Use of Modeling and Simulation (M&S) in Support of the Quantitative Assessment of FORCEnet Systems and Concepts

William K. Stevens, Ph.D.[*]
Metron, Incorporated
512 Via de la Valle, Suite 301
Solana Beach, CA 92075
Tel: 858-792-8904
Email: stevens@ca.metsci.com

Abstract

The work to be described in this paper addresses recent advances in the application of modeling and simulation (M&S) techniques to the problem of quantifying the force-level warfighting value-added of FORCEnet and related doctrine and systems in the context of realistic scenarios including Operational War Plans (OPLANs). The M&S activities discussed in this paper have been conducted in support of operational experiments and wargames, as part of analyses in support of CINC-level commands, and as a part of analyses in support of certain specific acquisition programs having the requirement to demonstrate synergy with ongoing U.S. Department of Defense (DoD) and U.S. Navy FORCEnet and Network Centric Warfare (NCW) improvement programs. Lessons-learned concerning the challenges associated with representing information technology (IT) infrastructure improvements along with required FORCEnet/NCW warfare process re-engineering (WPR) initiatives will be presented. An iterative cycle of WPR initiative formulation and evaluation is often a *required* part of an assessment of the force-level warfighting value-added of specific FORCEnet/NCW improvements. This paper will also describe the extent to which the M&S approaches employed in the analyses alluded to above are consistent with the OSD (C3I) *Network Centric Warfare Conceptual Framework*. This framework provides a basis for making quantitative assessments of the degree to which specific Mission Capabilities Packages (MCPs), IT infrastructure improvement initiatives, and associated warfighting process improvements yield operational value-added in the manner envisioned by the tenants of NCW.

1. Description of the Problem

The U.S. Navy FORCEnet initiative, as the next generation of Network Centric Warfare (NCW), holds the promise of enabling light, mobile, and technologically advanced forces across the spectrum of Military and Homeland Security mission areas. Under this FORCEnet vision, U.S. Joint and Naval forces will be supported by mobile technologies tailored to each force element enabling tactical decisions (which under current operational doctrine require central command authorization) to be made at the unit or even individual unit or soldier level without deviating from applicable Joint and Naval Forces Commanders' objectives and guidance. This self-synchronization of Joint and

[*] This work was performed under SPAWAR Contract N00039-01-D-2202.

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE
JUN 2003

2. REPORT TYPE

3. DATES COVERED
00-00-2003 to 00-00-2003

4. TITLE AND SUBTITLE
Use of Modeling and Simulation (M&S) in Support of the Quantitative Assessment of FORCEnet Systems and Concepts

5a. CONTRACT NUMBER

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)
Metron Inc,512 Via de la Valle Suite 301,Solana Beach,CA,92075

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 **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**		**42**	

Naval forces will maximize the likelihood that the response timelines required to successfully achieve mission objectives (e.g. the engagement of time critical targets) are obtained.

The work to be described in this paper addresses recent advances in the application of modeling and simulation (M&S) techniques to the problem of quantifying the force-level warfighting value-added of FORCEnet in the context of realistic scenarios including Operational War Plans (OPLANs). The FORCEnet M&S activities to be reported in this paper have taken place in support of operational experiments and wargames, as part of analyses in support of CINC-level commands, and as a part of analyses in support of certain specific acquisition programs having the requirement to demonstrate synergy with ongoing DoD/Service FORCEnet and IT improvement programs. Lessons-learned concerning the challenges associated with representing IT infrastructure improvements along with required FORCEnet warfare process re-engineering (WPR) initiatives will be presented. It will be shown that an iterative cycle of WPR initiative formulation and evaluation is often a ***required*** part of an assessment of the force-level warfighting value-added of specific FORCEnet and IT improvements. We have found that M&S tools hence provide an important adjunct to operational experimentation in the role of formulating and evaluating the WPR initiatives which will likely provide the most warfighting value-added for specific IT improvements relative to specific sets of scenarios or war plans.

This paper will also describe the extent to which the M&S approaches employed in the analyses alluded to above are consistent with the OSD (C3I) *Network Centric Warfare Conceptual Framework*[1]. This framework provides a basis for making quantitative assessments of the degree to which specific Mission Capabilities Packages[2], IT infrastructure improvement initiatives, and associated warfighting process improvements yield operational value-added in the manner envisioned by the tenants of Network Centric Warfare[3]. This paper includes a generic Conceptual Framework Case Study illustrating the degree of this consistency.

2. **Background**

2.1 ***FORCEnet***

The information age is clearly changing the nature of conflict. The Gulf War showed the power of information and precision guided weapons in defeating an enemy employing traditional military formations. The wars in Somalia and Kosovo, as well as the subsequent terrorist acts of Al Qaeda and others, however, have also shown that paramilitary groups (or terrorist cells) organized in small, dispersed, networked units can deploy effectively against U.S. and Allied military and civilian defense/security forces. In response to these events, each of the U.S. military services are investigating new approaches to enable light, mobile, and technologically advanced forces; but the doctrine (along with needed situation assessment and planning/control technologies) have yet to be developed and hence the current warfighting and security capabilities provided by these new initiatives are significantly short of what is possible technically. The

[1] *Network Centric Warfare Conceptual Framework*, Network Centric Warfare and Network Enabled Capabilities Workshop: Overview of Major Findings, 17-19 December, 2002, OSD(C3I) in conjunction with RAND Corporation and Evidence Based Research (EBR) Inc.

[2] Alberts, David S., *Mission Capability Packages*, Washington, D.C., National Defense University Strategic Forum, 14 January 1995.

[3] Alberts, David S., John J. Garstka, and Frederick P. Stein, *Network Centric Warfare: Developing and Leveraging Information Superiority*, 2nd Edition (Revised), Washington, D.C., CCRP Publication Series, 1999.

analyses described here have the goal of providing technology to enable the U.S. military to use mobile communications and pervasive network-based computing to achieve the goals articulated in the Naval Transformation Roadmap[4] (NTR).

Current U.S. Navy FORCEnet related initiatives are at best at an embryonic state of design and development. R&D addressing network-based shared awareness and the dynamic allocation of forces and effects to tasks is critically needed. From *Washburn*[5]*,* "*… without changes in the way that an organization does business, it is not possible to fully leverage the power of information,*" and "*information is of no value unless the decision maker has the power to use it.*" *Stevens*[6,7] provides concrete examples of the utility of FORCEnet (and NCW) concepts to a real world OPLAN including examples of the typical warfare process re-engineering steps required to fully leverage FORCEnet information related improvements. The analyses discussed here have the goal of generating warfare process re-engineering recommendations and supporting prototype decision support technologies required to enable U.S. Joint and Naval operations to be conducted in the form of a dispersed, self-synchronized, networked force.

2.2 *Network Centric Warfare Conceptual Framework*

The OSD (C3I) *Network Centric Warfare Conceptual Framework (NCW CF)* provides a basis for making quantitative assessments of the degree to which specific Mission Capabilities Packages (MCPs), IT infrastructure improvement initiatives, and associated warfighting process improvements yield operational value-added in the manner envisioned by the tenants of NCW. The NCW CF partitions warfighting into three main domains as follows: the Physical Domain, the Information Domain, and the Cognitive Domain. The **Physical Domain** is the domain in which physical warfighting entities reside, e.g. the platforms, systems, and command entities operating in the ground, sea, air, and space environments. This domain is often referred to as "ground truth" or the actual time evolving state of all physical warfighting entities. Metrics in this domain measure the degree to which literal warfighting objectives are achieved, e.g. threats killed, own forces killed, and resources expended.

The **Information Domain** is the domain in which information is created, manipulated, and shared. Information in this context includes sensor reporting, intelligence system reporting, and all command and control (C2) interactions. The time evolving Information Domain will generally contain multiple characterizations of the Physical Domain or ground truth. These multiple characterizations may correspond to information held and processed at different C2 locations or alternate characterizations that may evolve at a single C2 location. Metrics in this domain generally address the extent to which collected information and subsequent processing results in information products that a decision maker could use to characterize or capture ground truth.

[4] *Naval Transformation Roadmap, Power and Access … From the Sea*, U.S. Department of the Navy.

[5] *Bits, Bangs, or Bucks? The Coming Information Crisis*, Naval Postgraduate School, by Alan R. Washburn, May 2000.

[6] *Use of Modeling and Simulation (M&S) in Support of the Assessment of Information Technology (IT) and Network Centric Warfare (NCW) Systems and Concepts,* Proceedings of the Second SMi Conference on Network Centric Warfare, London, UK, 4-5 October 2000, by W.K. Stevens.

[7] *Use of M&S in Support of the Assessment of Information Technology (IT) and Network Centric Warfare (NCW) Systems and Concepts,* Proceedings of the 5th International Symposium on Command and Control Research and Technology, Canberra ACT, Australia, 24-26 October 2000, by W.K. Stevens.

The **Cognitive Domain** resides in the mind of the decision maker. This domain includes all processes by which commanders transform information into decisions; and it specifically includes the concepts of commander's knowledge, awareness, and understanding. In more traditional military terms, this includes commander's objectives; commander's intent; concept of operations (CONOPs); tactics, techniques, and procedures (TT&P), etc. Metrics in this domain address the extent to which commander's decisions based on his perception of the Physical Domain compare with the theoretical optimal decisions that he might make given perfect perception of the Physical Domain.

