access to information
- Enable multiple security levels across same network seamlessly

Experimentation

Sea Trial is a Naval process of integrating emerging concepts and technologies, leading to continuous improvements in warfighting effectiveness and a sustained commitment to innovation. With the fleet as a major partner, the Naval Warfare Development Command develops the Sea Trial Concept Development and Experimentation (CD&E) Campaign Plan to describe a continuum from concept development to wargames, demonstrations, experiments and prototyping. The plan also provides the means to fully integrate new technologies, facilitate initial fleet insertion, and accelerate full-scale production of systems.

Trident Warrior 2004 (TW04), the US Navy's major annual FORCEnet Sea Trial event, was conducted in October 2004. Conceptually, TW04 included new technologies for networks, processes to enable ESG operations, operational procedures that extended to shore-based capabilities, quality of life, and information services for career maintenance. TW04 also explored the means by which human-systems interactions with systems could be better defined and studied—making HSI a veritable component of what FORCEnet systems are intended to become. TW04 took place onboard the TARAWA Expeditionary Strike Group (ESG) off the California coast; at nodes ashore in Ft. Hood, Texas; Fleet Imaging Support Team (FIST), in Maryland; and at locations on San Clemente Island.

Another Sea Trial experiment - Silent Hammer (SH) was loosely linked to TW04. SH was designed to test the concept of a battle management center located on a SSGN. These two experiments were conducted at the same time but executed separately. TW 04 and SH had a common scenario and used common ISR assets. SH and TW04 have published separate analysis and assessment reports. [9] TW04 was organized around the FORCEnet impact in the following ten areas mapped to the FORCEnet analytic framework and the gaps, with important objectives in each listed:

- Intelligence, Surveillance & Reconnaissance
  - Provide expeditionary, multi-tiered sensor and weapon information
    - Persistent Intelligence, Surveillance, Reconnaissance, and Targeting (ISRT) for Accurate Target Discrimination and Location

[9] Additional information may be found in the FORCEnet Innovation and Research Enterprise (FIRE), operated and maintained by Naval Postgraduate School's Department of Information Sciences.

- Improve collaboration and support in a networked environment by "reach-in" to other ISR networked nodes.

❖ Common Operational & Tactical Picture
  - o Conduct distributed, collaborative command and control
    - Common and Persistent Maritime Picture on/below the Surface (i.e. capability to network ISR data)

      - Assess the ESG architecture for fires and develop appropriate changes to TTP.
      - Information Management (IM)/ IM Plan (IMP) – improve collaboration and coordination by improving information flow and documenting the process.
      - Information operations (IO) – evaluate the preparation and distribution of psychological operations (PSYOP) products, management of the electro-magnetic spectrum in an ESG, and other new tools.

  - o Provide dynamic, multi-path and adaptive/automated decision aids

    - Joint Combat ID (i.e. capability to automate, merge, and display the full range of Blue force tracking capability)

      - Demonstrate the capability to use service-oriented architecture (SOA) to successfully ingest other-service Blue force tracking (BFT) tracking information and determine issues needing resolution.

  - o Provide human-centric integration

      - Assess the effectiveness of the Web-enabled warrior (WEW) Navy-Marine Corps Portal (NMCP) and a distributed server architecture, among other new systems, in supporting tactical forces
      - Assess the accessibility of the Navy Knowledge On-Line (NKO) portal and the 5 Vector Model for career management
      - Explore the treatment of knowledge gaps with resources brought by FORCEnet capabilities; measure knowledge inventory of watchstanders and propose relationships to other performance metrics.
      - Assess Human systems integration (HSI) efficiency in utilization of FORCEnet systems by the warfighter, shared situational awareness of collaborative teams, and speed of command in using multi-tiered sensor and weapon information.

❖ Communication & Data Networks
  - o Provide dynamic, multi-path and survivable networks

- Ubiquitous, Secure Communications and Network Infrastructure

- Networks, Information Management (IM)/Information Management Plan ((IMP) – increase data throughput by improving bandwidth management and provide multi-path, multi-tiered network architecture.

Trident Warrior 05 will focus on distributed C2 and associated Techniques, Tactics and Procedures (TTP) and will have an ISR emphasis. Specifically, the two most significant demonstrations will be Global Hawk Maritime Demonstration and Network Centric Collaborative Targeting ACTD (which will use the Trident Warrior venue as a "graduation event"). Coalition participation (AUSCANNZUKUS) both real and virtual is planned.

There is a direct linkage between FORCEnet experimentation and the NCDP process. For example, TW03 results demonstrated the value of the FORCEnet analytic framework and the experiment objectives were mapped directly to the FORCEnet capabilities. Specifically, the Intra BG Wireless Networking coupled with upgraded shipboard fail-over resulted in improved connectivity. TW04 objectives were mapped to the NCDP capability gaps. The results justify the relative increases in Integrated Shipboard Network Systems, JTRS, Tactical switching and the SATCOM programs in general. TW05 objectives will be closely mapped to the NCDP and in addition will emulate to the extent possible the same scenarios in order to better support the NCDP analysis with the integration of empirical data (specifically with respect to human systems integration).

Human systems integration (HSI)

Human systems integration (HSI) plays an important role in efforts to create systems that accommodate human performance characteristics. HSI can be defined as a comprehensive management and technical strategy to integrate human considerations early in the system design, development, and demonstration process. HSI assists with the total system approach by focusing attention on the human part of the total system. Its major goals are to improve total system performance and reduce costs of ownership. Failure to take HSI into account during system design and implementation often results in systems that are difficult to learn and operate reliably and efficiently requiring later, expensive modifications to system design after fielding. HSI addresses several elements associated with system design, development, and implementation, including manpower, personnel, training, human factors engineering, safety, health hazards, and survivability. Together, these elements define how human users affect a system (in terms of effectiveness, operation, and support and their associated costs) and how a system affects the humans (*e.g.*, operators, maintainers, supporters, and trainers) who interact with it.

In order to assess FORCEnet processes and their component technologies during TW03, warfighting attributes in terms of human performance variables were defined. Five HSI analytic elements were used: Performance, User Interface, Information Transfer, Training, and Manpower and Personnel. Together, these five HSI elements furnished the

foundation needed to formulate and implement an analytic plan that enabled meaningful HSI assessments of the technological systems used during TW03 in support of FORCEnet objectives.

Experimentation lends itself particularly to the analysis of empirical data that supports the Navy's investment strategies, mainly because as systems become more complex, the end-to-end solution requires an understanding of the capabilities and limitations of the human in the loop. Put another way, experimentation is an opportunity to take the results of Modeling and Simulation and examine the results from a behavioral context. Because FORCEnet systems rely upon the performance of human operators and/or maintainers, HSI issues need to be examined along with the technical aspects of the systems themselves as part of the total systems engineering approach

Summary

Not only has the FORCEnet analytical framework made an important contribution to the assessment of NCW in the naval domain, it also has potential application in the joint, interagency, allied, and coalition environments. These applications, as well as the continued utility of the framework in assessing progress toward the goals of FORCEnet implementation, will depend upon the establishment of sound and stable definitions of the capabilities FORCEnet is expected to deliver.

The annual FORCEnet Analysis Report will use this framework to measure improvement in FORCEnet capabilities based upon the objective results from experimentation, SYSCOM assessments, M&S results, and other assessments.[10] This initial report establishes the baseline from which future improvement in FORCEnet capabilities can be assessed.

FORCEnet has been regarded as key to achieving interoperability with the other services, our allies and coalition partners. The benefits to joint operations have been explored in the campaign analysis and at-sea experiments, but the issues of allied and coalition interoperability have received less attention. Two initiatives are planned in this area, one involving an excursion to the campaign analysis scenario and the other based on participation in the Trident Warrior 05 experiment by the navies of the Australia, Canada, New Zealand, and the United Kingdom through the AUSCANNZUKUS C4C organization.

This paper has provided a foundation for an assessment framework involving C4ISR processes in FORCEnet. This framework reflects and expands upon work done by a number of organizations engaged in efforts to structure a process that links traditional and evolved C4ISR attributes, measures, and metrics to network centric outcomes. Not only has the FORCEnet analytical framework made an important contribution to the Naval domain, but can potentially be used in the Joint environment. The FORCEnet analytic framework can effectively measure improvement in FORCEnet capabilities based upon

[10] Additional information may be found in the FORCEnet Innovation and Research Enterprise (FIRE), operated and maintained by Naval Postgraduate School's Department of Information Sciences.

the objective results from experimentation, SYSCOM assessments, M&S results, and other assessments. Initial use of the framework has established the baseline from which improvement in FORCEnet capabilities can continue to be measured.

Appendix A

To facilitate analyses related to FORCEnet capabilities, an initial analytical framework has been developed that is consistent with Assistant Secretary of Defense for Networks, and Information Integration (ASD (NI2)) NCW concepts and analytical resources. This framework further couples newer concepts with existing metrics and systems performance assessment criteria associated with the Universal Joint Task List (UJTL) and service based Mission Essential Task Lists (METLs). A number of traditional measures and metrics also may be applied to analysis of the FORCEnet core capabilities. Table 1 includes descriptions of the six FORCEnet core capabilities and identifies "assessment criteria" that reflect the mapping of C4ISR operational attributes to notional metrics. These metrics have been drawn from an initial review of several C4ISR research efforts which include a recent C2 Concepts and Experimentation Literature Review sponsored by the Joint C4ISR Decision Support Center, the Joint C4ISR Battle Center's Assessment Methodology, the ASD/C3I Architecture Working Group, the National Security Agency/Defense Information Systems Agency sponsored Information Assurance Technical Framework, and Defense Planning Guidance. In general, the metrics are evolving, and it should be recognized that in some cases an attribute could be further operationalized in order to develop a meaningful metric. Many of the metrics and measures mentioned earlier in the paper provide additional candidates for inclusion in the evolving framework as well.

1. Provide expeditionary, multi-tiered sensor and weapon information: The expeditionary, multi-tiered sensor and weapons grid capability uses a full spectrum of manned and unmanned vehicles, platforms, sensors and weapons to provide the Force Commander with what is needed to locate targets and attack them across the depth and breadth of a theater-sized battlespace. Sensors must determine their position, time and movement at the precise time they are reporting their target or other intelligence information. The time and position information of the track provided by sensors in the grid must be properly attributed (e.g., linked to a standard reference frame with uncertainty (error) and confidence level) for it to be accurately understood, represented and fused with other data / information. Many modern weapons are also dependent on precise time and position (including uncertainty) for effective operation.

Attribute	Notional Metric
Accuracy	Correspondence with ground truth-correlation coefficient (0= no correspondence with ground truth, 1= full correspondence with ground truth). Data matrix comprised of relevant information items estimates (for instance: detection, ID, velocity, location, heading, etc.)
Consistency	Degree of lack of ambiguity with previous information
Completeness	Percentage of ground truth relevant and necessary for ongoing task
Precision	Error and confidence level for time and position information compared to a standard reference

Timeliness	Degree to which currency matches what is needed (0=no match, 1=high degree of matching between currency level needed and available)

2. Conduct distributed, collaborative Command & Control: To collaboratively manage land, air, sea, and space operational forces in time, space, and purpose to produce maximum relative combat power and minimize risk to own forces. This activity ensures all elements of the operational force, including supported agencies' and nations' forces, are efficiently and safely employed to maximize their combined effects beyond the sum of their individual capabilities.

