Author Information Sheet
11th ICCRTS
Coalition Command and Control in the Networked Era

FORCEnet Science and Technology Needs with Potential Solutions

Topic Areas C2 Concepts and Organization and C2 Analysis
CCRP # I-099

Jude E. Franklin, PhD
Technical Director
Raytheon Network Centric Systems Command and Control
Suite 1700
1100 Wilson BLVD
Arlington, VA 22209

703-284-4463
Jude_E_Franklin@Raytheon.com

Raytheon Release 06-0051
Version1.2

FORCEnet Science and Technology Needs with Potential Solutions

Jude E. Franklin, Ph. D.
Technical Director, Raytheon NCS Command and Control Systems
Suite 1700
1100 Wilson Blvd.
Arlington, VA, 22209

Paper for the OASD-NII International Command and Control Research and Technology Symposium, 26-28 September, 2006
Raytheon release # TD-06-0010

ABSTRACT

Coalition Command and Control in a Network Era has many science and technology implications in the general area of Sensemaking, Situational Understanding, Knowledge Management, Information Management, and Information Assurance. The U.S. Navy has examined Net-Centric Operations and its implementation via FORCEnet. This paper is derived from a recent study, "**FORCEnet Implementation Strategy"** that was conducted by the National Academies' National Research Council, NRC. (http://darwin.nap.edu/books/0309100259/html/). The paper identifies S&T shortfalls and looks at potential near and mid-term solutions.

The National Academies FORCEnet study addressed eight critical operational capabilities and this paper examines five of these:

- Information Management
- Situational Awareness and Understanding
- Persistent Intelligence, Surveillance and Reconnaissance, ISR
- Information Assurance
- Dynamic Composability and Collaboration

Each of the above operational capabilities is broken down into technology related capabilities with associated critical technologies. Some potential solutions to satisfy these S&T gaps are introduced.

Introduction

The Net Enabled Capability and the Net-Centric Operations world is a complex operational scenario as shown in Figure 1. It requires a high degree of coordination to accomplish the FORCEnet mission [Reference 1, 2].