The Network Centric Warfare Conceptual Framework (NCW CF) introduces a set of *primitives*, associated *attributes* and *metrics* and organizes these in the form of a hierarchy of measures useful for understanding and quantifying NCW military value-added. This NCW CF is pictured below in Figure 2.2-1. Some of the more important NCW CF *attributes* include sensing, information, knowledge, awareness, understanding, sharing, collaboration, decisions, actions, agility, and synchronization. Each of these *primitives* has associated sets of *attributes* and *metrics*. *Attributes* are used to capture the key characteristics of each *primitive* within the context of a specific military application or set of applications. *Metrics* are standards of measurement which enable the quantification of warfighting value-added. *Metrics* in this context are typically computed as functions of the *attributes* of the associated *primitive*. Brief definitions of some of the more important NCW CF *primitives* are provided in the paragraphs that follow.

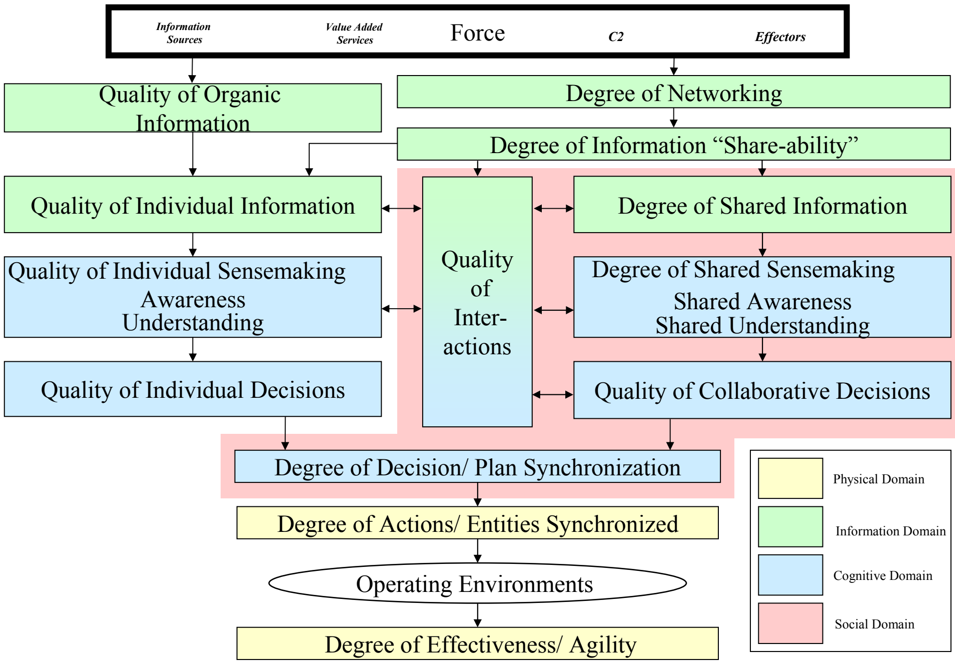

Information Sources
Value Added Services
Force
C2
Effectors
Quality of Organic Information
Degree of Networking
Degree of Information "Share-ability"
Quality of Individual Information
Quality of Interactions
Degree of Shared Information
Quality of Individual Sensemaking
Awareness
Understanding
Degree 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

Figure 2.2-1. Network Centric Warfare Conceptual Framework (Reference [1]).

Sensing is the use of direct (i.e. observation) or indirect (i.e. via a sensor system) means to generate observations of some aspect of the physical domain. Sensing attributes include the direct and indirect sensing physical architecture (represented at the platform and system level), physical domain observables (represented at the platform and platform emission/observable level), and the stream of observations/detections generated over time. Sensing metrics might include real detection rates, accuracies (e.g. spatial miss distances), correctness (e.g. correct/incorrect classification/ID), completeness, and latencies (e.g. for observations requiring processing) for each observable.

Information is the result of a process whereby collections of observations (generated as the result of Sensing) are put into a meaningful context. Information attributes include the data fusion physical architecture (represented at the platform/node level), physical domain observables (represented at the platform and platform emission/observable level), resultant set of tracks generated over time at each data fusion node. Here track = set of correlated observations with the means to estimate past, current, or future states. Information metrics might include tracking times/durations, track accuracies (e.g. spatial miss distances), track correctness (e.g. correct/incorrect classification/ID), track purity, and track latencies for each observable, and numbers of false tracks vs. time.

Knowledge is the result of a process whereby collections of observations (generated as the result of Sensing and placed in context as the result of Information processing) are employed to draw operationally relevant conclusions. Knowledge attributes include the C2 physical architecture (represented as a hierarchy of group, mission, unit commanders), individual commanders plans and tactics. Here *tactics* = agent-based rules which operate on the commanders tactical picture and result in situation assessment conclusions and pre-planned responses. Knowledge metrics might include command order latencies = time from threat initiation of an observable activity requiring an own force response to the time that an own force commander issues an order which adequately addresses the threat activity. A more involved knowledge metric might attempt to compare the own force assessment/response with the theoretically optimal assessment/response.

Awareness is the ability to place one's Knowledge of the current perceived situation in the context of prior relevant experiences. **Understanding** builds on awareness and represents the commanders ability to predict the future consequences of current actions/decisions.

Decisions are a commander's operational directions to subordinate forces over time. Decisions are made within the context of high level objectives, CONOPs, TT&Ps, and the commanders levels of Knowledge, Awareness, and Understanding. Decision attributes include the C2 physical architecture (represented as a hierarchy of group, mission, unit commanders), individual commanders plans and tactics. Here *plans* = pre-planned actions and *tactics* = agent-based rules which operate on the commanders tactical picture and result in situation assessment conclusions and pre-planned responses. Decision metrics might include command order latencies = time from threat initiation of an observable activity requiring an own force response to the time that an own force commander issues an order which adequately addresses the threat activity.

Actions are the physical domain result of a commander's Decision. Actions include directed force movements, sensing, communicating, employment of countermeasures, engaging, etc. Action attributes include the force physical architecture (represented at the platform and system level), and related platform and system capabilities and performance (C&P) attribute data. Action metrics include a wide range of metrics designed to capture the ability of a force to sense (see Sensing), communicate, employ countermeasures, engage, etc.

Information Sharing is the use of direct (e.g. human interactions) or indirect (e.g. via a communications system) means to share Information between two or more warfighting entities. Information sharing attributes include the C2 physical architecture (at the force, mission, and unit levels of command), communications physical architecture (represented at the platform and system level), and communications plan (which specifies the rules by which information is shared/distributed). As an example, the Cooperative Engagement Capability (CEC) architecture can be explicitly represented. Information Sharing metrics might include the comparison of the tactical pictures held vs. time at two or more command locations in terms of the **Information** metrics listed above.

Shared Knowledge is the result of a process whereby observations generated/received at multiple command sites are employed at each site to draw operationally relevant conclusions and responses which result in coordinated force-level actions. Shared Knowledge attributes include the communications physical architecture, communications plan, C2 physical architecture (represented as a hierarchy of group, mission, unit commanders), individual commanders plans and tactics. A combination of Information Sharing and coordinated tactics can be used to represent Shared Knowledge and resultant coordinated force actions. Shared Knowledge metrics might include the comparison of warfighting outcomes for coordinated and uncoordinated C2 excursions.

Collaboration is the result of a defined process whereby multiple command entities work together for a common purpose, e.g. resolve tactical picture ambiguities over a common AOR. Collaboration attributes include the communications physical architecture, communications plan, C2 physical architecture (represented as a hierarchy of group, mission, unit commanders), individual commanders plans and tactics. A combination of Information Sharing and coordinated plans and tactics can be used to represent Collaboration and resultant increased force effectiveness. Collaboration metrics might include a comparison of warfighting outcomes for collaborative and non-collaborative C2 excursions.

Synchronization is the orchestration of distributed operations in order to achieve a desired effect. This orchestration can be achieved via detailed planning or via shared awareness plus commander's guidance sufficient to achieve the desired level of orchestration. Synchronization attributes include the communications physical architecture, communications plan, C2 physical architecture (represented as a hierarchy of group, mission, unit commanders), individual commanders plans and tactics. A combination of Information Sharing and coordinated plans and tactics can be used to represent Synchronization and resultant increased force effectiveness. Synchronization metrics might include a comparison of the warfighting outcomes for synchronized and non-synchronized C2 excursions.

3. **The Naval Simulation System (NSS)**

3.1 ***Overview***

The Naval Simulation System (NSS) provides a comprehensive force-on-force modeling and simulation capability. NSS models individual platforms, weapons, sensors, C3 systems, and the responsive tactical decision making of commanders. NSS is capable of representing C4ISR, logistics, forces engagement, and commander's logic simultaneously for multiple players at a common level of fidelity. NSS models operations ranging from mission-level M-on-N engagements to full theater-level campaigns. NSS is capable of gathering a variety of performance metrics. These metrics provide for graphic results display and for post-processing data analysis.

NSS models the interaction of various force assets, based on initial plans, and the dynamic reaction of commanders. Dynamic command decisions in NSS are based upon a generated, perceived tactical picture, not the ground truth position of targets. The tactical picture is generated from the inputs of organic and remote sensors. Commanders dynamically respond to this perceived tactical picture based on tactics tables and the availability of resources.

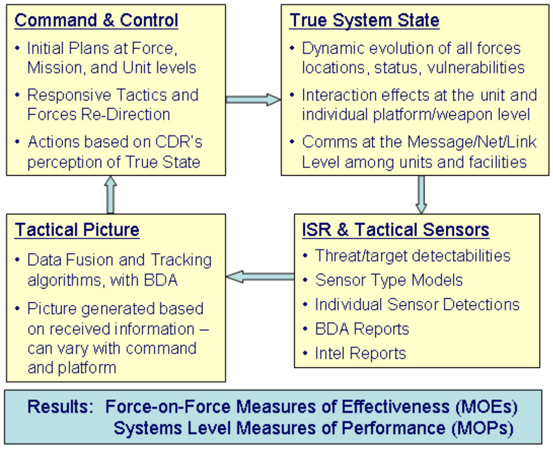

Command & Control
• Initial Plans at Force, Mission, and Unit levels
• Responsive Tactics and Forces Re-Direction
• Actions based on CDR's perception of True State
True System State
• Dynamic evolution of all forces locations, status, vulnerabilities
• Interaction effects at the unit and individual platform/weapon level
• Comms at the Message/Net/Link Level among units and facilities
Tactical Picture
• Data Fusion and Tracking algorithms, with BDA
• Picture generated based on received information – can vary with command and platform
ISR & Tactical Sensors
• Threat/target detectabilities
• Sensor Type Models
• Individual Sensor Detections
• BDA Reports
• Intel Reports
Results: Force-on-Force Measures of Effectiveness (MOEs)
Systems Level Measures of Performance (MOPs)

Figure 3.1-1. NSS Functional Segments.