Attribute	**Notional Metric**
Shared Situational Awareness	Degree to which the different individual mental models of the situation are integrated into a common operational picture.
Quantity of Posted Information	Percent of collected information posted
Quantity of Retrievable Information	Percentage of nodes that can retrieve various sets of information.
Understandability	Degree to which information is easy to use (0=low degree of ease of use, 1=high degree of ease of use)
Precision	Error and confidence level for time and position information compared to a standard reference
Timeliness	Degree (speed of effect) to which currency matches what is needed (0=no match, 1=high degree of matching between currency level needed and available)

3. Provide dynamic, multi-path and survivable networks: To provide data and information flow seamlessly and transparently to the warfighter across a fault tolerant, adaptable, self-organizing, holistically engineered continuously available network. The data and information flows across a wide range of transmission paths in an interoperable manner with naval, joint, coalition and civil / law enforcement agencies. Platforms and vehicles are able to communicate freely and autonomously with other elements of the architecture thus the existence and functions of the underlying network are transparent to the warfighter.

Attribute	**Notional Metric**
Capacity	Throughput (1) effective systems capacity = maximum data rate - system overhead rate (2) bandwidth utilization = available data rate / effective systems capacity
Reach	Percentage of nodes that can communicate in desired access modes, information formats, and applications
Connectivity	Percentage of time that all required nodes are connected to the network
Information Assurance	Extent to which node supports the assurance of information in the areas of privacy, availability, integrity, authenticity, and non-

	repudiation
Quality of Service	Measures of jitter, packet loss and latency
Timeliness	Degree (speed of effect) to which currency matches what is needed (0=no match, 1=high degree of matching between currency level needed and available)
Agility	Extent to which the network can maintain QOS in response to environmental changes (incorporates robustness, responsiveness, flexibility, innovativeness and adaptation)
Robustness	Number of differing conditions/environments over which network is capable of operating at a given level of effectiveness (baseline level determined by SME, simulation, analysis, empirical analysis, etc.) Effectiveness of network across varying levels of attack/degradation (baseline level determined by SME, simulation, analysis, empirical analysis, etc.) Number of tasks/missions, which the network is capable of operating at a given level of effectiveness (baseline level determined by SME, simulation, analysis, empirical analysis, etc.)
Responsiveness	The timeliness of the response to an environmental change (baseline level determined by SME, simulation, analysis, empirical analysis, etc.)
Flexibility	Number of options for responding to an environmental change Compatibility of different responses (0=not compatible, 1=fully compatible; determined by SME, simulation, analysis, empirical analysis, etc.)
Innovativeness	Number of novel responses developed and implemented (baseline determined by SME, simulation, analysis, empirical analysis, etc.)
Adaptiveness	Number and timeliness of changes to network structure and processes (baseline determined by SME, simulation, analysis, empirical analysis, etc.)

4. Provide adaptive / automated decision aids: To support warfighter decision making by providing recommended courses of action that are adaptive and based upon knowledge of the operational context, commander's intent, rules of engagement, order of battle, etc. and evolution of the battlespace landscape	
Attribute	**Notional Metric**
Robustness	Degree to which decision aids support decision making across a range of situations and degradation conditions
Responsiveness	Degree to which decision aids support decision making which is relevant and timely
Innovativeness	Degree to which decision aids support decision making that reflects novel ways to perform known tasks

Adaptability	Degree to which decision aids support a decision making process with the flexibility to alter decision making in response to the evolution of the battlespace landscape
Consistency	Extent to which decision aids support decision making are internally consistent with prior understanding and decisions
Currency	Extent to which decision aids support decision making that minimizes latency (e.g. Notification - Time of detection = Cueing Time, Time of detection – receipt of refined positional estimate = Update rate, Time of cueing data – time of weapon firing = weapons release time, Firing report received by group commander – weapons firing time = Firing report time)
Precision	Error and confidence level for time and position information compared to a standard reference
Fitness for Use	Relative quality in reference to criteria that are determined by the situation
Appropriateness	Extent to which decision aids support decisions that are consistent with existing understanding, command intent and values
Completeness	Extent to which decision aids support relevant decisions that encompass the necessary: • Depth: range of actions and contingencies included • Breadth: range of force elements included • Time: range of time horizons included

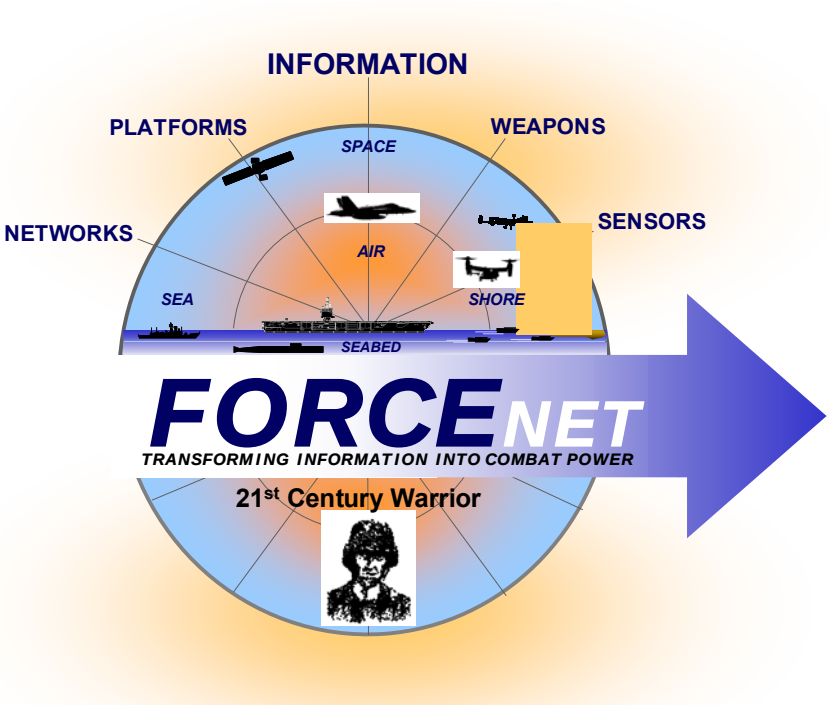
5. Provide human-centric integration: Enhance the ability of warriors to multi-task through all phases of warfare while taking advantage of improved Human-Computer Interfaces which dynamically assign function to human and information systems that best leverage the relative strengths of each (e.g., human decision making in uncertain/ambiguous circumstances, computer systems in situations relying upon high speed complex calculations).

Attribute	**Notional Metric**
Competence	Distribution of members' knowledge, skills, abilities and attitudes.
Trust	Extent to which members are willing to rely on one another
Confidence	Extent to which members have expectations of the reliability of the organization
Size	Number of team members involved adequate to support mission
Experience	Degree to which team members have interacted in the past on the same task
Diversity	Degree to which team members are heterogeneous or homogeneous across exogenous variables: experience, age, gender, etc.

Autonomy	Extent to which organization is externally or self directed
Structure	• Numbers of layers of authority • Functional Differentiation Effectiveness
Interdependence	Extent to which members depend on one another for resources
Cooperation	Extent to which member(s) are willing and able to work together
Efficiency	Extent to which members utilize one another's resources so as to minimize costs and maximize benefits
Synchronization	Extent to which organization is conflicted, deconflicted, or synergistic
Engagement	Extent to which all members actively and continuously participate
Risk Propensity	Extent of risk aversion

6. Provide information weapons: To integrate the use of military deception, psychological operations, electronic warfare, and physical destruction, mutually supported by intelligence, in order to deny information, influence, degrade, or destroy adversary information, information-based processes, and information systems. (Metrics are under development.)	
Attribute	**Notional Metric**
Lethality	Extent of capability to precisely deliver desired Non-Kinetic (NK) Information Operations (IO) effects.
Coverage	Extent of capability to accomplish IO effects.
Persistence	Extent of capability to sustain IO effects.
Timeliness	Extent of capability to deliver desired NK IO effects at a desired time.
Survivability	Extent of capability to avoid enemy threats, counter ISR, and employ IO techniques to reduce targeting of adversary kinetic systems allowing increased secure maneuvering by ASMD/Deny ISR/SEAD/Networks.

Table 1 FORCEnet Capability Descriptions, Attributes and Metrics



Analysis for Network Centric Warfare in the Navy

Mr. Edgar Bates
Dr. Michael Bell

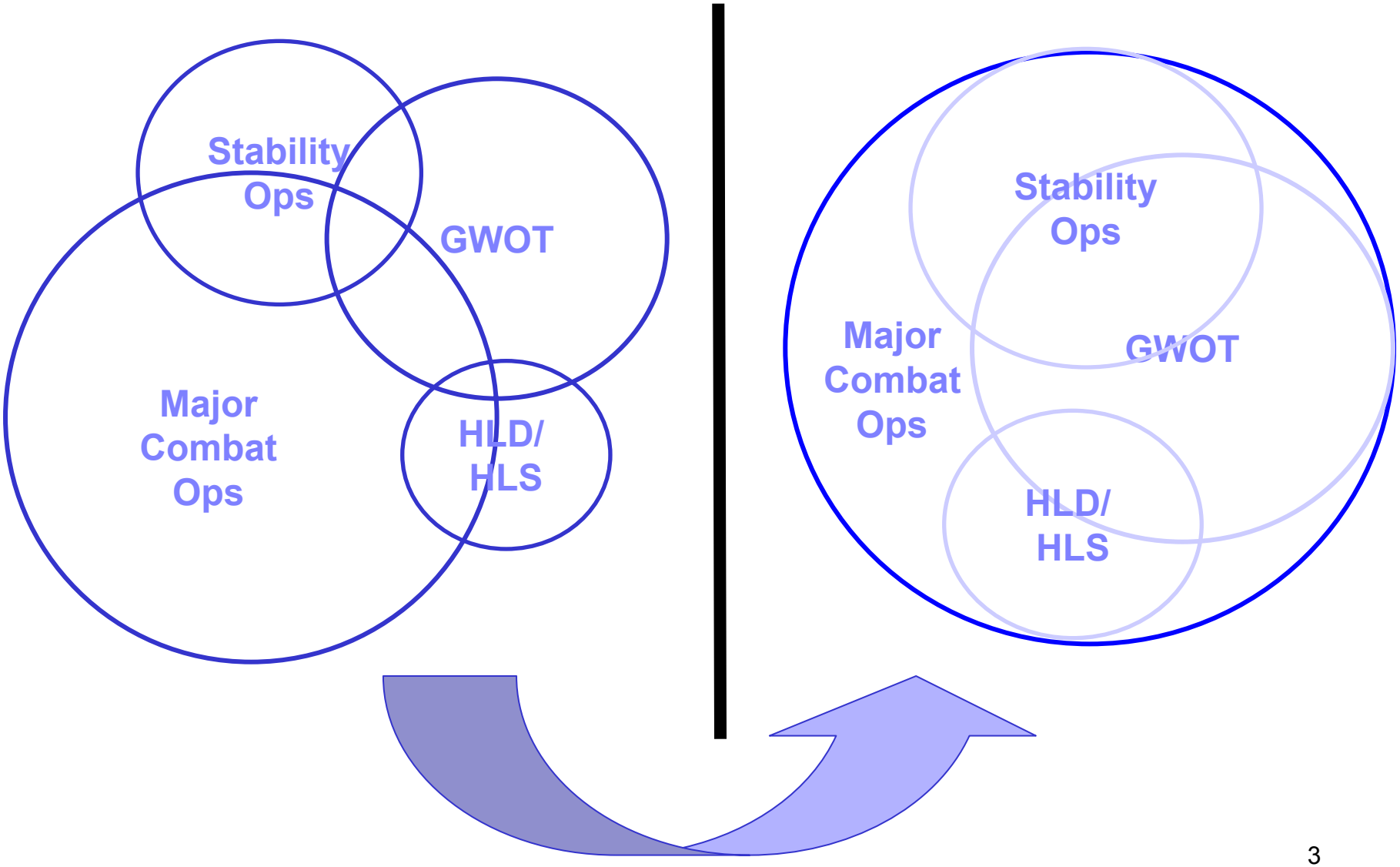
Chief of Naval Operations (N71F)