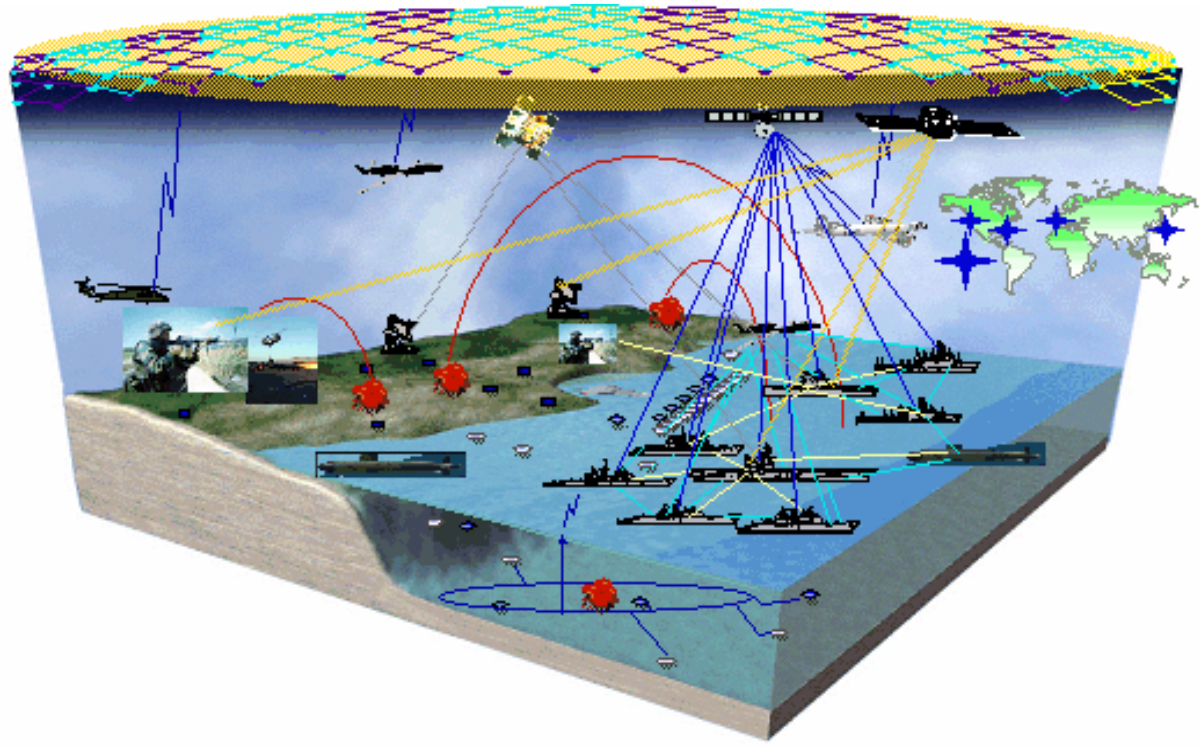

Figure 1. FORCEnet Scenario

The members of the National Academies NRC FORCEnet Study are shown below. The ones that are highlighted participated on the team that examined science and technology shortfalls:

.

- Rich Ivanetich, IDA
- Bruce Wald, former Assoc TD, NRL
- Robert Brammer, NGIT
- Joseph Cipriano, LMIT
- Admiral Archie Clemins, Caribou Technologies
- **Chip Elliott, BBN**
- **Joel Engel, Former IBM Fellow**
- **Jude Franklin, Raytheon**
- John Hanley, IDA
- Kerrie Holley, IBM Global Services
- **Ken Jordan, SAIC**
- **Otto Kessler, MITRE**
- **Jerry Krill, JHU APL**
- Ann Miller, U. Missouri-Rolla
- RADM Bill Morris
- RADM Richard Nibe
- LTG. John Rhodes

- **Daniel Siewiorek, CMU**
- Ed Smith, Boeing
- **Mike Zyda, USC**

The critical operational areas that were identified by the National Academies NRC FORCEnet study are listed below and the ones addressed in this paper are highlighted:

- Reliable Wideband Mobile Communications
- Information Management (including Common Operational Picture [COP])
- Situation Awareness and Understanding
- Persistent Intelligence Surveillance and Reconnaissance, ISR
- Information Assurance
- Modeling and Simulation
- Dynamic Composability and Collaboration
- Supporting the Disadvantaged User-personnel, Platform or Sensor

The CNO in 2005, identified 15 FORCEnet required capabilities, and they are listed below [Ref 3]:

1. "Provide robust, reliable communications to all nodes, based on the varying information requirements and capabilities of those nodes
2. Provide reliable, accurate and timely location, identity and status information on all friendly forces, units, activities and entities / individuals
3. Provide reliable, accurate and timely location, identification, tracking and engagement information on environmental, neutral and hostile elements, activities, events, sites, platforms, and individuals
4. Store, catalogue and retrieve all information produced by any node on the network in a comprehensive, standard, repository so that the information is readily accessible to all nodes and compatible with the forms required by any nodes, within security restrictions
5. Process, sort, analyze, evaluate, and synthesize large amounts of disparate information while still providing direct access to raw data as required
6. Provide each decision maker the ability to depict situational information in a tailorable, user-defined, shareable, primarily visual representation
7. Provide distributed groups of decision makers the ability to cooperate in the performance of common command and control activities by means of a collaborative work environment
8. Automate lower-order command and control sub-processes and to use intelligent agents and automated decision aids to assist people in performing higher-order sub processes, such as gaining situational awareness and devising concepts of operations
9. Provide information assurance
10. Function in multiple security domains and multiple security levels within a domain and manage access dynamically
11. Interoperate with command and control systems of very different type and level of sophistication

12. Allow individual nodes to function while temporarily disconnected from the network
13. Automatically and adaptively monitor and manage the functioning of the command and control system to ensure effective and efficient operation and to diagnose problems and make repairs as needed
14. Incorporate new capabilities into the system quickly without causing undue disruption to the performance of the system
15. Provide the decision makers the ability to make and implement good decisions quickly under conditions of uncertainty, friction, time, pressure, and other stresses"

These 15 CNO required capabilities are consistent and supportive of the National Academies FORCEnet Study's eight operational capabilities. The CNO objectives stress Situational Awareness and Persistent Surveillance, Information Management, Information Assurance, Dynamic Composability / Collaboration, and the Decision Support Systems that facilitate the operational needs.