NSS Scenario Development: The NSS Graphical User Interface, see Figure 3.1-2, provides a five-step process for scenario creation, in which the user defines:

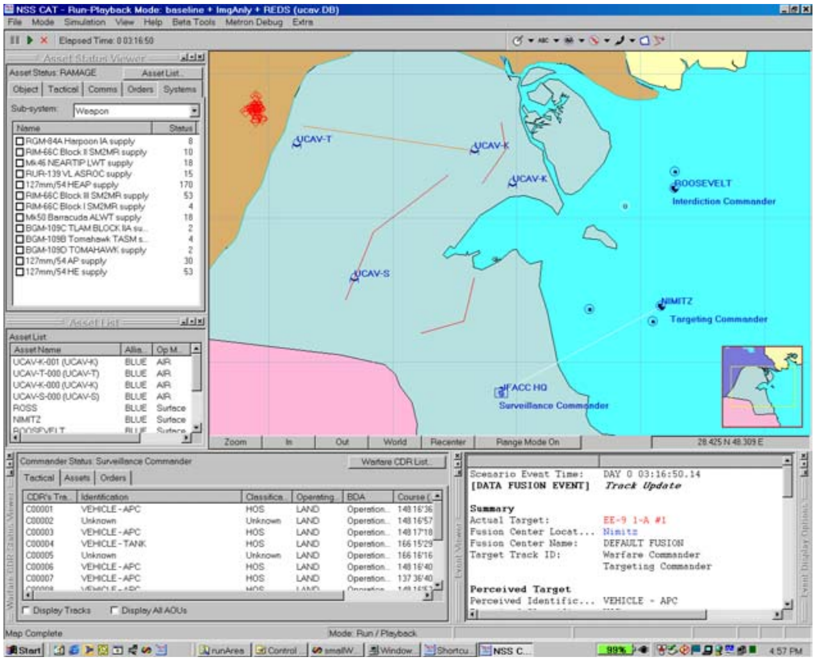
- **Forces**: Forces' OOB, command structures, and alliances are defined. Assets are assigned to commanders.
- **C2 Plans and Tactics**: Initial plans and responsive tactics are defined for each commander and asset.
- **Ops plans**: Motion Plans for surface, subsurface, and land assets are defined. Communication networks, surveillance schedules, and logistic plans are specified.
- **Platform Mission Plans**: Initial ISR, AW, ASW, SUW, and STW plans for aircraft are defined.
- **Metrics**: The user specifies and defines the metrics to be collected. Over 100 metrics are pre-defined. Additional metrics may be specified by users.

Characteristics and Performance Database: NSS comes with a fully-defined, yet modifiable, classified database containing data on specific U.S. and foreign platforms, communications, surveillance, weapons, and C2 systems that are immediately available to the user.

Interactive Playback: The NSS Run/Playback mode provides for interactive review of an NSS scenario. The Run/Playback interface allows the user to display the following features:

- Ground truth location of assets.
- Commanders' perceived location of targets for selected assets and facilities.

- Commander and Asset Status Viewer for display of the tactical picture of each commander and asset, messages transmitted, and orders given and received.
- Sensor and weapon ranges.
- Communication links and message transmission.
- Alert messages indicating the details of each event in the scenario.



Name	Status
□ RGM-84A Harpoon IA supply	8
□ RIM-66C Block II SM2MR supply	10
□ Mk46 NEARTIP LWT supply	18
□ RUR-139 VL ASROC supply	15
□ 127mm/54 HEAP supply	170
□ RIM-66C Block III SM2MR supply	53
□ RIM-66C Block I SM2MR supply	4
□ Mk50 Barracuda ALWT supply	18
□ BGM-109C TLAM BLOCK IIA su...	2
□ BGM-109B Tomahawk TASM s...	4
□ BGM-109D TOMAHAWK supply	2
□ 127mm/54 AP supply	30
□ 127mm/54 HE supply	53

Asset Name	Allia...	Op M...
UCAV-K-001 (UCAV-K)	BLUE	AIR
UCAV-T-000 (UCAV-T)	BLUE	AIR
UCAV-K-000 (UCAV-K)	BLUE	AIR
UCAV-S-000 (UCAV-S)	BLUE	AIR
ROSS	BLUE	Surface
NIMITZ	BLUE	Surface
ROOSEVELT	BLUE	Surface

CDR's Tra...	Identification	Classifica...	Operating	BDA	Course (...
C00001	VEHICLE - APC	HOS	LAND	Operation...	148 16'36
C00002	Unknown	Unknown	LAND	Operation...	148 16'57
C00003	VEHICLE - APC	HOS	LAND	Operation...	148 17'18
C00004	VEHICLE - TANK	HOS	LAND	Operation...	166 15'29
C00005	Unknown	Unknown	LAND	Operation...	166 16'16
C00006	VEHICLE - APC	HOS	LAND	Operation...	148 16'40
C00007	VEHICLE - APC	HOS	LAND	Operation...	137 36'40
C00008	VEHICLE - APC	HOS	LAND	Operation...	148 16'5

□ Display Tracks □ Display All AOUs

```
Scenario Event Time:     DAY 0 03:16:50.14
[DATA FUSION EVENT]      Track Update

Summary
Actual Target:           EE-9 1-A #1
Fusion Center Locat...   Nimitz
Fusion Center Name:      DEFAULT FUSION
Target Track ID:         Warfare Commander
                         Targeting Commander

Perceived Target
Perceived Identific...   VEHICLE - APC
```

Figure 1.1-2. NSS Graphical User Interface.

Quantitative Analysis: Upon completion of the construction of a scenario, NSS employs a study mode to set up and execute production simulation runs. The study mode GUI permits determination of the number of Monte Carlo simulation replications for each simulation run, and parameter ranges for each run. Measures of performance and effectiveness are then automatically collected during execution. Data generated by NSS is ported to Microsoft Excel for graphical visualization and post processing, see Figure 3.1-3 below.

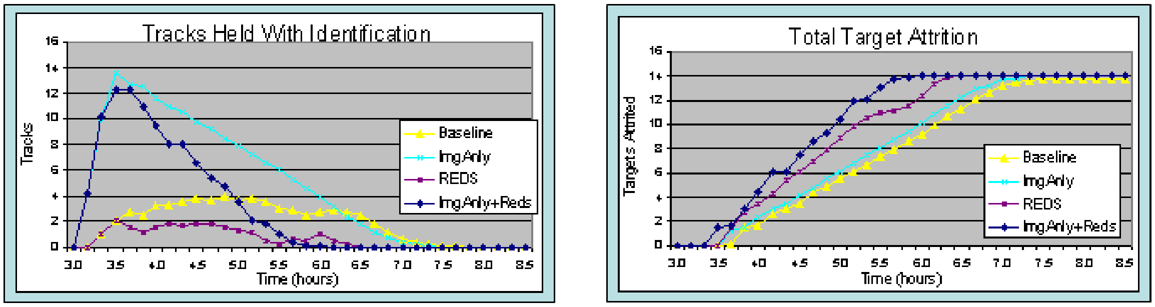


Figure 3.1-3. Example NSS Outputs.

3.2 *NSS Capability Relative to the CF for NCW Assessment*

Table 3.2-1 provides and overview summary of the attributes and metrics, associated with each Conceptual Framework primitive listed above in Section 3.1, which are currently supported within the Naval Simulation System (NSS).

Primitive	Attributes Represented in NSS	Metrics Represented in NSS
Sensing	Direct and indirect sensing physical architecture (represented at the platform and system level), physical domain observables (represented at the platform and platform emission/observable level), stream of observations/detections generated over time.	Real detection rates, accuracies (e.g. spatial miss distances), correctness (e.g. correct/incorrect classification/ID), completeness, and latencies (e.g. for observations requiring processing) for each observable.
Information	Data fusion physical architecture (represented at the platform/node level), physical domain observables (represented at the platform and platform emission/observable level), resultant set of tracks generated over time at each data fusion node. Here track = set of correlated observations with the means to estimate past, current, or future states.	Tracking times/durations, track accuracies (e.g. spatial miss distances), track correctness (e.g. correct/incorrect classification/ID), track purity, and track latencies for each observable. Numbers of false tracks vs. time.
Knowledge	C2 physical architecture (represented as a hierarchy of group, mission, unit commanders), individual commanders plans and tactics. Here *tactics* = agent-based rules which operate on the commanders tactical picture and result in situation assessment conclusions and pre-planned responses.	Command order latencies = time from threat initiation of an observable activity requiring an own force response to the time that an own force commander issues an order which adequately addresses the threat activity. *A more involved metric might attempt to compare the own force assessment/response with the theoretically optimal assessment/response.*
Awareness and Understanding	Current NSS decision making representations do not explicitly account for the impact of current actions/decisions on the emerging situation, except to the extent that these considerations can be built into intelligent agent tactical (assessment/response) rule sets.	The degree of a commander's awareness or understanding cannot currently be assessed in NSS, except to the degree that the specified plans and intelligent agent tactical rule sets can be shown to result in the desired warfighting outcome.
Decisions	C2 physical architecture (represented as a hierarchy of group, mission, unit commanders), individual commanders plans and tactics. Here *plans* = pre-planned actions and *tactics* = agent-based rules which operate on the commanders tactical picture and result in situation assessment conclusions and pre-planned responses.	Command order latencies = time from threat initiation of an observable activity requiring an own force response to the time that an own force commander issues an order which adequately addresses the threat activity.