10th ICCRTS
13 June 2005

Outline

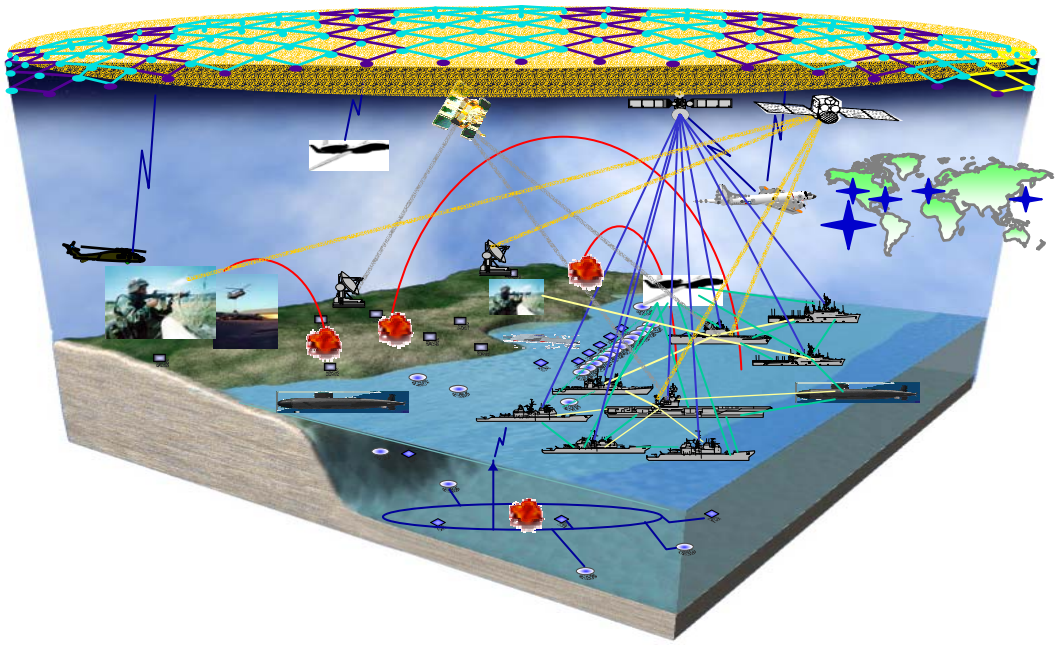
- FORCEnet analysis framework
- Examples
  - M&S and Campaign Analysis
  - Experimentation
  - Science and technology
- Conclusions

Naval Transformation



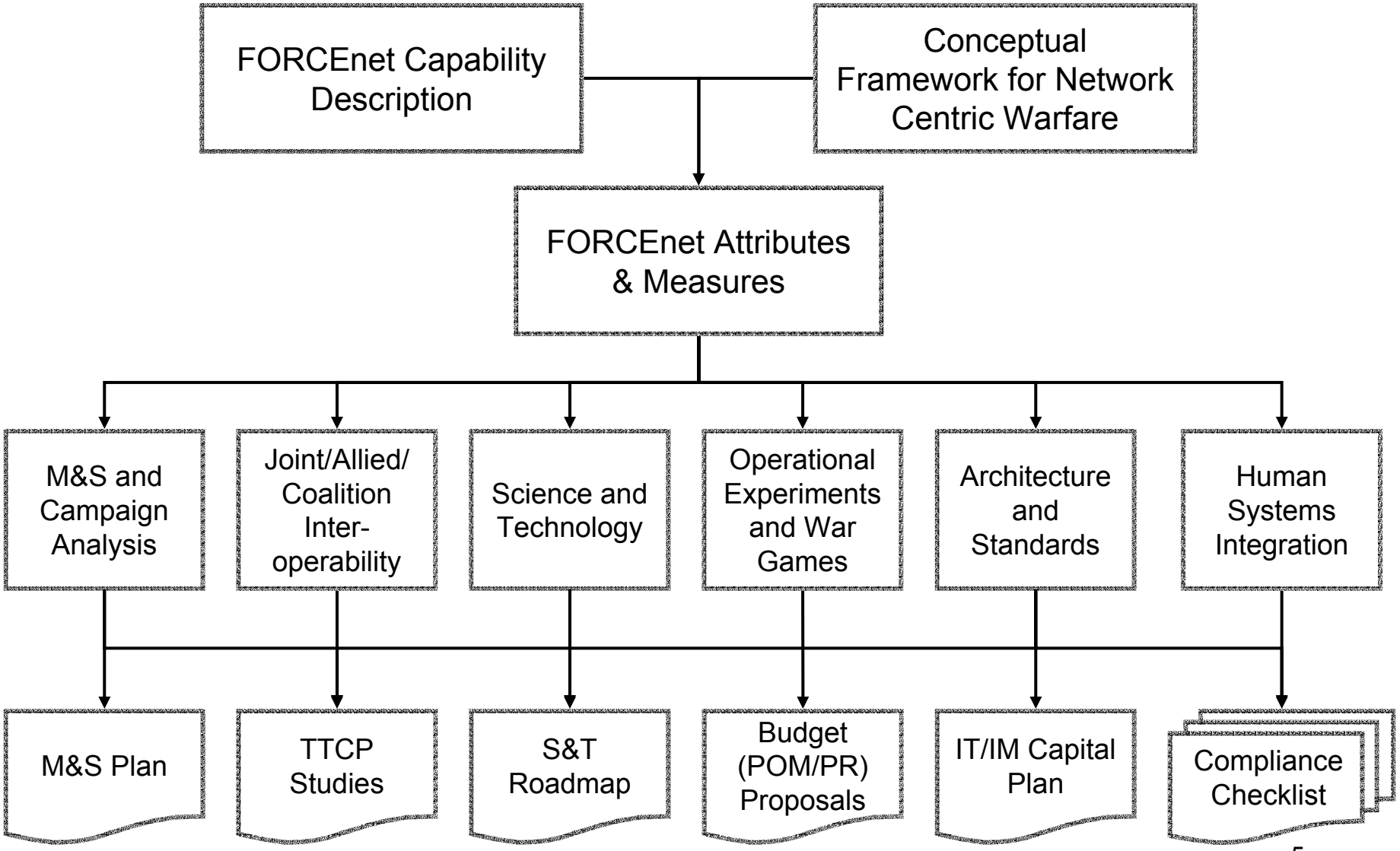
FORCEnet Definition

"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."



Source: CNO Strategic Study Group XXI, definition from 22 July 02 CNO Briefing

FORCEnet Analysis Framework

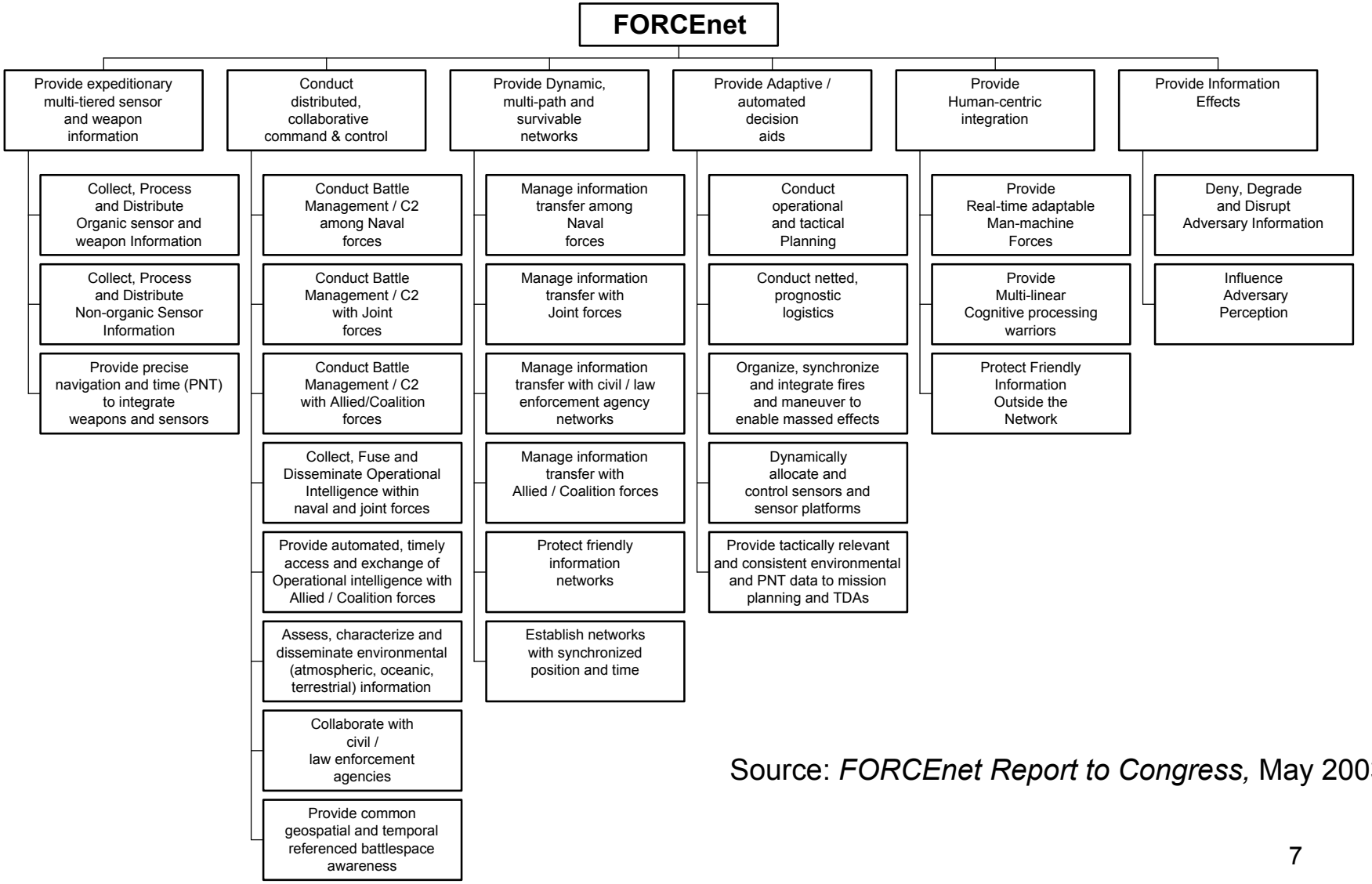


FORCEnet Capabilities

1. Provide expeditionary, multi-tiered sensor and weapon information
2. Conduct distributed, collaborative command and control
3. Provide dynamic, multi-path and survivable networks
4. Provide adaptive/automated decision aids
5. Provide human-centric integration
6. Provide information effects