Information Management

In a Net-Centric Operations world, information is available from sensors, humans and other sources. In fact, this information centric world is a major driver to make FORCEnet a reality. The problem is that the massive increase in information as depicted in Figure 2 is also a major impairment to FORCEnet's success. This Net Enabled Capability must have an ubiquitous form of information management that will eliminate information overload and that will ensure that timely information is transmitted to the correct node, person or machine.

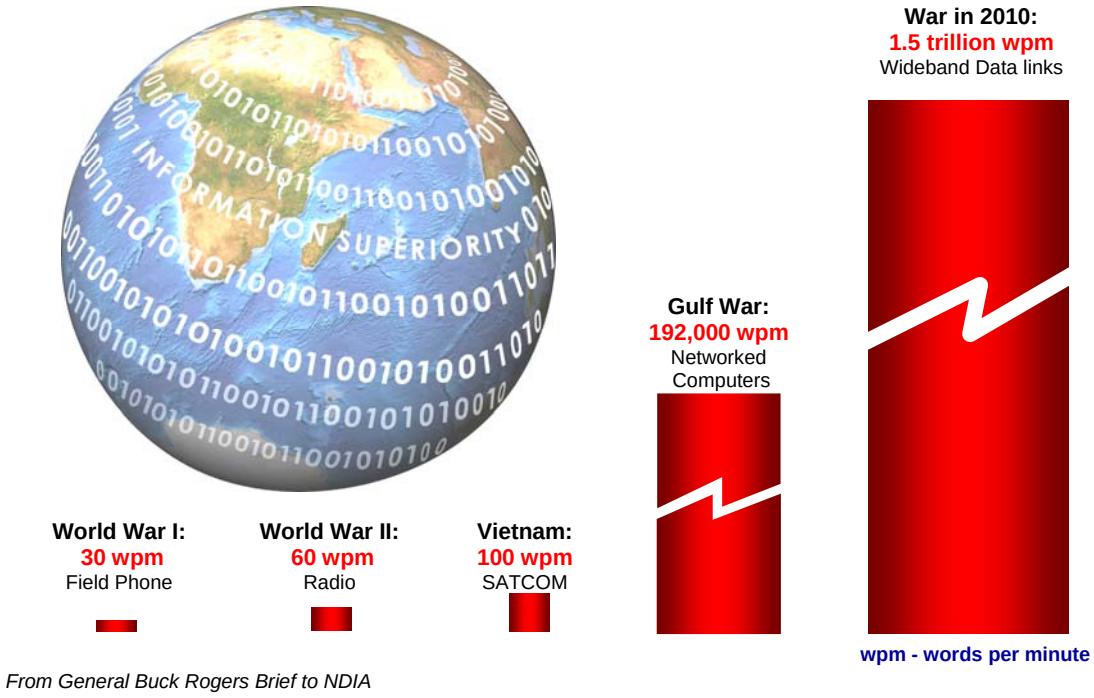

Figure 2. Information Management is driven by the Information Explosion

Insufficient technology exists, for reliable support of Naval warfighting capability, including limited understanding of the information management issues (accessing, processing, dissemination, presentation) which must be implemented with distributed functionality in network centric environments. In particular, these current technology gaps include [Ref1]:

- "Ontology consistency to enable automated machine collaboration across communities of interest
- Information services to enable management of information content / quality
- Automated sensor resource management, coupled to dynamic tactical needs and military operational needs
- Distributed, heterogeneous, real time level 1 data fusion
- User defined visualization and automation for decision support
- Enterprise monitoring and control to give the user feedback concerning information processes, in terms of performance, expected latency, flow, and quality"

There are key technical challenges that must be addressed before Information Management can be deployed for FORCEnet and they are:

- Trust
- Contamination
- Utility
- GIG Task, Push, Process, and Use (TPPU); and Only Handle Information Once (OHIO)
- Metrics
- Pedigree
- Models to capture and share knowledge of phenomenology and sources to guide human interpretation

Figure 3. depicts a possible solution for information management that must be accomplished prior to deployment of FORCEnet. The information must be prioritized and driven by the warfighters' needs that exist at that specific time. This will demand that the overall FORCEnet system must be capable of automatically understanding the situation, the message traffic, the information derived from sensors and sources, the adversary's intent and capability, and then to be able to manage the information to ensure that the **right** information gets to the **right** node / person at the **right** time.