Actions	Force physical architecture (represented at the platform and system level). Platform and system capabilities and performance (C&P) attribute data.	Numerous NSS metrics exist to capture the ability of a force to sense (see **Sensing**), communicate, employ countermeasures, engage, etc.
Information Sharing	C2 physical architecture (at the force, mission, and unit levels of command), communications physical architecture (represented at the platform and system level), and communications plan (which specifies the rules by which information is shared/distributed). As an example, the Cooperative Engagement Capability (CEC) architecture can be explicitly represented.	Comparison of the tactical pictures held vs. time at two or more command locations in terms of the **Information** metrics listed above.
Shared Knowledge	Communications physical architecture, communications plan, C2 physical architecture (represented as a hierarchy of group, mission, unit commanders), individual commanders plans and tactics. A combination of **Information Sharing** and coordinated tactics can be used to represent Shared Knowledge and resultant coordinated force actions.	No current NSS metrics directly address the level of Shared Knowledge and resultant force-wide coordination. One could, however, compare warfighting outcomes for coordinated and uncoordinated C2 excursions.
Collaboration	Communications physical architecture, communications plan, C2 physical architecture (represented as a hierarchy of group, mission, unit commanders), individual commanders plans and tactics. A combination of **Information Sharing** and coordinated plans and tactics can be used to represent Collaboration and resultant increased force effectiveness. FBE-D CSOF distributed/collaborative small boat ID/prosecution CONOPs is an example of this.	No current NSS metrics directly address the level of Collaboration and resultant increased effectiveness. One can, however, compare warfighting outcomes for collaborative and non-collaborative C2 excursions.
Synchronization	Communications physical architecture, communications plan, C2 physical architecture (represented as a hierarchy of group, mission, unit commanders), individual commanders plans and tactics. A combination of **Information Sharing** and coordinated plans and tactics can be used to represent Synchronization and resultant increased force effectiveness.	No current NSS metrics directly address the level of Synchronization and resultant increased effectiveness. One can, however, compare warfighting outcomes for synchronized and non-synchronized C2 excursions.

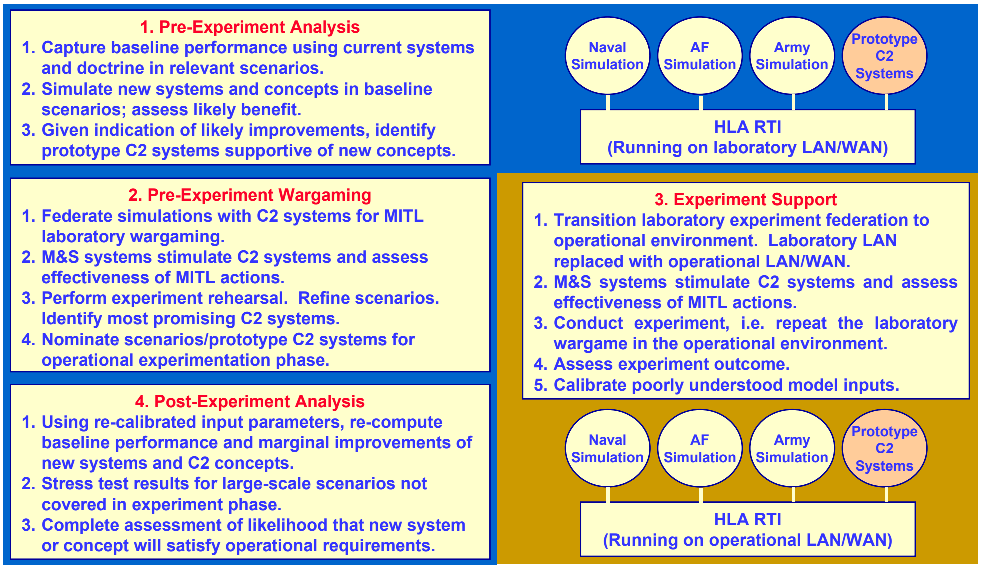
Table 3.2-1. CF Attributes and Metrics Represented in NSS.

4. Generic NSS Conceptual Framework Use Case

The following subsections describe the manner in which NSS is employed to conduct Network Centric Warfare and FORCEnet analyses. Several classified NSS FORCEnet analyses are underway which will be distilled into unclassified Conceptual Framework Case Studies in the coming year.

4.1 *Analysis Approach*

There are four main phases associated with the quantitative evaluation of FORCEnet systems and CONOPs (see Figure 4.1-1): pre-experiment analysis; pre-experiment wargaming; experimental evaluation; and post-experiment analysis. In the pre-experiment analysis phase, baseline performance is assessed for current systems and procedures within the context of relevant warfighting scenarios. Analytic representation of FORCEnet and associated warfare process re-engineering (WPR) initiatives are also assessed as excursion cases and the potential value-added of these initiatives are assessed. Given sufficient predicted valued-added, existing or planned C2 decision-support systems supportive of the FORCEnet technologies and CONOPs of interest are also identified during this first phase.



1. Pre-Experiment Analysis

1. Capture baseline performance using current systems and doctrine in relevant scenarios.
2. Simulate new systems and concepts in baseline scenarios; assess likely benefit.
3. Given indication of likely improvements, identify prototype C2 systems supportive of new concepts.

2. Pre-Experiment Wargaming

1. Federate simulations with C2 systems for MITL laboratory wargaming.
2. M&S systems stimulate C2 systems and assess effectiveness of MITL actions.
3. Perform experiment rehearsal. Refine scenarios. Identify most promising C2 systems.
4. Nominate scenarios/prototype C2 systems for operational experimentation phase.

3. Experiment Support

1. Transition laboratory experiment federation to operational environment. Laboratory LAN replaced with operational LAN/WAN.
2. M&S systems stimulate C2 systems and assess effectiveness of MITL actions.
3. Conduct experiment, i.e. repeat the laboratory wargame in the operational environment.
4. Assess experiment outcome.
5. Calibrate poorly understood model inputs.

4. Post-Experiment Analysis

1. Using re-calibrated input parameters, re-compute baseline performance and marginal improvements of new systems and C2 concepts.
2. Stress test results for large-scale scenarios not covered in experiment phase.
3. Complete assessment of likelihood that new system or concept will satisfy operational requirements.

Figure 4.1-1. Four Phases of FORCEnet Evaluation.

In the pre-experiment wargaming phase, the existing or planned C2 systems supportive of the FORCEnet technologies in question are federated with simulation systems in order to support laboratory wargaming evaluation of the FORCEnet concepts and CONOPs to be evaluated during the experimental phase. Simulations are employed to appropriately stimulate the selected C2 decision support systems in order to assess the effectiveness on man-in-the-loop (MITL) decision-making. The objectives of this phase are experiment (phase 3) rehearsal, scenario refinement, and preliminary identification of the existing or planned C2 systems most supportive of the FORCEnet concepts and WPR initiatives in question. The result of this phase is the nomination of scenarios and C2 systems for employment during the experiment phase.

In the experiment phase, the laboratory MITL wargaming environment is transitioned to the operational environment. The laboratory local area network (LAN) is in effect replaced with corresponding operational local/wide area networks (LANs/WANs). Simulation systems may be again employed in this phase as necessary to augment live play. The aggregate of live and simulated warfighting activities and associated message and data flows are used to stimulate the manned C2 systems selected during phase 2. The conduct of the operational experiment mirrors phase 2 wargaming, with military operators and operational communications systems and data links replacing their laboratory equivalents. The result of this phase is an operational assessment of the value-added of the FORCEnet concepts and WPR initiatives proposed, taking into account as many of the complexities associated with the actual operational environment as is possible. An important by-product of this activity is the calibration of poorly understood simulation inputs such as key operator decision delays (e.g. time to resolve ambiguous contact reports, time to allocate fire assets to targets, etc.).

In the post-experiment analysis phase, the results of the three previous phases can be collected and augmented to form a complete assessment of the likelihood that the proposed FORCEnet concepts and WPR initiatives will satisfy relevant operational requirements. In this final phase, re-calibrated model input values derived from phase 3 experimentation can be used to re-compute baseline performance and to re-assess the expected marginal improvements derived from the proposed FORCEnet concepts and WPR initiatives. Analytic stress testing of the results for larger-scale scenarios is also possible in this phase.

4.1.1 *Metric Selection*

The entity-based, Monte Carlo, discrete-event simulation approach described in the paper has proven to provide one means to directly measure relevant Network Centric Warfare (NCW) and FORCEnet metrics in mission-to-campaign level scenarios. The key enabler of this IS metric capability is the explicit, entity-based representation of C4ISR effects including explicit representation of platforms, systems, and commanders; representation of detailed aspects of the command organization; commander's plans and doctrine including responsive behavior; information collection; information dissemination; tactical picture processing; and resultant warfighting interactions. Metrics computed with this approach can be used to quantify the impact of information technology (IT) infrastructure improvements and warfare process re-engineering (WPR) initiatives on warfighting outcome. This approach hence provides a perhaps unique means to capture, simulate and dynamically view, and quantify the performance of alternate C4ISR architectures and warfighting plans.