Source: *Sea Power 21* and *Naval Transformation Roadmap*

Capability Hierarchy



Source: *FORCEnet Report to Congress,* May 2003

NCW Conceptual Framework

Quality of Organic Information

Degree of Networking

Degree of Information "Share-ability"

Quality of Individual Information

Degree of Shared Information

Quality of Individual Sensemaking
Awareness
Understanding

Quality of Inter-actions

Degree of Shared Sensemaking
Shared Awareness
Shared Understanding

Quality of Individual Decisions

Quality of Collaborative Decisions

Degree of Decision/ Plan Synchronization

Degree of Actions/ Entities Synchronized

Operating Environments

Degree of Effectiveness/ Agility

Physical Domain

Information Domain

Cognitive Domain

Social Domain

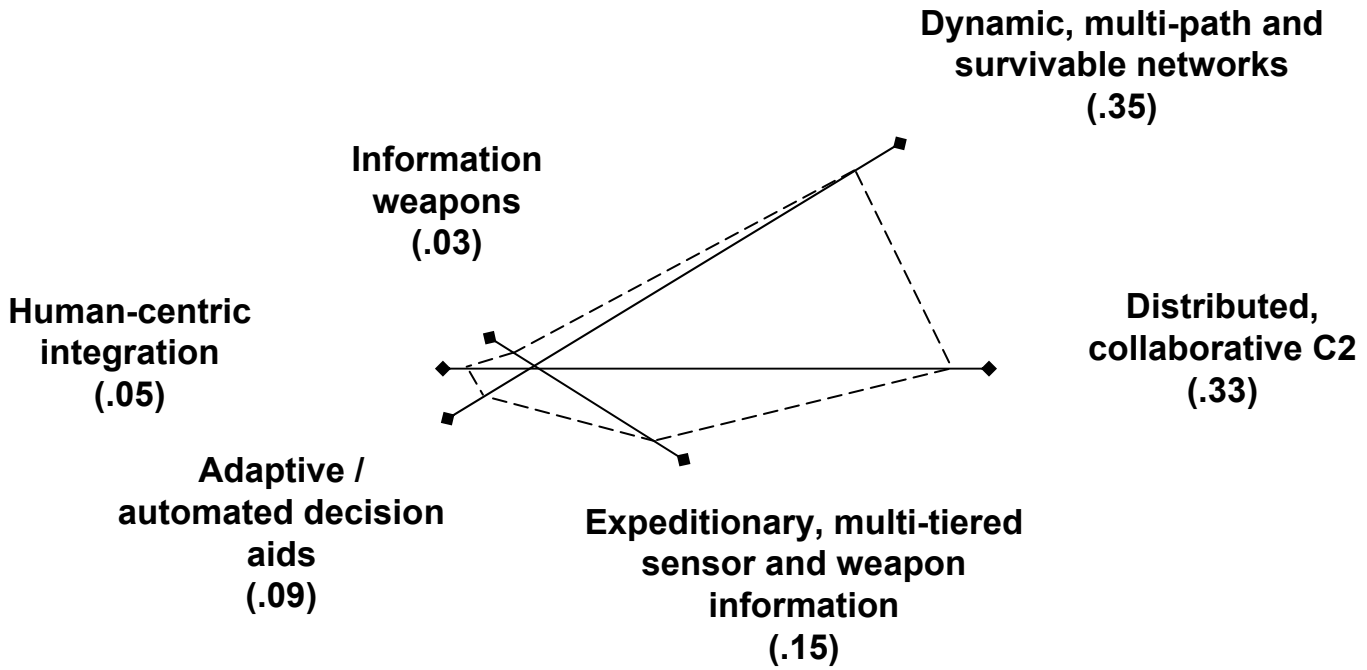
Attributes, Measures, and Metrics

- Terminology based on
  - OASD(NII)/OFT Framework for NCW
  - CCRP and NATO Codes of Best Practice (C2 Assessment & Experimentation)
- Attribute: some aspect of an event, situation,person, or object considered important to understanding the subject under study
- Measure: a standard by which some attribute of interest is recorded
- Metric: the application of a measure to two or more cases or situations

Sample Attributes and Measures

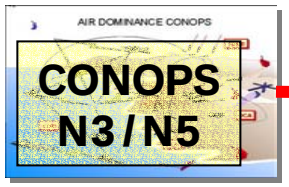
Capability: provide expeditionary, multi-tiered sensor and weapon information	
Attribute	**Notional Measure**
Accuracy	Correspondence with ground truth-correlation coefficient (0 = no correspondence with ground truth, 1 = full correspondence with ground truth). Data matrix comprised of relevant information items estimates (for instance: detection, ID, velocity, location, heading, etc.)
Consistency	Degree of lack of ambiguity with previous information
Completeness	Percentage of ground truth relevant and necessary for ongoing task
Precision	Error and confidence level for time and position information compared to a standard reference
Timeliness	Degree to which currency matches what is needed (0 = no match, 1 = high degree of matching between currency level needed and available)

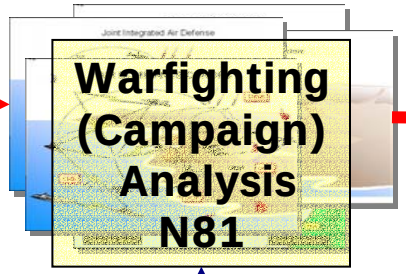
FORCEnet Capability Growth

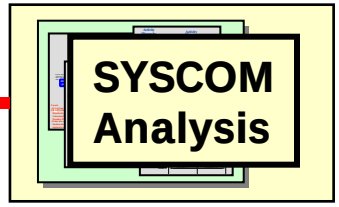


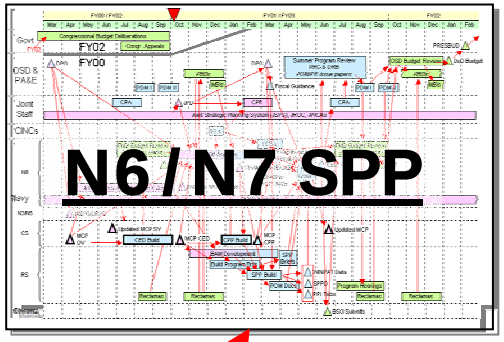
♦ = Desired "end state" for each capability
(value) = Weight in warfighting outcomes (N6/N7 PR-05 scenarios)
------- = notional status of capability