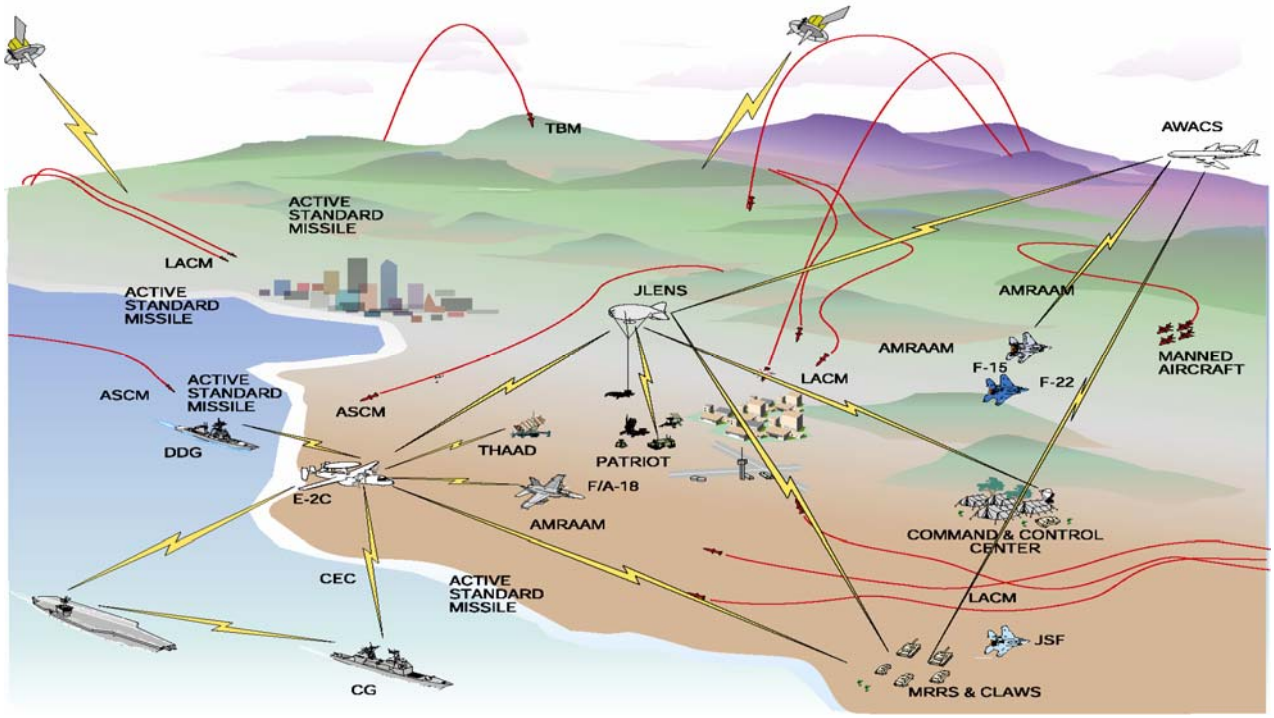

Figure 3. Automated Information Management is critical for FORCEnet Success

Situational Awareness and Persistent Intelligence, Surveillance, and Reconnaissance; ISR

FORCEnet must have Situational Awareness and Persistent ISR that will allow joint services and coalitions to work together to maximize the offensive power and to ensure successful effects based operations. Situational awareness demands technology related capabilities including automated consistent understanding, automated understanding of adversarial intent, forecast of battlespace situations, data mining, information discovery, automated target recognition, activity pattern recognition, and dynamic "what if" analysis. Figure 4. illustrates the complexities associated with the Situational Awareness and Persistent Surveillance problem.