4.1.2 *Metrics and Statistics*

Typical Monte Carlo metrics are random variables which are computed once for each Monte Carlo replication of each warfighting scenario of interest. Examples of these metrics (X_n = value of metric X in replication number n) can include: (1) the percentage of threat subsurface units of a particular country/type tracked (or trailed or killed) on a particular day and time; (2) the average positional area of uncertainty of mobile missile launcher units of a particular country/type on a particular day and time; and (3) many others pertaining to the ability of a C4ISR architecture to observe, orient, decide, and act. Monte Carlo simulations can and should provide the following basic statistical outputs for each of these C4ISR metrics.

The estimated mean (μ) of X provides an estimate of the typical value of each metric X over some number N of Monte Carlo replications. See the equation below.

$$\mu \cong m = \frac{1}{N}\sum_{n=1}^{N} X_n .$$

The estimated variance (σ) of X provides an estimate of the variance of X, e.g. for a normally distributed random variable metric X, 95% of its values lie within 2σ of μ. See the equation below.

$$\sigma^2 \cong s^2 = \frac{1}{N-1}\sum_{n=1}^{N}(X_n - m)^2 .$$

The estimated variance of μ is approximated by the variance of m and (for normally distributed X) provides a 95% confidence bound on the estimated mean value of X. See the equation below.

$$\text{Variance}[m] = \frac{\sigma^2}{N} \cong \frac{s^2}{N}.$$

4.1.3 *Sensitivity and Excursion Analysis*

Monte Carlo runs can be organized in the form of multiple excursions of a baseline scenario plus multiple excursion cases. Excursion cases can be organized so as to support systematic investigation of variations of key study parameter values (e.g. variations in the assumed probability of kill of a threat surface-to-air missile site or sites) or of force composition (e.g. variations in squadron mix associated with an aircraft carrier or airbase). Evaluation of a common set of metrics across the baseline and excursion scenario cases permits the sort of sensitivity analysis pictured below in Figure 4.2.3-1.

Pictured in Figure 4.2.3-1 are notional results illustrating the possible sensitivity of a key metric (number of BLUE fighters killed) to variations in threat surface-to-air missile system probability of kill (Pk) and BLUE squadron mix. It is this type of sensitivity or excursion analysis which is normally of most interest to C4ISR analysis customers. It is also the case that metric sensitivities and trends arising from important parametric and force composition variations can be reported with a higher level of confidence than can the absolute values of individual metrics.

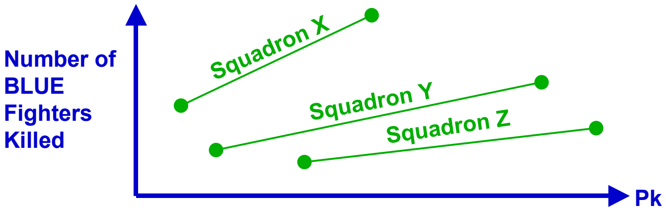


Figure 4.2.3-1. Excursion Analysis.

4.1.4 *Cause-and-Effect Analysis*

It is also the case that often times the most desired output of a C4ISR analysis is the answer to the following set of questions: "Did the proposed new C4ISR architecture yield a significantly improved warfighting result?" If so, what specific aspects or features of the proposed new C4ISR architecture were responsible for this improved warfighting result? What was the marginal contribution of each relevant aspect or feature of the C4ISR architecture to the overall improved warfighting outcome? While an automated approach for answering these questions is not available for Monte Carlo discrete-event simulation tools, there does exist a semi-automated, cause-and-effect analysis approach which can be used to address many questions of this type.

Pictured below in Figure 4.2.4-1 is a schematic diagram illustrating the cause-and-effect analysis approach employed in Naval Simulation System studies and analyses. For each C4ISR operational sequence (see left third of Figure 4.2.4-1) there can be associated sets of automated cause-and-effect metrics at the individual threat present level (see middle third of Figure 4.2.4-1), at the force level (see right third of Figure 4.2.4-1), and others. In addition, high-level metrics are computed to measure the ability of the C4ISR architecture to meet commander's objectives such as threats killed, own forces killed, resources expended, and the degree to which specific objectives were achieved. Given a high-level outcome (e.g. all commanders objectives achieved within desired time, resource, and own-force attrition constraints), the automated sets of cause-and-effect metrics can be examined to determine what specific aspects or features of the C4ISR architecture gave rise to the high-level result.

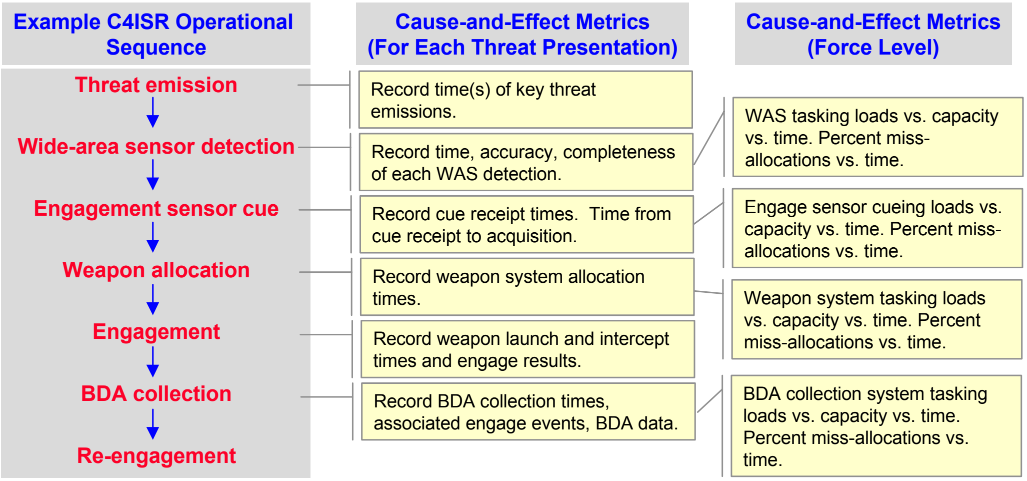

Example C4ISR Operational Sequence
Threat emission
Wide-area sensor detection
Engagement sensor cue
Weapon allocation
Engagement
BDA collection
Re-engagement
Cause-and-Effect Metrics (For Each Threat Presentation)
Record time(s) of key threat emissions.
Record time, accuracy, completeness of each WAS detection.
Record cue receipt times. Time from cue receipt to acquisition.
Record weapon system allocation times.
Record weapon launch and intercept times and engage results.
Record BDA collection times, associated engage events, BDA data.
Cause-and-Effect Metrics (Force Level)
WAS tasking loads vs. capacity vs. time. Percent miss-allocations vs. time.
Engage sensor cueing loads vs. capacity vs. time. Percent miss-allocations vs. time.
Weapon system tasking loads vs. capacity vs. time. Percent miss-allocations vs. time.
BDA collection system tasking loads vs. capacity vs. time. Percent miss-allocations vs. time.

Figure 4.2.4-1. Cause-and-Effect Analysis.

Marginal analyses can be conducted using a combination of sensitivity analysis and cause-and-effect analysis techniques. Suspected key performance drivers or collections of drivers are selectively added or removed from the baseline architecture. Differences in the high-level warfighting outcome measures provide quantification of the marginal value of the selected C4ISR drivers.

4.2 *Warfighting Process Improvement*

Information Technology (IT) infrastructure improvement programs in and of themselves are often not sufficient to result in warfighting value-added. What is often required are new command processes supported by new command and control (C2) applications designed specifically to take advantage of the Information Superiority (IS) that might result from IT improvement programs. *A commander who commands without regard to his information state will not benefit from an improved information situation.* Hence IT improvement programs will only result in significant warfighting value-added if there are associated C2 warfare process improvement programs designed specifically to leverage resultant IT/IS improvements.

The following notes briefly summarize lessons-learned to date concerning Network-Centric C2 application requirements. It is hypothesized here that individual commander/execution nodes should be allowed to exercise maximum autonomy and flexibility consistent with the force commander's guidance. The union of individual commander's actions must yield coherent, consistent, and effective global command and control. The above relies on existence of a common operational/tactical picture. The goal of network-centric C2 is to leverage the power of the network to enable speed of command improvements. What distinguishes a network-centric architecture from a platform-centric architecture is not just connectivity, but the attempt to push C2 functionality down to the lowest possible command level without having the C2 architecture degenerate into "every man for himself".

Network Centric Warfare relies on the existence of a single integrated operational/tactical picture which is managed via tactical picture management functions distributed throughout the C2 network. On-scene operational players should be able to support the management of the local picture for the force. Such distributed, network centric tactical picture management can be expected to yield the most significant performance impacts for manual processes such as ambiguous contact resolution in high-density cluttered target and background traffic environments and imagery and intelligence correlation and assessment. It is evident that the results of past-distributed fusion R&D can be applied to this problem.

Figure 4.3-1 provides a schematic for how Network Centric fusion might work, based on previous distributed data fusion prototyping efforts conducted for the Applied Physics Laboratory at Johns Hopkins University (APL/JHU) and elsewhere[8,9]. Under this approach, each command node in the network maintains a local picture as well as a shared common (networked) picture. The processing required for each local picture involves the following summary steps: (1) receive local/external data; (2) update the local picture; (3) compare the local picture with shared global picture; and (4) if differences exceed preset thresholds, communicate information "deltas" to others via the Joint Data Network (JDN). Similarly, the processing steps for each shared picture involves a similar set of processing steps: (1) upon receipt of a tactical picture information "delta", update both the local and global pictures; (2) compare the local picture with the global picture; and (3) if differences exceed preset thresholds, communicate information "deltas" to others via JDN. In this way, local on scene commanders can manage the local picture while providing appropriately down-sampled updates of the local picture to the entire force via the network. Figure 4.3-2 provides a slightly different view of this network centric data fusion scheme. Other concepts for Network Centric distributed data fusion exist as well.

[8] Fludzinski, M. T., Davidson, M. E., and Corwin, T.L., "Distributed Correlation and Tracking Study : Phase II", Metron Report to Applied Physics Laboratory, Johns Hopkins University (APL/JHU), 2 May 1984.