Naval Capability Development Process

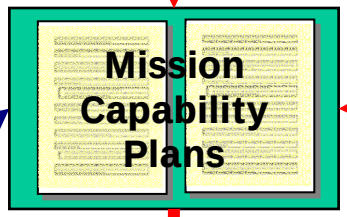








FORCEnet Analysis



Mission Area Analysis

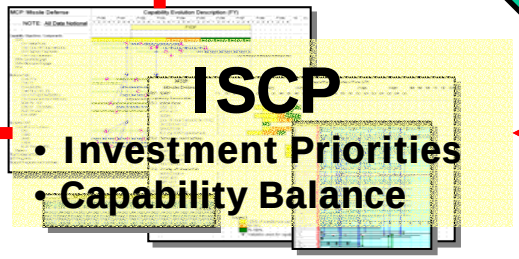
S & T Assessment

Naval Capability Plan

Transformation Roadmap

N6 / N7 Program Guidance

Other Resource Issues



Force Structure & Munitions Analysis

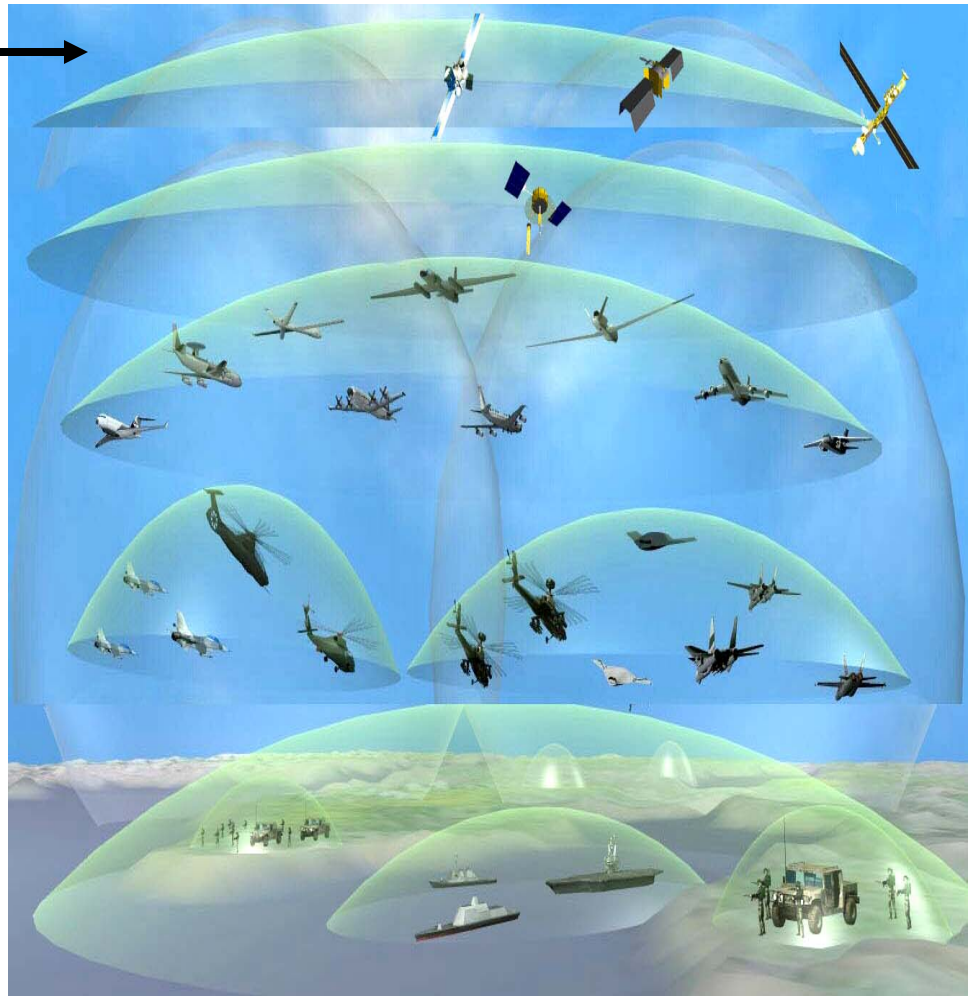
Source: CNO N704

Campaign Analysis Questions

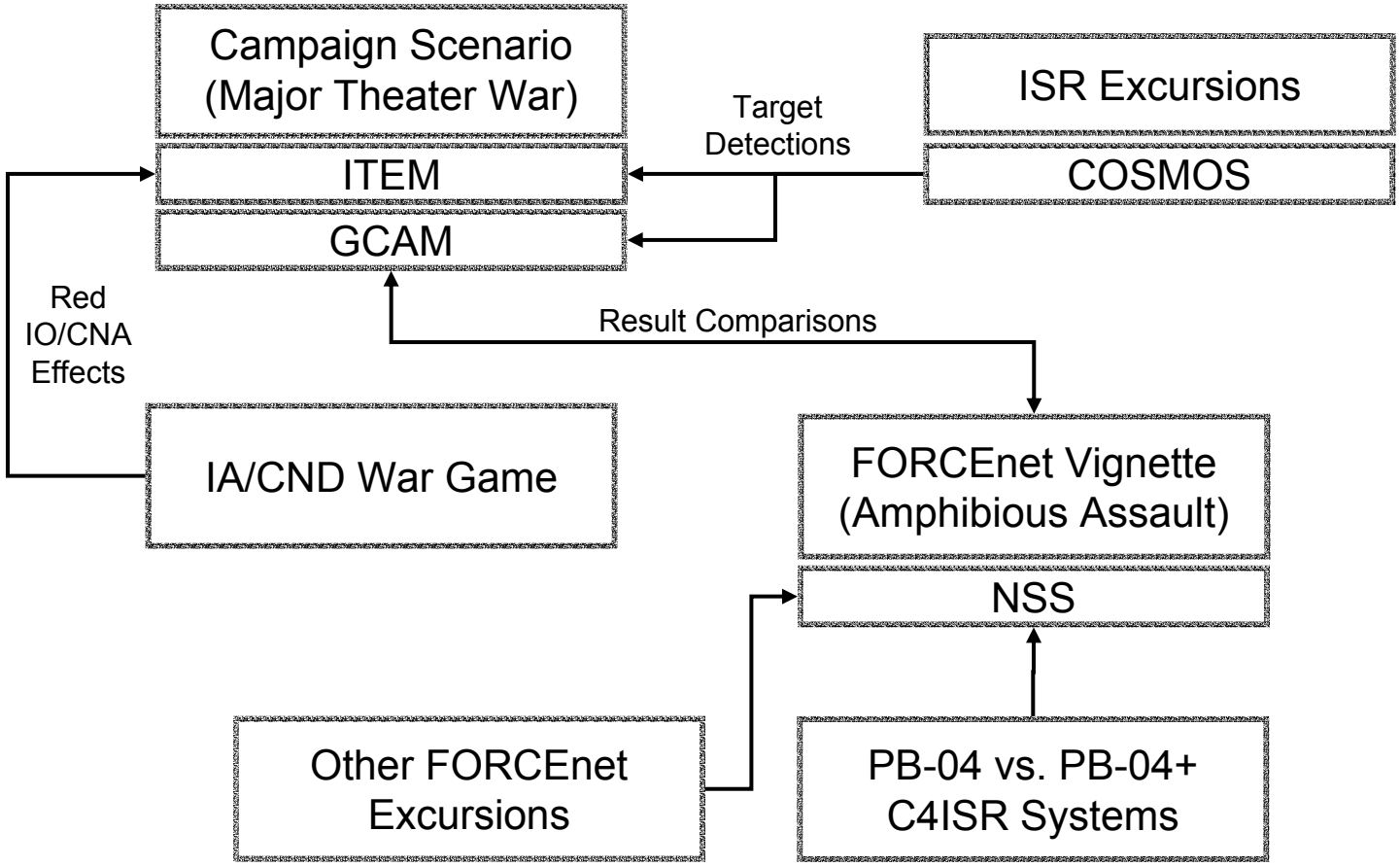
- Template:
  - “What is the impact of [selected capability] on the outcome of the campaign”
- Chief of Naval Operations :
  - What is the impact of Joint and Navy unmanned and/or autonomous systems (sub/surface/air) on the number and type of naval forces needed to provide levels of ISR required to achieve a successful warfighting outcome?
  - How much bandwidth, and over what transmission modes (e.g. single channel, multi-channel terrestrial and SATCOM), will U.S forces require to support combat operations, and how does this compare to available bandwidth? What operations would not be conducted within bandwidth constraints?
  - What is the impact of varying levels of network attacks on the successful outcome of combat operations? What types of redundancy, backups, and alternative paths are necessary to ensure successful warfighting outcomes?
- Sea Strike:
  - Are planned ISR assets sufficient to support the required rate of strike missions? If not, would additional assets mitigate the shortfall, and how many would be needed?

Measuring a “Pound of C4ISR”

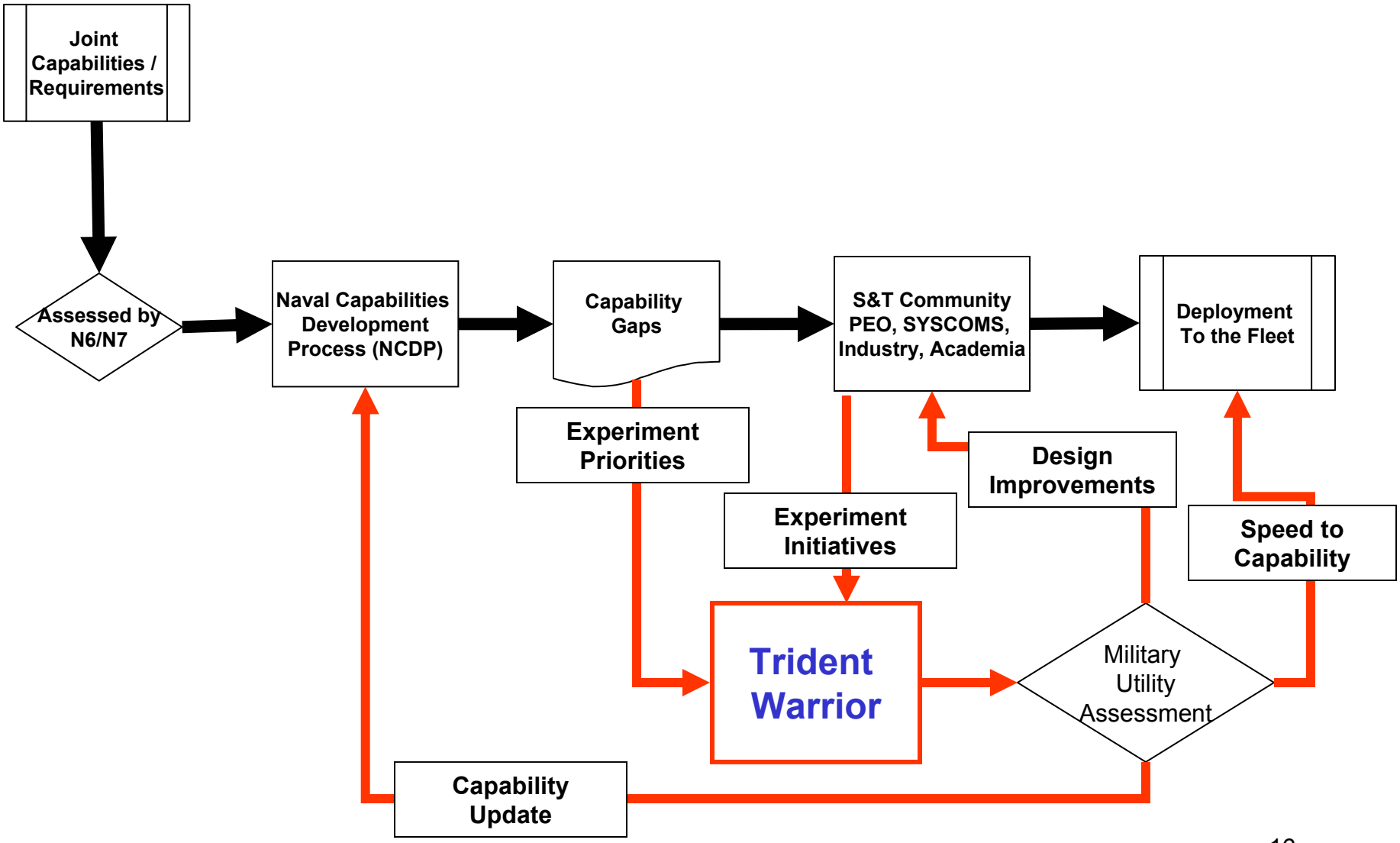
- Previous work assumed “perfect” C4ISR
- Models should provide a more realistic assessment of:
  - System capabilities
  - Performance limitations and bottlenecks
  - Impact of new systems
- Integrated multiple mission-level models:
  - C4ISR Space and Missile Operations Simulator (COSMOS) – ISR
  - Naval Simulation System (NSS) – C4I
- These feed our campaign models:
  - General Campaign Analysis Model (GCAM) – maritime campaign
  - Integrated Theater Engagement Model (ITEM) – air land battle
- Models federated by “sneaker net”
- Combat outcomes determined by campaign level models



Campaign Analysis Process



Trident Warrior Intake / Exhaust



Giant Shadow Objectives

- Technology demonstration for new SSGN class
  - 4 SSBNs to be converted to support TLAMs by 2007
  - Advanced Payload Capability would allow support of SOFs (ASDS) & uninhabited vehicles (UUVs, UAVs)
- FORCEnet experiment to examine layered C2ISR network requirements to support SSGN/SOF ops
  - Clandestine clarification of ambiguous HUMINT
  - Persistent comms & ISR for time-critical activities

FORCEnet Metrics

Provide dynamic, multi-path and survivable networks

Current Metrics

• **Capacity:** Throughput (1) effective systems capacity = maximum data rate - system overhead rate (2) bandwidth utilization = available data rate / effective systems capacity

- ⇧⇧ **Approximations of capacity of a channel can be inferred from the sniffer logs**
- ⇧⇧ **Max data rate required during the experiment**
- ⇔ **Not all of the links were sniffed => difficult to get an indication of capacity across channels**
- ⇩ **Non-operational setting => non-realistic usage of tactical systems**

• **Connectivity:** Percentage of time that all required nodes are connected to the network

- ⇧⇧ **Can extrapolate from packet traffic between MS and HB**
- ⇔ **Only available on days when significant traffic**
- ⇔ **Not all nodes were sniffed => cannot get timed connection info. on all nodes**

⇧⇧ Quantitative ⇧ Qualitative ⇔ Not collected ⇩ Could not be collected ⇩⇩ Difficult to address

Trident Warrior

- Major annual FORCEnet Sea Trial Experiment (NETWARCOM sponsored)
- Goals:
  - Rapid fielding of improved capability to the Fleet, with full supportability and maintainability.
  - Supporting Tactics/Techniques/ Procedures (TTP) and concept of operations (CONOPS)
- Trident Warrior 03
  - 25-30 Sept 03, USS ESSEX with the FDNF Expeditionary Strike Group (CTF 76) off Okinawa
- Trident Warrior 04
  - Fall 2004, TARAWA ESG off SoCal (COMTHIRDFLT host)
- Trident Warrior 05
  - Fall 2005, CSG (TBD) off East Coast (COMSECONDFLT host)

TW03 Metrics
USS Ft. McHenry Network Improvements

		Before (satcom only)	After (satcom and IBGWN)	Percent Improvement
Throughput	Inbound	20.0 kbps	25.8 kbps	29%
	Outbound	59.0 kbps	67.1 kbps	14%
Availability	Inbound	87.7%	99.4%	13%
	Outbound	86.0%	99.2%	15%
Total Outage Time per Day	Inbound	2 hrs 57 min	9 min	95% reduction
	Outbound	3 hrs 22 min	12 min	94% reduction
# of Outages		23	2	91% reduction
Time to Reconnect	Mean	12 min 16 sec	3 min 12 sec	74% reduction
	Max	2 hrs 19 min	6 min	96% reduction

99+% Network Availability; 91% Reduction in Outages;
74% Reduction in Average Network Outage Times

FORCEnet Focus Areas

1. Common, Persistent Maritime picture - improving shared situational awareness across the force
2. Computer Network Defense and Information Assurance - assured info
3. Ubiquitous communications and network infrastructure - bandwidth management, IPv6, etc.
4. Data link management & architecture - improving data link throughput
5. Joint Combat ID - IFF and Blue Force Tracking
6. Persistent and pervasive ISR

Trident Warrior 04

- Continues “speed to capability” via LOE to *Trident Warrior* series
- Builds upon *Trident Warrior 03* baseline
  - Improve traffic management and efficient use of bandwidth
  - Increase shared situational awareness
  - Contribution of mature TTP to both
  - Processing and exploitation of imagery ashore, in a networked environment and product pushed to Expeditionary Strike Group
- Alignment of *Silent Hammer* and *Trident Warrior* provides efficient use of Fleet assets, enhances both experiments
  - *Silent Hammer* demonstrates how a *network of forces* consisting of Ground Forces Sea Based on an SSGN can fill Joint Gaps *(ISR and Time Sensitive Strike)* by conducting a *large scale clandestine* operation, aided by advanced unmanned systems to reduce risk and increase capabilities.