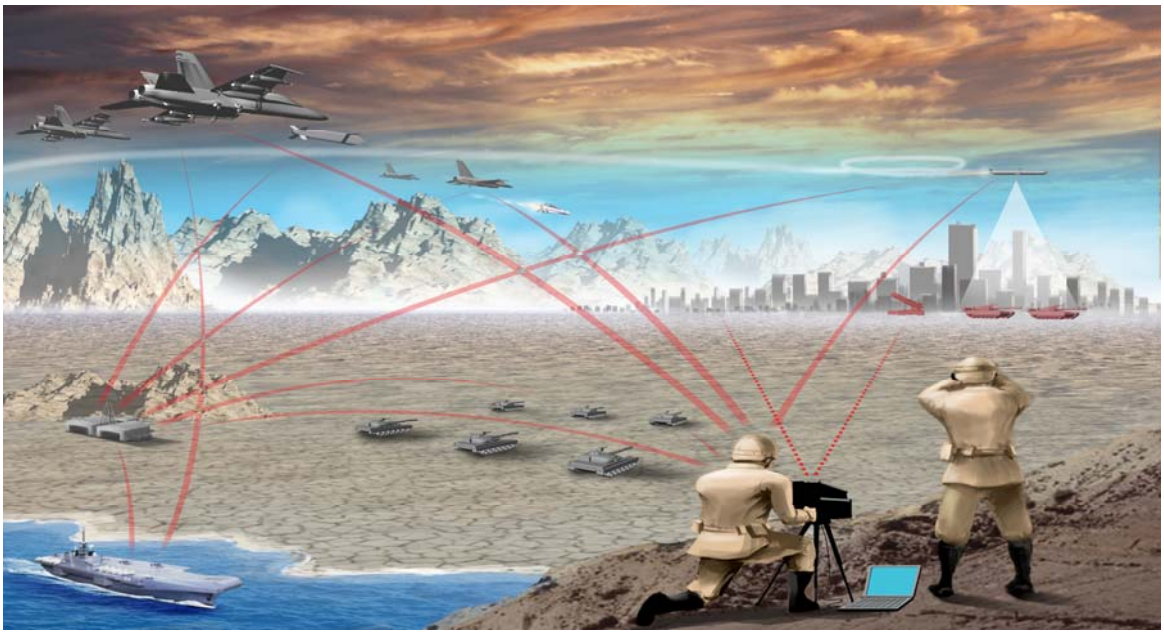

Figure 4. The Situational Awareness and Persistent Surveillance Problem

.

The technical challenges associated with Situation Awareness are [Ref 1]:

- Inference engines
- Knowledge management
- Large scale relational and control frameworks
- Human-machine collaboration
- Cognitive modeling
- Dynamic "What If?" Analysis
- Contextual reasoning regarding problems having scale and uncertainty of battlespace issues
- Knowledge bases and tools to capture and represent diverse battlespace expertise
- Interactive human-machine hypothesis management
- Visualization and cognitive interfaces

The technical challenges associated with Persistent ISR are:

- Persistent sensing
- Pervasive sensing
- C2 of platforms and sensors to meet dynamic operational and tactical needs
- Dynamic planning and replanning of sensor modality and coverage
- Distributed autonomous networks
- Automation to support Net-Centric Warfare
- Dynamic netted sensors

For Network-Centric Operations traditional intelligence, surveillance, and reconnaissance sensing (national and theatre, platform-based coverage) will need to be augmented by organic tactical sensors for responsive coverage of areas which are difficult to monitor, or for which access is denied. In particular, these current technology gaps include [Ref1]:

- "Automation for coordinated usage of multiple sensors, adaptive sensor control, and more robust sensing modalities
- Automation to drastically reduce manpower requirements and reverse the ratio of humans per sensor from a positive number to a fractional number — this will become especially important with the likely proliferation of small sensors for wide area coverage of difficult areas
- Small, networked sensors for wide area, inexpensive alerting in difficult / denied areas"

Figure 5. shows one possible solution to the Situational Awareness and Persistent ISR problem.