[9] Chrysostomou, A. K., and Maurer, D. E., "Measures for Attaining Consistent Tactical Pictures in Distributed Multiple-Hypothesis Correlation and Tracking Systems.", JHU/APL FS-92-004, January 1992.

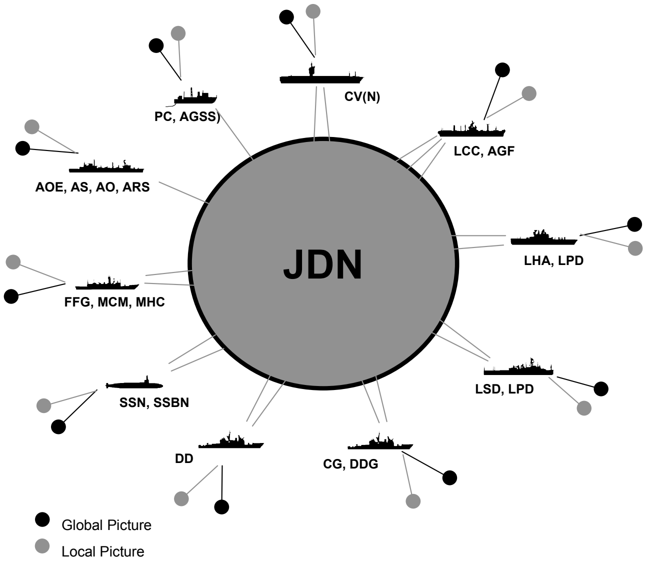


Figure 4.3-1. Network Centric Fusion.

In a similar fashion, network centric decision making will attempt to distribute tactical planning and decision functions throughout the C2 network. E.g. under network centric operations, force strike planning will be conducted as a collaborative, iterative process between the Joint force, component, and wing levels of command. As an example, the network centric decision making process might be characterized as follows. The force-level commander defines global and local mission goals and devises initial component-level plans. These initial plans are then disseminated to the component level. The component-level commanders then optimize the component-level plans based on local goals and information and then communicate refined plans back to force-level commander. The force-level commander resolves conflicts among multiple component-level plans and initiates a second round of iterations as required. Significant automation of this process, employing mathematical optimization techniques has been shown to be possible and R&D demonstration systems exist.

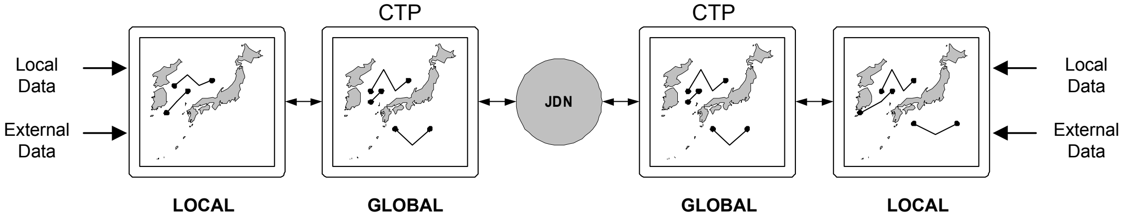


Figure 4.3-2. Another View of Network Centric Fusion.

Figure 4.3-3 provides a schematic for how network centric command and control (C2) might work, based on previous distributed C2 prototyping efforts conducted for the Naval Research Laboratory (NRL) and elsewhere[10,11]. Under this approach, the common operational/tactical picture supports

[10] "Weapon Target Allocation for Force Level Strike Planning", by R. Jakobovits, D. Carroll, and J. Hofmann, Proceedings of the 62nd MORS Symposium, June 1994.

coordinated decision-making across multiple levels of command. Each node in Figure 4.3-3 represents decision making at a single command level, which itself may be distributed over a large network of computer workstations. Tasks, in the form of targeting objectives, resource availability, and planning constraints, flow down the chain of command, and responses, in the form of subplans that accomplish each commander's assigned tasks, flow up the chain of command. Appropriate plan generation algorithms can be invoked by commanders at any level. At the unit level, the algorithms apply a mixture of classical mathematical programming techniques in order to produce attack and suppression plan recommendations. At the command level, conflicts among the subplans received from subordinates are identified and a combination of classical and heuristic deconfliction algorithms are used to recommend changes in subordinate tasking. Tasking is the mechanism by which each commander controls the planning process of his subordinates. Detailed planning is performed as far down in the chain of command as possible. Consensus plans, i.e. best feasible deconflicted plans currently available, can be generated at any point in time as the current response from one command level to the next. The entire system is recursive, i.e. additional layers add no further complication. Other concepts for network centric command and control (C2) exist as well.

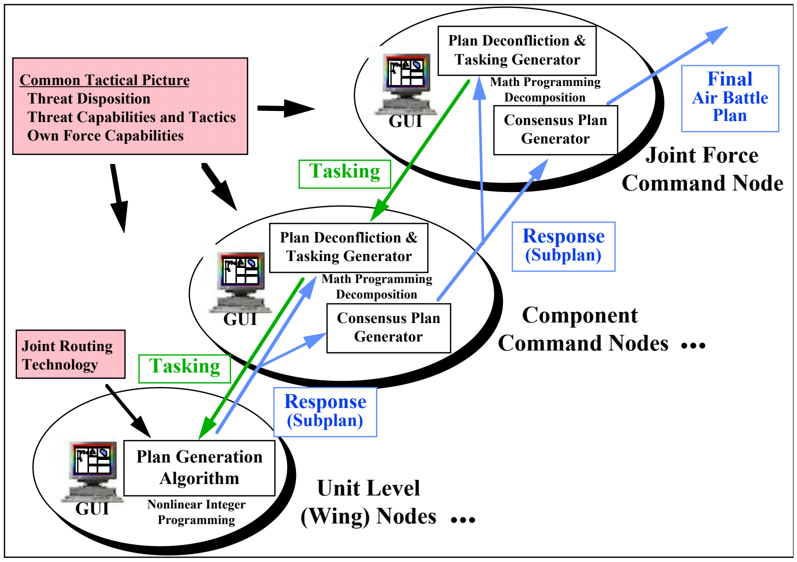

Common Tactical Picture
Threat Disposition
Threat Capabilities and Tactics
Own Force Capabilities
GUI
Plan Deconfliction & Tasking Generator
Math Programming Decomposition
Consensus Plan Generator
Final Air Battle Plan
Joint Force Command Node
Tasking
Response (Subplan)
GUI
Plan Deconfliction & Tasking Generator
Math Programming Decomposition
Consensus Plan Generator
Component Command Nodes •••
Joint Routing Technology
Tasking
Response (Subplan)
GUI
Plan Generation Algorithm
Nonlinear Integer Programming
Unit Level (Wing) Nodes •••

Figure 4.3-3. Another View of Network Centric Fusion.

5. Summary

In this paper we have discussed how the quantitative evaluation of Network Centric Warfare (NCW) and FORCEnet systems and concepts will typically involve both the representation and evaluation of information technology (IT) infrastructure improvements required to achieve information superiority (IS) plus the warfare process re-engineering (WPR) initiatives required to translate IS into warfighting value-added. Most of today's NCW and FORCEnet related initiatives are focused on the IT/IS part of this problem. Surprisingly little current effort is focused on identifying WPR requirements and beginning the job of designing, implementing, and fielding the needed set of next-

[11] *"Distributed Resource Allocation for Strike Planning",* by R. Jakobovits, and J. Hofmann, presented to the AFCEA/NRaD Joint C4I Symposium, May 1995.

generation NCW command and control (C2) decision support systems. A systematic, Department of Defense (DoD) focused effort is **required** to examine and, where necessary, re-formulate in NCW terms all Military decision processes in order to fully leverage ongoing IT, NCW, and FORCEnet investments.

The OSD (C3I) *Network Centric Warfare Conceptual Framework* has been proposed as a means for providing a basis for making quantitative assessments of the degree to which specific Mission Capabilities Packages, IT infrastructure improvement initiatives, and associated warfighting process improvements yield operational value-added in the manner envisioned by the tenants of Network Centric Warfare. It has been shown that the Naval Simulation System (NSS) is in many aspects consistent with this NCW conceptual framework and many of the metrics implied by the framework can be computed within NSS. Metrics which cannot be currently addressed by NSS correspond to higher cognition processes associated with Awareness and Understanding. Potential technical approaches for addressing these missing metrics are available however.

From a simulation technology point-of-view, the first generation of quantitative evaluations of NCW and FORCEnet systems and concepts (involving both IT/IS improvements plus WPR initiatives) are underway. Some of these are summarized in this paper. With the increasing recognition that simulation of the full C4ISR sensor-to-shooter decision chain is the key requirement for the next generation of DoD models, along with continued advancements in simulation software and hardware components, it is becoming increasingly feasible to conduct scientifically credible evaluations of relevant NCW systems and concepts. It is also the case, however, that significant challenges remain. Prominent among these challenges are model verification, validation, and accreditation (VV&A) and data verification, validation, and certification (VV&C). Nevertheless, there is good reason to believe that the future for the use of C4ISR entity-based, Monte Carlo, discrete event simulation to assess and iteratively improve upon NCW systems and concepts is bright.