Undersea Dominance FORCEnet Analysis Thrusts

UD04 ASW Concepts

- Battlespace Prep (BSP)
- Hold at Risk
- Maritime Shield

FORCEnet Enabling Capabilities: Comm & Networks | ISR | COTP

System	UFn IWG Systems	U/D
USW-DSS (CUP)	X	X
T-USWC	X	X
WebCOP	X	X
Composeable Fn	X	X
SEAWEB	X	X
ACOMMS	X	X
BLOOM	X	X
Special Radio	X	X
HAIL	X	X
LFACOMMS	X	X
U/K ACOMMS	X	
Deep Siren	X	

UD04 Mission Analysis

- Mission Capability Analysis
- Campaign Analysis
- FORCEnet aspects:
  - Battlespace Preparation
  - Situational Awareness
  - ASW Timeline Reduction
  - Cueing (Deployed Sensors)
  - C4I (Sub Comms, USW-DSS)

UD04 Systems Analysis

- System Assessment
- Technical Analysis
- FORCEnet aspects:
  - Comms & Networks
    - Latency, Data Rate, Range, Availability, Covertness
  - C2
    - Effectiveness & coherency of Plan
    - Uniformity of situational awareness
    - Improved utilization of multi-sensor types
    - HSI attributes
  - ISR
    - Improved BSP through bottom mapping

N61F UD04 FORCEnet Analysis

- Goal
  - Provide analysis of Fn capabilities employed in UD04
- Approach
  - **Network Thrust & C2 Thrust**
  - Leverage UD04 Mission & Systems analysis
  - Identify C4 capabilities necessary for new ASW technologies

USW Fn Implementation Working Group (IWG)

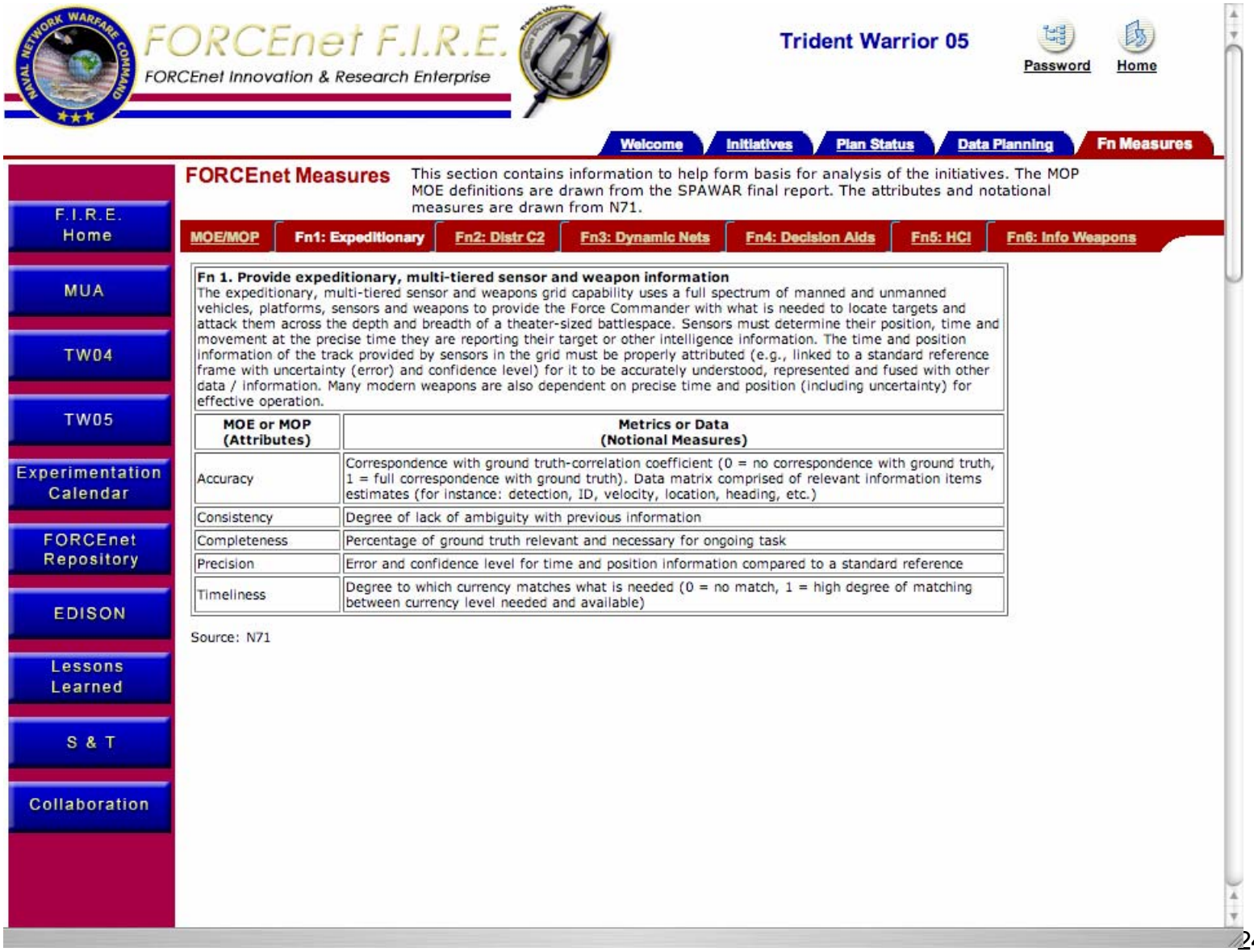
- Requirements
- Arch & Standards
- Implementation Plan
- Technologies / System Comparison

FORCEnet MCP/NCP

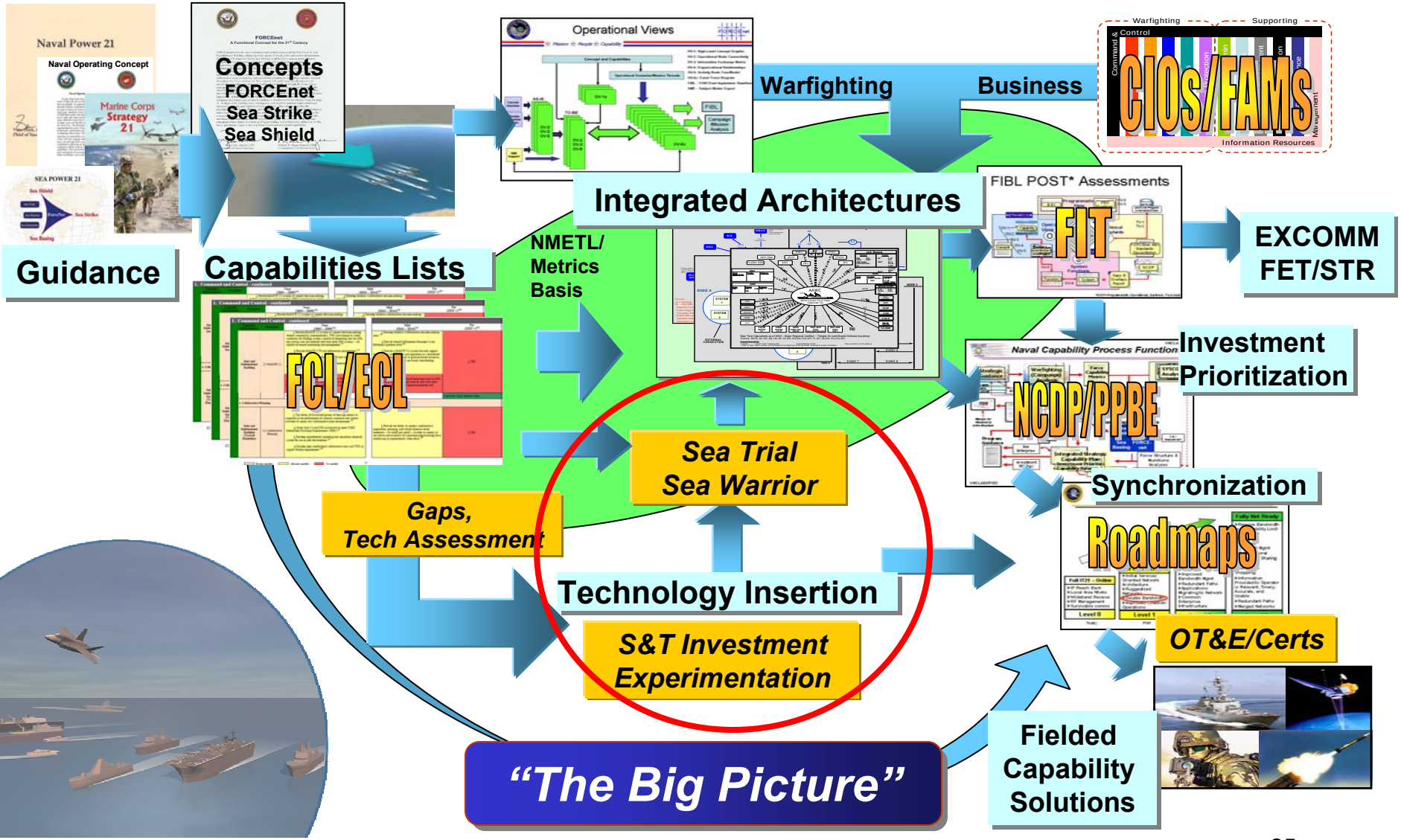
- Requirements Validation
- Assessment of Technologies
- Budget Recommendations

Rigorous C4 analysis to feed USW development efforts, IWG & MCP/NCP

FORCEnet Innovation & Research Enterprise (FIRE)



Concept Based Strategy Development



Trident Warrior

Goal: Fleet Driven Speed to Capability

Fully supportable Fleet leave-behinds

OPNAV / NETWARCOM / MCCDC / SPAWAR / PEO / Industry

Process

Organization

Technology

TTP

Sea Trial

Military Utility Assessment DOTMLPF

Sea Trial Executive Steering Group

OPNAV

Acquisition

Quicklook & Analysis influencing programmatic decisions

Trident Warrior Evolution

TW 03 Essex ESG

Oct 2003

- Fn Integrated Prototype Demonstration, ESG LOE & JTF WARNET PDX

5 Focus Areas
17 Specific Initiatives
7 Rapid Acquisition Recommendations

- Bandwidth Management (ADNS)
- Integrated Supporting Arms Control Center – Automated (SACC-A)
- Intra BG Wireless Network