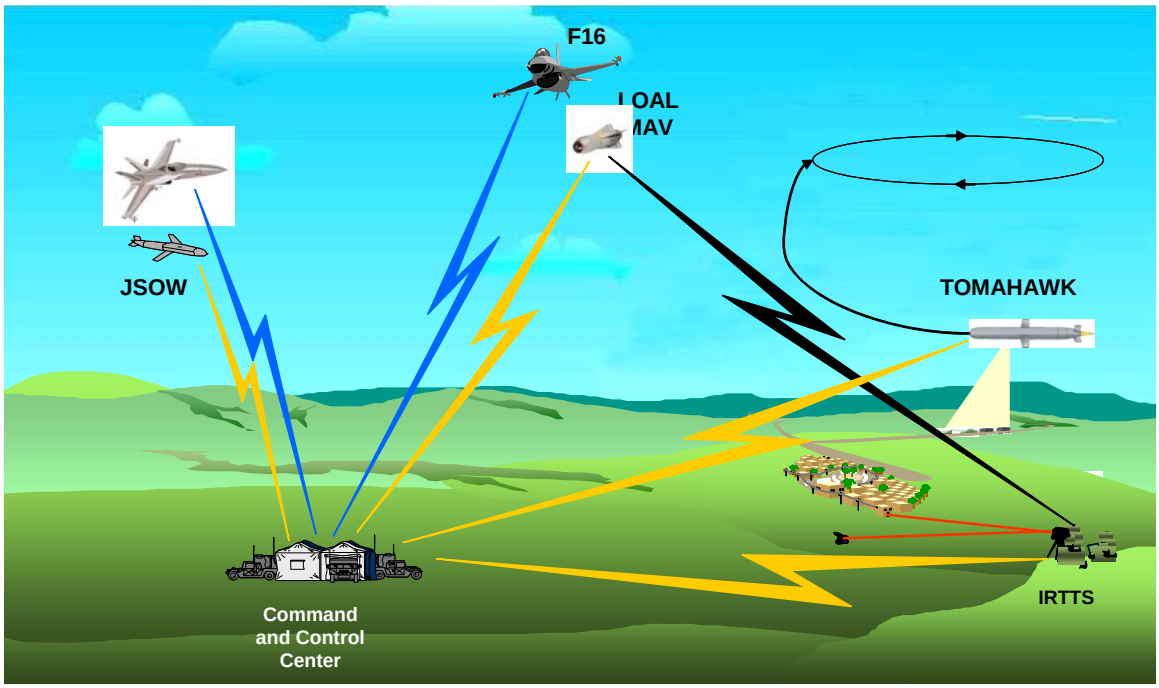

Figure 5. Potential Solution for Situational Understanding and Persistent ISR Problem

Information Assurance

Information Assurance, IA, is one of the most critical operational capabilities for FORCEnet to be successful. There is a demand for assured information, assured processing, protection from intrusions, protection from insider threats, ability to share data across joint services and coalitions, and the ability to be able to trust the data and information. Inadequate technology exists to provide the necessary level of information assurance to support the FORCEnet vision. The network need for sharing information must be balanced with traditional information assurance roles involved in protecting information. This challenge is made more difficult under conditions requiring trusted information exchange across multiple independent levels of security and coalition partners.

The Information Assurance technical challenges include [Ref 1]:

- Automated network analysis / monitoring
- Dynamic balancing of protection levels, including policy adaptation, with sharing needed to maintain mission effectiveness
- Trustworthiness of software systems
- Intrusion detection
- Identify insider threats
- Metrics

Figure 6. One solution to cross domain information sharing with joint services and coalition partners

The Compartmented High Assurance Information Network, CHAIN, shown in Figure 6. is one possible solution to a portion of the Information Assurance problem. It is designed to support coalition sharing in a Net Enabled Capability Environment. It provides for filtering, automatic policy updates and dissemination, automated and manual data release, and spiraling-in of best of breed COTS. It supports E-Mail, Data sharing, and collaboration capabilities.

Dynamic Composability and Collaboration

Today's technology does not support Dynamic Composability and Collaboration on the fly. A number of essential elements must be addressed to achieve the FORCEnet vision

of a mission composable capability and still maintain campaign level control and coordination of forces. In particular, these current technology gaps include [Ref 1]:

- "Complexity of managing mission composability in a way that assures integrated resource allocation to meet dynamic mission goals and achieve desired campaign outcomes
- A 'readiness' monitor that confirms the state of the entire FORCEnet enterprise (core plus communities of interest, across all enterprise layers) in any given configuration, for all users
- Manpower and training programs to teach and utilize composed functionality
- Tools to support automated means to facilitate collaboration between people and / or machines and to include planning / replanning functions"