METRON

West Coast Operations

http://www.metsci.com

Use of Modeling and Simulation (M&S) in Support of the Quantitative Assessment of FORCEnet Systems and Concepts

Corporate Headquarters:
11911 Freedom Drive
Suite 800
Reston, VA 20190-5602
(703)787-8700
(703)787-3518 (FAX)

Prepared
By
Dr. Bill Stevens, Metron Inc.
for
8th ICCRTS (Track 7 – IS/IO)
17-19 June 2003

Simulation Sciences Division:
512 Via de la Valle
Suite 301
Solana Beach, CA 92075-2715
(858)792-8904 (Voice)
(858)792-2719 (FAX)

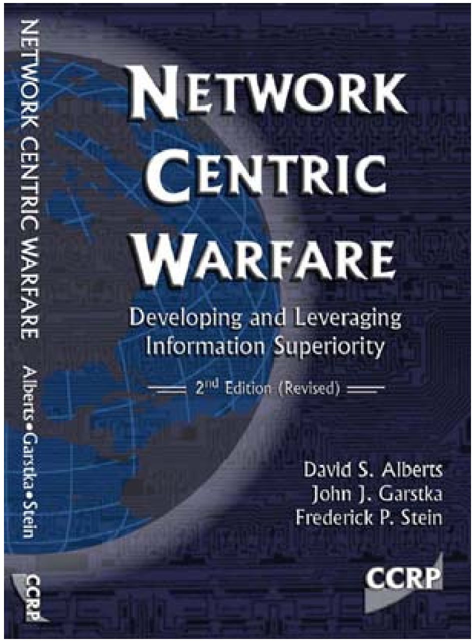
OUTLINE

- **FORCEnet**
  - **Definitions**
  - **Modeling and Simulation (M&S) Roles**
  - **Key M&S Challenges**
- Naval Simulation System (NSS)
  - Modeling Overview
  - Representation of FORCEnet
  - Current Applications
- POM-06 Campaign Assessment
  - Objectives
  - Approach
- Summary

FORCEnet

Fundamentals of Network Centric Warfare

- NCW: "An approach to the conduct of warfare that derives its power from the effective linking or networking of the warfighting enterprise".
  - "Effective linking/networking permits the employment of a geographically dispersed force".
  - "Effective linking/networking supports the shared awareness and understanding of commander's intent".
  - "Effective linking/networking permits dynamic allocation and re-allocation of forces and effects to tasks".

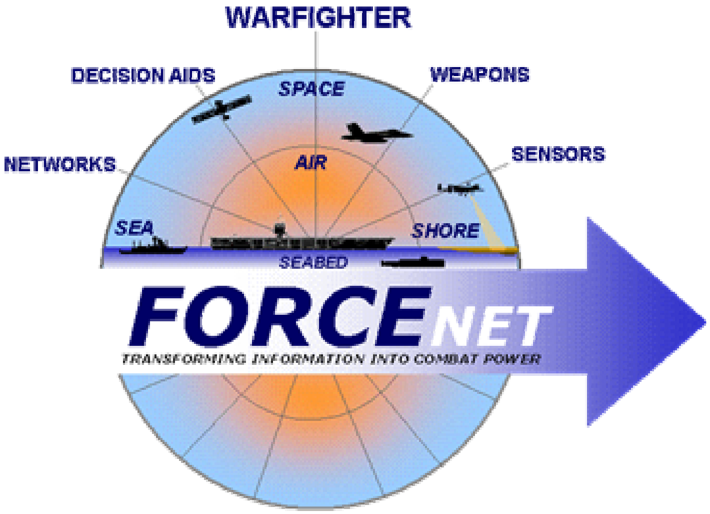

NETWORK CENTRIC WARFARE
Developing and Leveraging Information Superiority
2nd Edition (Revised)
David S. Alberts
John J. Garstka
Frederick P. Stein
CCRP
NETWORK CENTRIC WARFARE Alberts•Garstka•Stein CCRP

REF: *Network Centric Warfare: Developing and Leveraging Information Superiority,* Second Edition (Revised), Command and Control Research Program, May 1999, by David S. Alberts, John J. Garstka, and Frederick P. Stein.
REF: *Understanding Information Age Warfare*, Alberts, Garstka, Hayes, and Signori, Command and Control Research Program (CCRP), www.dodccrp.org, ASD(C3I), July 2002.

Key FORCEnet Goals

FORCEnet = USN Implementation of NCW

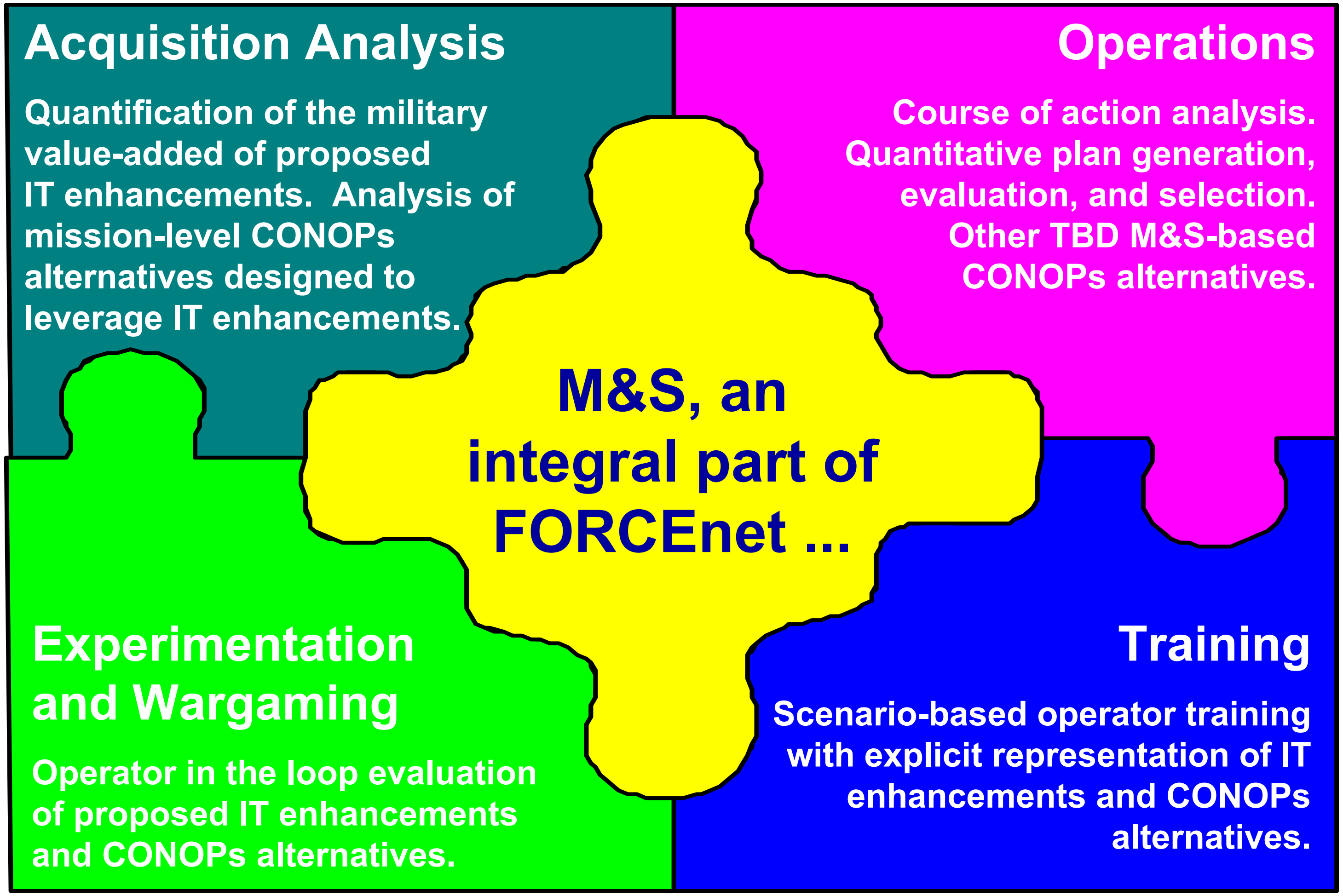
- “FORCEnet is the *architecture and building blocks* of *sensors, networks, decision aids, weapons, warriors* and *supporting systems* integrated into a highly adaptive, human-centric, comprehensive system that operates from seabed to space, from sea to land”.
- “By exploiting existing and emerging technologies, FORCEnet enables dispersed human decision-makers to leverage military capabilities to achieve *dominance* across the entire mission landscape with joint, allied, and coalition partners”.



REF: *Naval Transformation Roadmap, Power and Access … From the Sea*, U.S. Department of the Navy, 2003.

NCW and FORCEnet

M&S Roles



Acquisition Analysis

Quantification of the military value-added of proposed IT enhancements. Analysis of mission-level CONOPs alternatives designed to leverage IT enhancements.

Operations

Course of action analysis. Quantitative plan generation, evaluation, and selection. Other TBD M&S-based CONOPs alternatives.

M&S, an integral part of FORCEnet ...

Experimentation and Wargaming

Operator in the loop evaluation of proposed IT enhancements and CONOPs alternatives.

Training

Scenario-based operator training with explicit representation of IT enhancements and CONOPs alternatives.

NCW and FORCEnet

Key M&S Challenges

- Representation must be **information-based** vs. **attrition-based**.
- Representation must permit examination of mission-level CONOPs alternatives designed to leverage IS/IO infrastructure enhancements.
  - *"… without changes in the way that an organization does business, it is not possible to fully leverage the power of information".*
  - *"Information is of no value unless there is an uncertain decision maker".*
  - *"Information is of no value unless the decision maker has the power to use it".*
- Representation must be explanatory; e.g. it must be possible to trace cause and effect from FORCEnet infrastructure and CONOPs improvements to warfighting value-added.

REF: *Bits, Bangs, or Bucks? The Coming Information Crisis,* Prof. Alan R. Washburn, Naval Postgraduate School, May 2000.