TW 04 Tarawa ESG

Nov 2004

- End-to-end process established
- Objectives mapped into NCDP capability gaps

9 Focus Areas
28 Specific Initiatives
16 Rapid Acquisition Recommendations

- EHF TIP
- Dynamic Bandwidth Process (ADNS II)
- Bandwidth Managed Voice
- Doctrinal support to Fires
- Afloat Electromagnetic Spectrum Operations Program (AESOP)

TW 05 Iwo Jima ESG

Dec 2005

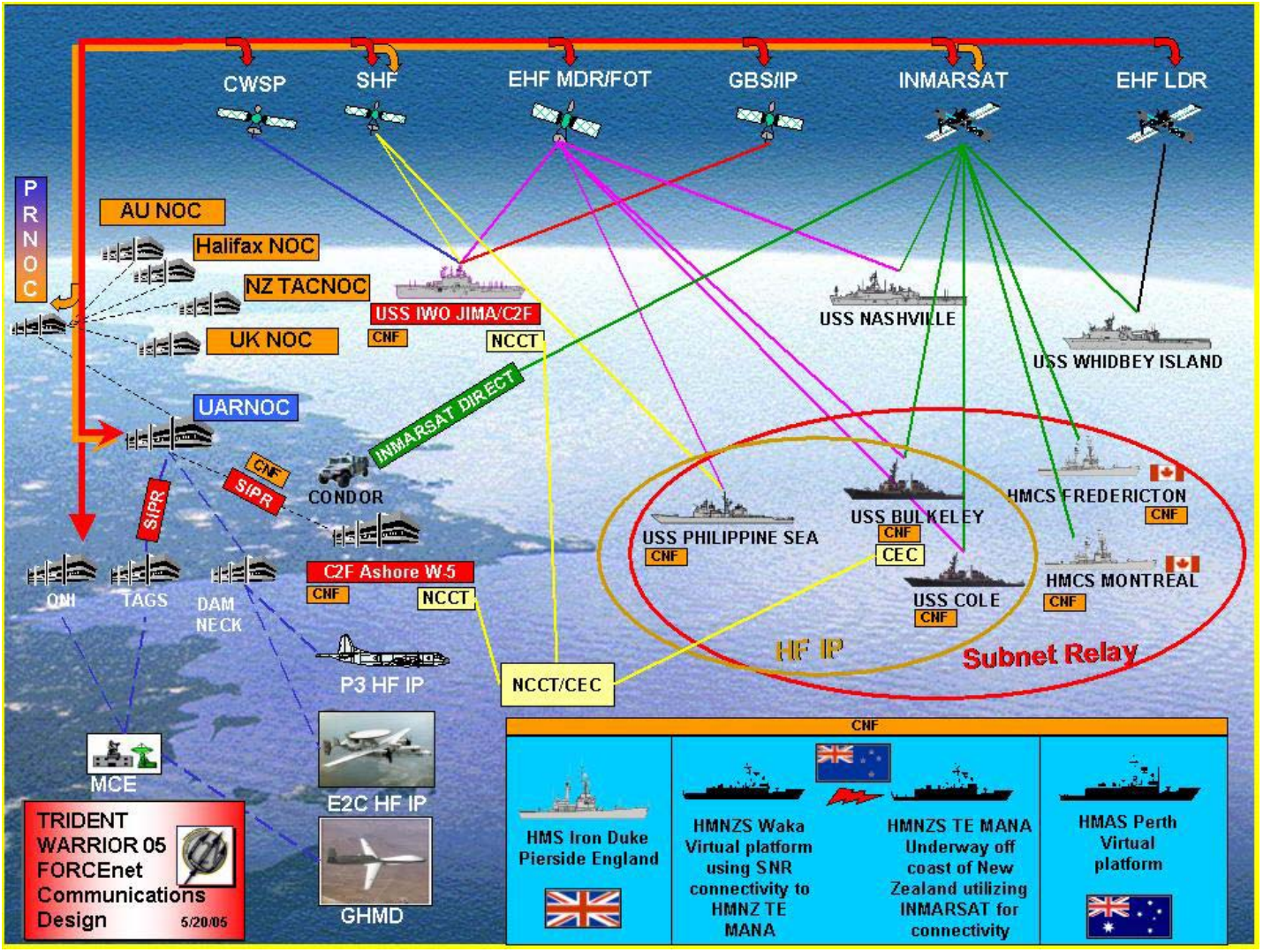
- CFMCC focus, GWOT scenario, extensive Coalition, Joint and Industry participation

11 Focus Areas
108 Measurable Objectives

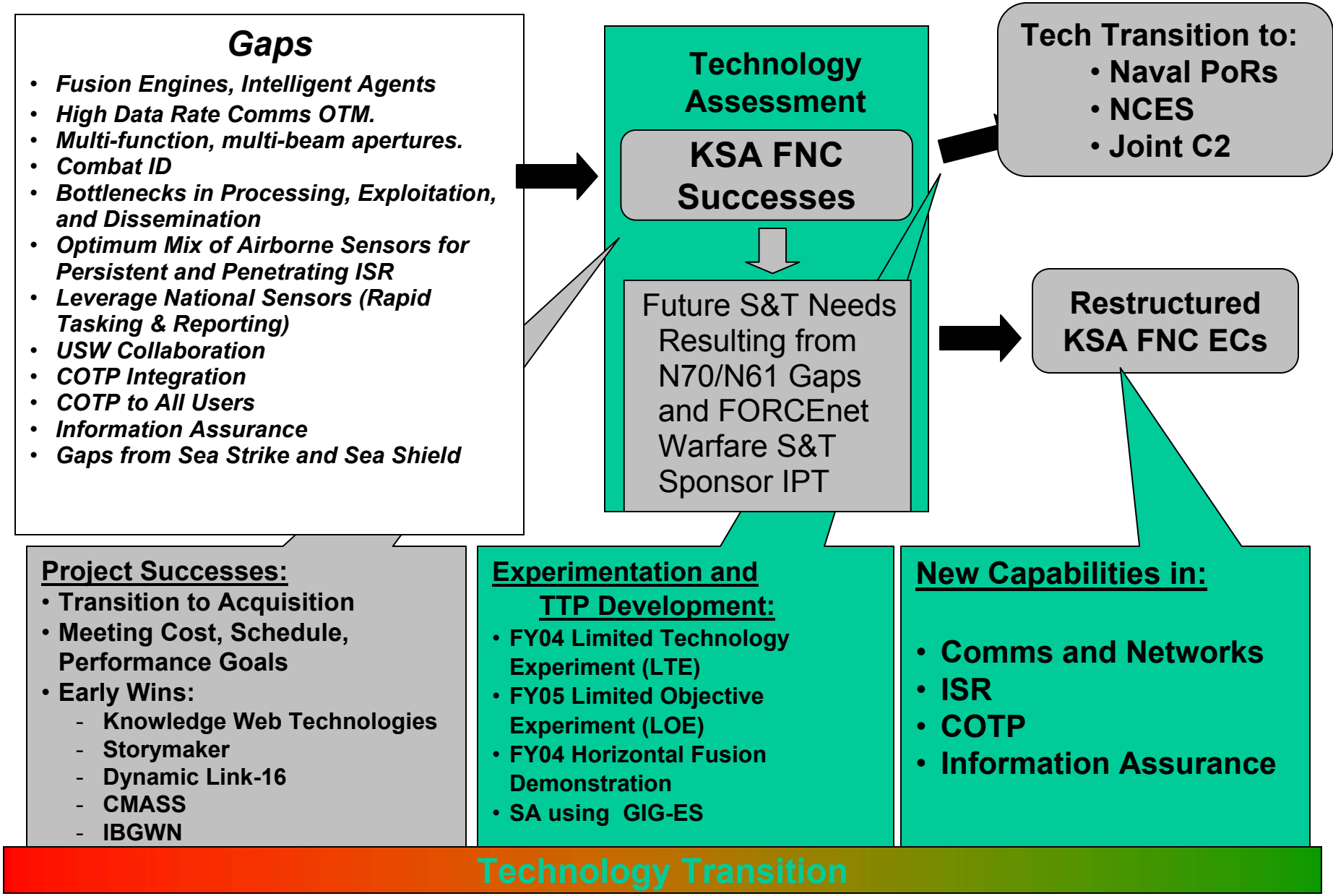
- CFMCC C2
- Cross Domain Solutions
- Five-Eyes Coalition Network
- Information Management Plan
- GHMD CONOPS
- Human Systems Integration
- ADNS II with ECP

Trident Warrior 05

- *CFMCC C2 Focus*
- *Exercise Distributed Staff With C2F*
- *Joint, Coalition & Industry Participation*
- *GHMD CONOPS Development*
- *Netted ISR Sensors*
- *Coalition Naval Forces (CNF) Network*
- *Laboratory Testing to Minimize Risk*
- *Wargame to Refine CONOPS & TTP's*



S&T (Future Naval Capabilities)



S&T (Discovery and Invention)

- Information Integration is primary focus
- Program examines critical S&T needs of
  - Automatic association and merger of information for unified presentation
  - Automated recognition and cueing for significant patterns of information, computer-aided reasoning for task-oriented information dissemination
  - Timely, accurate information and sensor fusion from heterogeneous sources
  - Supporting technologies to provide information assurance.
- Specific goals
  - Automated image understanding
  - Automated integration of disparate sources of information
  - Level 2 / Level 3 Information Fusion
  - Information Integrity

Capabilities Based Planning Approach

A top-down, competitive process that weighs options vs. resource constraints across a spectrum of challenges

- Link DoD decision-making to the Defense Strategy
  - Apportion risk across external challenges – traditional, irregular, catastrophic, and disruptive
  - At the level of portfolios and current/future concepts
- Inform risk tradespace – identify joint capability gaps, redundancies, and opportunities
- Facilitate the development of affordable capability portfolios that:
  - Hedge against uncertainty
  - Increase costs to adversaries while suppressing our costs
- Establish a common language that links COCOM capability requirements to Service force development and provider efforts, and integrates the five fundamental Departmental business processes *(Policy Formulation, Planning, Requirements, Resourcing, Acquisition)*