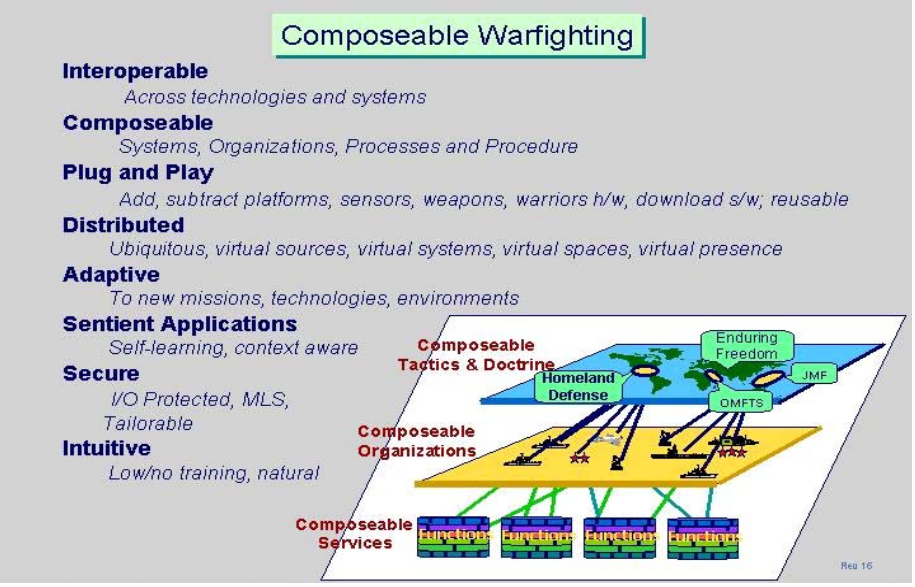

Figure 7. Navy Analysis of Composability [Ref 4]

Composability is the ability to assemble the systems components to allow for dynamic capability changes. These capabilities are composed to give the warfighter the specific capabilities that are needed for a particular operational scenario. The concept of FORCEnet Composability is discussed in Reference 4. The concept of composability involves all of the attributes as shown on the left side of Figure 7. In the right hand bottom corner of Figure 7 are the major types of components that must be dynamically composed to include tactics and doctrine, organizations, and services.

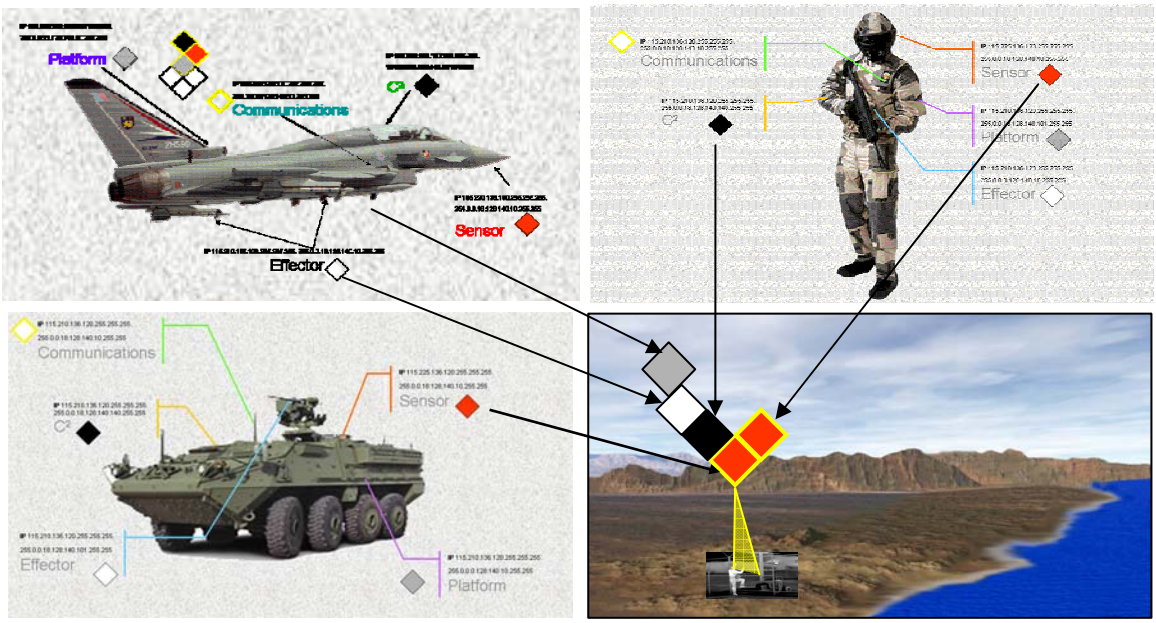

Figure 8. One aspect of the solution for composability

Composability will be facilitated by a systems of systems implementation and its transformation to a systems of elements as shown in Figure 8. The systems of elements will allow a battlespace to be completely connected and reconnected as the operational scenario evolves. The system will have a substantial understanding of the situation and can control the sources and sensors to ensure pervasive surveillance. The FORCEnet system can automatically task and reconfigure the sensors to provide the warfighter with a clear understanding of the environment, the threat, and the threat's intentions. The FORCEnet system can allocate resources to optimize their use and facilitate focused logistics.