Why we created Joint Capability Areas…

An SPG-directed study as a part of Operational Availability (OA) – 05

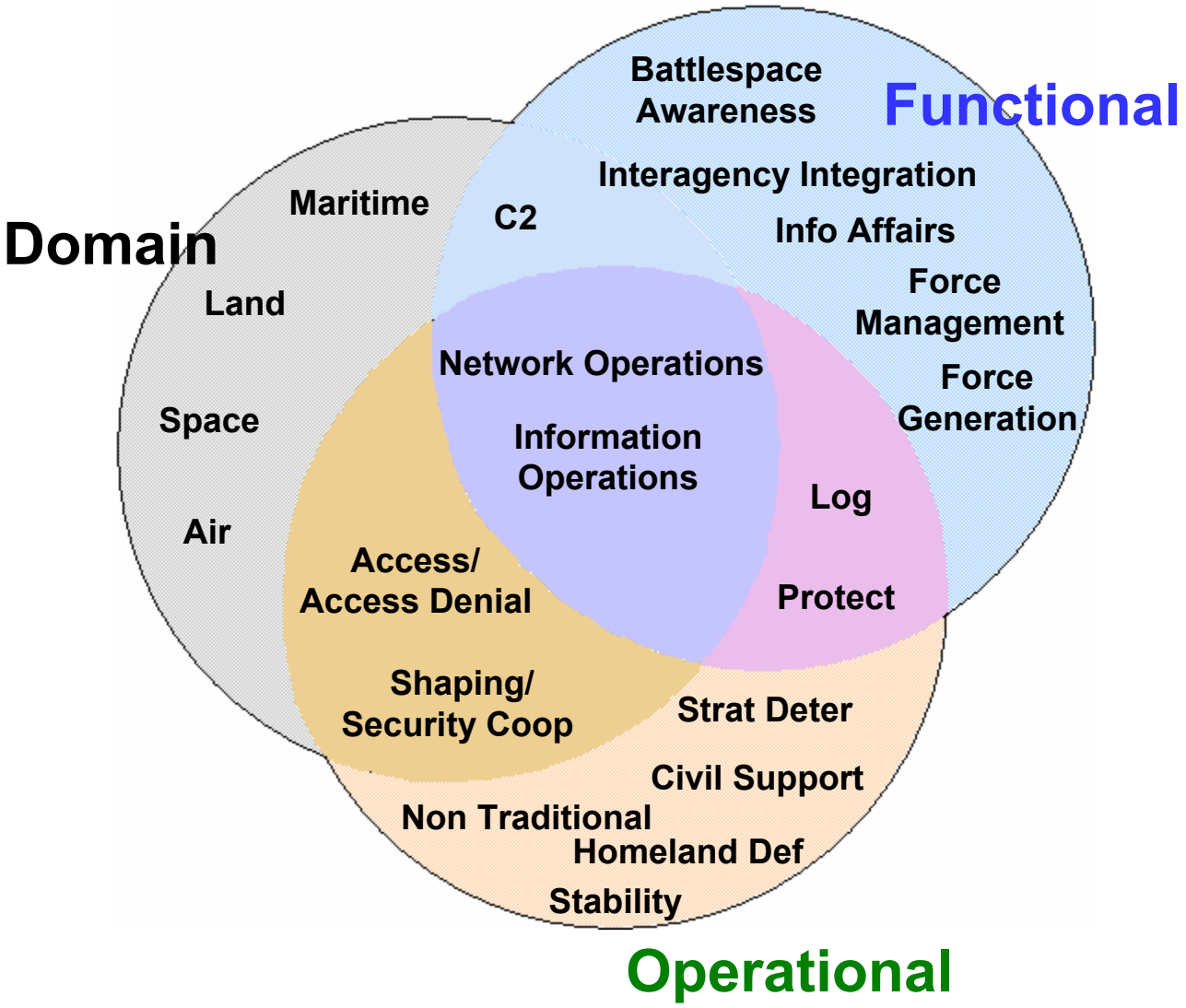
- Provide a common framework to:
  - define joint capability needs
  - allow Services to map their capabilities into something
- Identify "peer-level" capability categories to:
  - facilitate organizational binning
  - tee-up decision space for cross-Service trades
  - support strategy/senior leader guidance articulation
  - permit gap analysis and evaluation on capability contributions to various capability categories
  - Develop a compatible planning and programming framework
- Foster a "capabilities culture" in support of CBP

Tier 1 Joint Capability Areas

As of 15 Dec 04

- Battlespace Awareness
- Command and Control
- Network Operations
- Interagency Integration
- Information Affairs
- Information Operations
- Protection
- Logistics
- Force Generation
- Force Management
- Homeland Defense
- Strategic Deterrence
- Shaping & Security Cooperation
- Stability Operations
- Civil Support
- Non-Traditional Operations
- Access & Access Denial Operations
- Land Control Operations
- Maritime/Littoral Control Operations
- Air Control Operations
- Space Control Operations

JCA Mapped across Ops/Domain/Functional Views



JWSTP Example

Capability	Related Limitations	Related Technology	Related DTOs
Establish Appropriate Organizational Relationships	Ability to set up and change formal organizational and command relationships in accordance with mission and task needs Need flexible organizational constructs Need flexible authority relationships	Decision aids Visualization technology	HS.42, 47
Collaborate	Doctrinal, cultural, and organizational limits to full collaboration Lack of trust in collaborative decisionmaking processes Coalition interoperability Geographic limitations to collaboration	Collaboration support tools Effective user-centric displays Geographical information systems Automated embedding of geospatial data Multilingual translation technology	JF.04, 06; JA.25; JC.54; BE.11; HS.41, 47, 50, 57, 58, 63

Draft C2 JIC

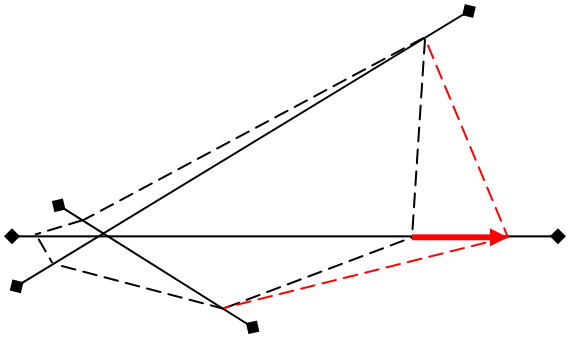
Capability	Operational Task	Attributes	Standard (2010)
5. Plan Collaboratively Future planning must be conducted with the collective knowledge of the decisions and plans of others. An effects-based approach that directly ties offensive actions to campaign objectives must guide plan development. Planners must be able to focus on exploiting critical adversary vulnerabilities and also must consider friendly critical capabilities and potential collateral damage. Parallel, distributed, collaborative planning capabilities and improved assessment tools are needed compress process timelines. The ability to assess the suitability of a plan and to rehearse prior to execution is also needed.	5.1 Form collaborative planning teams across components, missions, functions, and geographies, and with mission partners Develop, coordinate and build effective collaborative teams for specific missions and tasks. Use existing, historical and available staff collaboration structures and processes to develop tailored structures and processes.	Cohesion Interoperability Understanding	Cohesion -- XX% of group or team rewards match or meet unit and individual mission goals Interoperability--Users can access and use resources across all partners XX% of the time. Understanding— XX% of personnel receive necessary guidance and act in accordance with that guidance XX% of the time.

C2 Capabilities		Fn6	Fn7	Fn8	Fn15	Fn1	Fn4	Fn5	Fn9	Fn10	Fn11	Fn12	Fn13	Fn14	Fn2	Fn3
		Provide Situation Info	Provide Collab Environ	Automate Low C2, Decision Aids	Provide Quick/Good Decisions Capability	Coms All Nodes	Store/Retrieve Info	Process Info, Access	Provide IA	Multi-Level Security	C2 Systems Interoperability	Autonomous Nodes	Network Management	New Capabilities Incorporation	Provide Blue Info	Provide Red Info
Basic C2 Capabilities																
The ability to monitor and collect data	**N**															
The ability to develop situational understanding																
The ability to develop courses of action and select one																
The ability to develop a plan																
The ability to execute the plan including providing direction and leadership to subordinates																
The ability to monitor the execution of the plan and adapt as necessary																
The ability to execute the basic C2 process																
Collaborative C2 Capabilities		**Fn6**	**Fn7**	**Fn8**	**Fn15**	**Fn1**	**Fn4**	**Fn5**	**Fn9**	**Fn10**	**Fn11**	**Fn12**	**Fn13**	**Fn14**	**Fn2**	**Fn3**
The ability to netw ork																
The ability to share information	**C**															
The ability to interact	**C**															
The ability to develop shared aw areness	**C**															
The ability to develop shared understanding	**C**															
The ability to decide in a collaborative environment	**C**															
The ability to synchronize	**C**															
The ability to execute the collaborative C2 process	**C**															

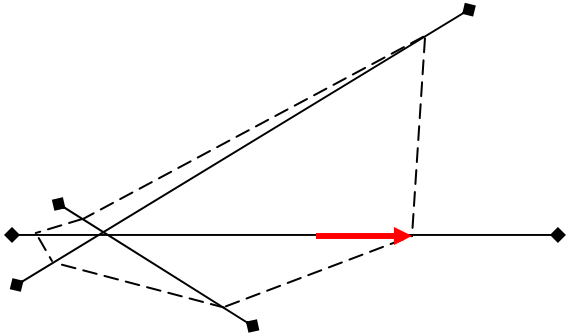
Net Centric Knowledge Area Capabilities		Fn6	Fn7	Fn8	Fn15	Fn1	Fn4	Fn5	Fn9	Fn10	Fn11	Fn12	Fn13	Fn14	Fn2	Fn3
		Provide Situation Info	Provide Collab Environ	Automate Low C2, Decision Aids	Provide Quick/Good Decisions Capability	Coms All Nodes	Store/Retrieve Info	Process Information	Provide IA	Multi-Level Security	C2 Systems Interoperability	Autonomous Nodes	Network Management	New Capabilities Incorporation	Provide Blue Info	Provide Red Info
Ability to establish appropriate organizational relationships	C															
Ability to collaborate.	C															
Ability to synchronize actions.	C															
Ability to share situational awareness	C															
Ability to share situational understanding	C															
Ability to conduct collaborative decisionmaking/planning	C															
Ability to achieve constructive interdependence	C															
Net Centric Technical Capabilities		**Fn6**	**Fn7**	**Fn8**	**Fn15**	**Fn1**	**Fn4**	**Fn5**	**Fn9**	**Fn10**	**Fn11**	**Fn12**	**Fn13**	**Fn14**	**Fn2**	**Fn3**
Ability to create/produce information.	I															
Ability to store, share, and exchange information and data.	I															
Ability to establish an information environment.	I															
Ability to process data and information	I															
Ability to employ geo-spatial information	I															
Ability to employ information.	I															
Ability to find and consume information	I															
Ability to provide user access	I															
Ability to access information	I															
Ability to validate/assure.	I															
Ability to install/deploy	D															
Ability to operate/maneuver	D															
Ability to maintain/survive.	D															
Ability to provide network services.	N															

Battlespace Awareness Operational Capabilities		Fn6	Fn7	Fn8	Fn15	Fn1	Fn4	Fn5	Fn9	Fn10	Fn11	Fn12	Fn13	Fn14	Fn2	Fn3
		COP / UDOP	Provide Collab Environ	Automate Low C2, Decision Aids	Provide Quick/Good Decisions Capability	Coms All Nodes	Store/Retrieve Info	Process Information	Provide IA	Multi-Level Security	C2 Systems Interoperability	Autonomous Nodes	Network Management	New Capabilities Incorporation	Provide Blue Info	Provide Red Info
Command and Control of BA Assets	C															
Execute Collection																
Exploitation and Analysis																
Model, Simulate and Forecast																
Manage Know ledge	I															
Battlespace Awareness Enabling Capabilities		**Fn6**	**Fn7**	**Fn8**	**Fn15**	**Fn1**	**Fn4**	**Fn5**	**Fn9**	**Fn10**	**Fn11**	**Fn12**	**Fn13**	**Fn14**	**Fn2**	**Fn3**
Integrate BA Netw ork	N															
Rapidly Infuse Technology																
Recruit, Retain, and Train World-Class BA Personnel																

Capability Gaps



Progress
New systems
Demo “leave-behinds”
DOT_LPF innovations



Effort
New programs
Experimentation
S&T investment

Accomplishments

- Demonstrated value of analytical framework:
  - Connects FORCEnet capabilities and NCW Framework
  - Capabilities under revision
  - Quantitative measures partially successful and improvements proposed
- Improved representation of C4ISR in campaign analysis
- Increased analytical support for PR-05, POM-06, PR-07 submissions
- Provided additional products: S&T Roadmap, M&S Plan, IT/IM Capital Planning Metrics, Compliance Checklist, Experimentation CD&E Plan