Figure 9. depicts a solution that will support the Navy by using dynamic composability and collaboration. This will improve overland sensor performance by netting sensors, platforms and warfighters to expand the FORCEnet view of the battlespace. Improved missile performance and sensing, coupled with augmented autonomous guidance will expand the detection envelope of the sensor network and will free the missiles to operate overland and beyond radar line of sight of the firing ship. Taken together, these improvements will free strike fighter assets for power projection missions.

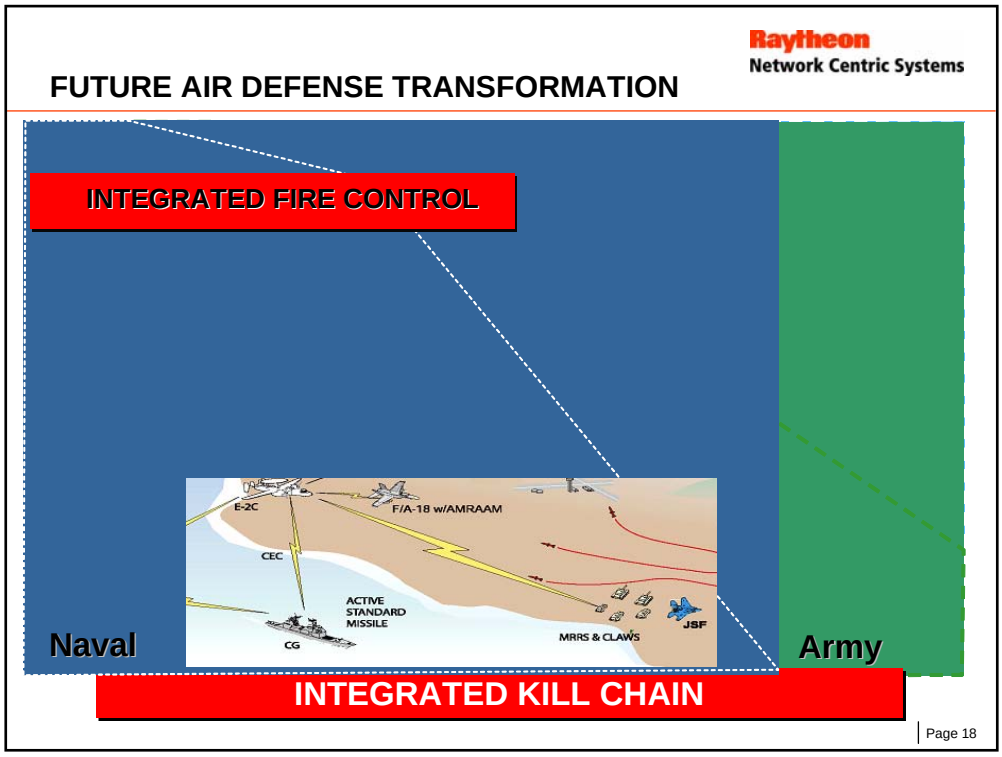

Figure 9. The vision for the future is to use dynamic composability and collaboration to transform into the next generation integrated fire control

Summary

The FORCEnet operational capabilities were described and technical challenges were identified. Several key science and technology needs were identified and they must be overcome before FORCEnet will be a success. Potential solution sets were presented that will permit the Navy to carryout the FORCEnet concept and coalitions to work in a Net Enabled Concept, NEC.

References

1) **NRC "FORCEnet Implementation Study", December, 2005** (http://darwin.nap.edu/books/0309100259/html/
2) **Franklin, Jude E., "FORCEnet Science and Technology Needs, CCRTS, June, 2006**
3) **CNO FORCEnet Operational Capabilities, 2005**
4) **Space and Naval Warfare Systems Command, FORCEnet Government Reference Architecture Version 1.0, April, 2003**