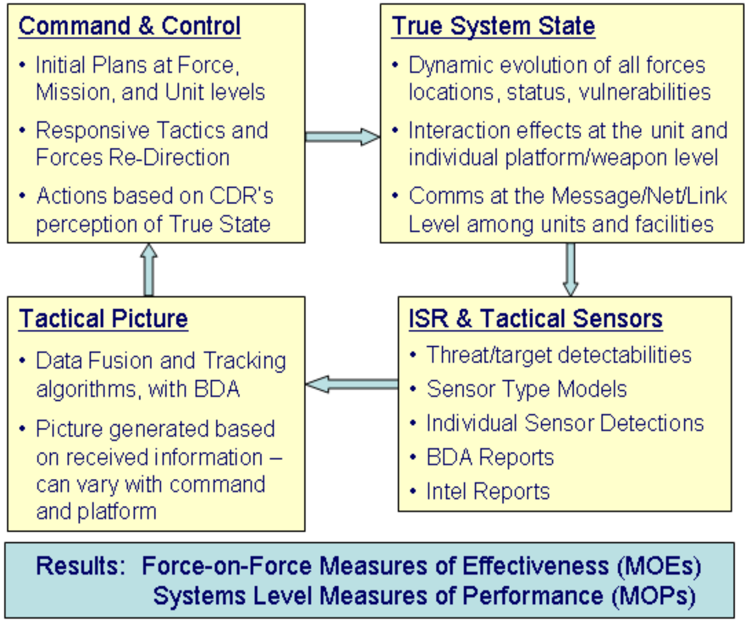
OUTLINE

- FORCEnet
  - Definitions
  - Modeling and Simulation (M&S) Roles
  - Key M&S Challenges
- **Naval Simulation System (NSS)**
  - **Modeling Overview**
  - **Representation of FORCEnet**
  - **Current Applications**
- POM-06 Campaign Assessment
  - Objectives
  - Approach
- Summary

Naval Simulation System (NSS)

Summary Model Capability

- **Force-on-force M&S capability.**
- **Models individual platforms, weapons, sensors, C3 systems, responsive decision making process.**
- **Simulated perceived tactical picture is generated from the inputs of organic and remote sensors.**
- **Models interaction of forces based on initial plans plus simulated dynamic reaction of commanders.**
- **Dynamic decision making is based on simulated perceived tactical picture vs. ground truth.**
- **Commanders respond to the picture based on tactical rule sets and availability of resources.**



Command & Control
- Initial Plans at Force, Mission, and Unit levels
- Responsive Tactics and Forces Re-Direction
- Actions based on CDR's perception of True State

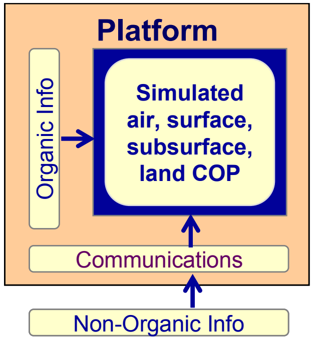
True System State
- Dynamic evolution of all forces locations, status, vulnerabilities
- Interaction effects at the unit and individual platform/weapon level
- Comms at the Message/Net/Link Level among units and facilities

Tactical Picture
- Data Fusion and Tracking algorithms, with BDA
- Picture generated based on received information – can vary with command and platform

ISR & Tactical Sensors
- Threat/target detectabilities
- Sensor Type Models
- Individual Sensor Detections
- BDA Reports
- Intel Reports

Results: Force-on-Force Measures of Effectiveness (MOEs)
Systems Level Measures of Performance (MOPs)

Fog of War Model Components:



Platform

Organic Info

Simulated air, surface, subsurface, land COP

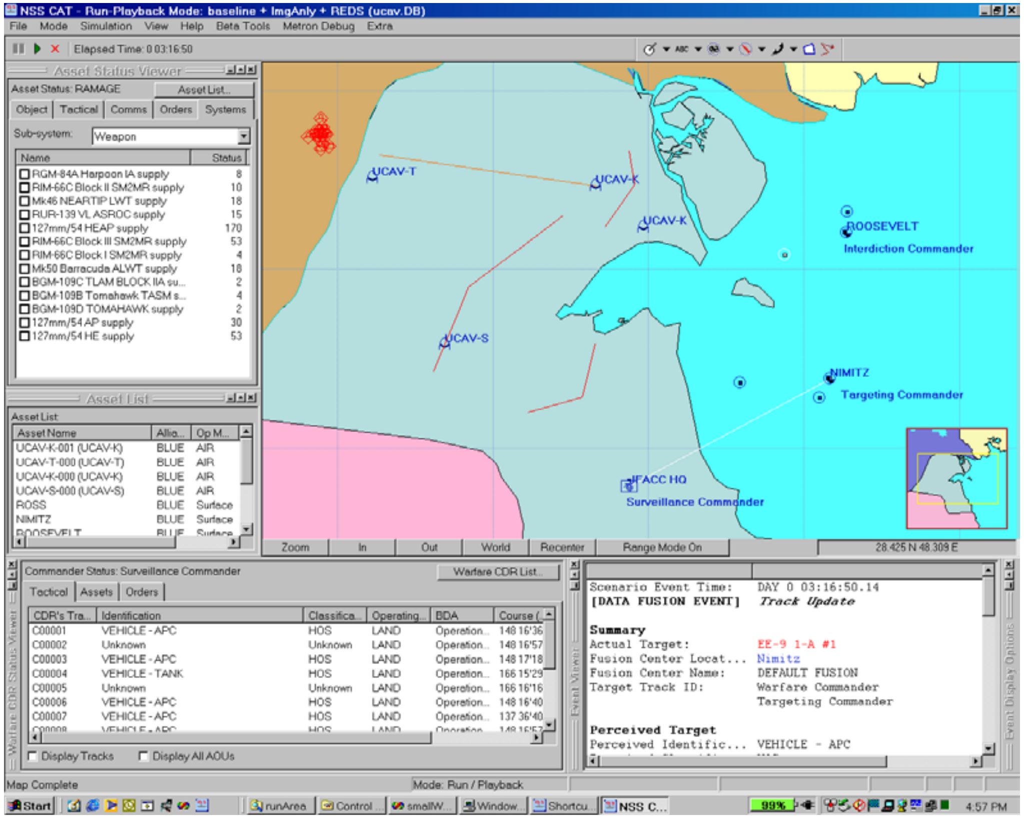
Communications

Non-Organic Info

Naval Simulation System (NSS)

Scenario Development Steps

- **Forces: Define OOB, command structures, and alliances. Assign assets to commanders.**
- **C2 Plans and Tactics: Define initial plans and responsive tactics for commanders and assets.**
- **Ops Plans: Define asset motion plans. Specify communications networks, surveillance schedules, and logistic plans.**
- **Platform Mission Plans: Define initial ISR, AW, ASW, SUW, STW, etc. mission plans.**
- **Metrics: Define the metrics to be collected.**



Asset Status: RAMAGE

Name	Status
□ RGM-84A Harpoon IA supply	8
□ RIM-66C Block II SM2MR supply	10
□ Mk46 NEARTIP LWT supply	18
□ RUR-139 VL ASROC supply	15
□ 127mm/54 HEAP supply	170
□ RIM-66C Block III SM2MR supply	53
□ RIM-66C Block I SM2MR supply	4
□ Mk50 Barracuda ALWT supply	18
□ BGM-109C TLAM BLOCK IIA su...	2
□ BGM-109B Tomahawk TASM s...	4
□ BGM-109D TOMAHAWK supply	2
□ 127mm/54 AP supply	30
□ 127mm/54 HE supply	53

Asset List:

Asset Name	Allia...	Op M...
UCAV-K-001 (UCAV-K)	BLUE	AIR
UCAV-T-000 (UCAV-T)	BLUE	AIR
UCAV-K-000 (UCAV-K)	BLUE	AIR
UCAV-S-000 (UCAV-S)	BLUE	AIR
ROSS	BLUE	Surface
NIMITZ	BLUE	Surface
ROOSEVELT	BLUE	Surface

Commander Status: Surveillance Commander

CDR's Tra...	Identification	Classifica...	Operating...	BDA	Course (...
C00001	VEHICLE - APC	HOS	LAND	Operation...	148 16'36
C00002	Unknown	Unknown	LAND	Operation...	148 16'57
C00003	VEHICLE - APC	HOS	LAND	Operation...	148 17'18
C00004	VEHICLE - TANK	HOS	LAND	Operation...	166 15'29
C00005	Unknown	Unknown	LAND	Operation...	166 16'16
C00006	VEHICLE - APC	HOS	LAND	Operation...	148 16'40
C00007	VEHICLE - APC	HOS	LAND	Operation...	137 36'40
C00008	VEHICLE - APC	HOS	LAND	Operation...	148 16'57

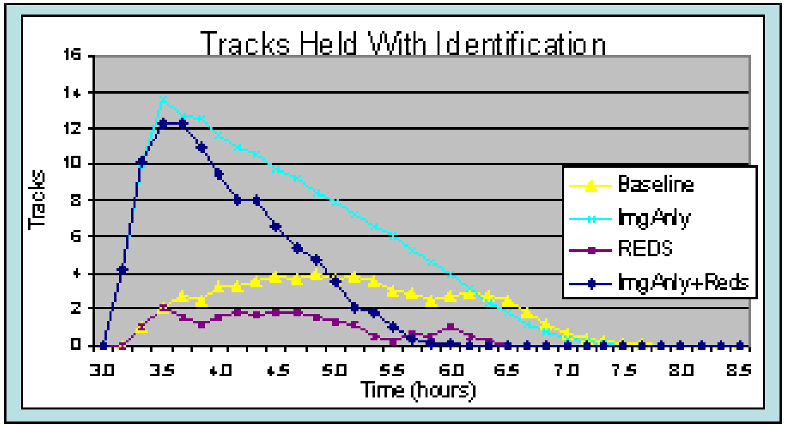
□ Display Tracks □ Display All AOUs

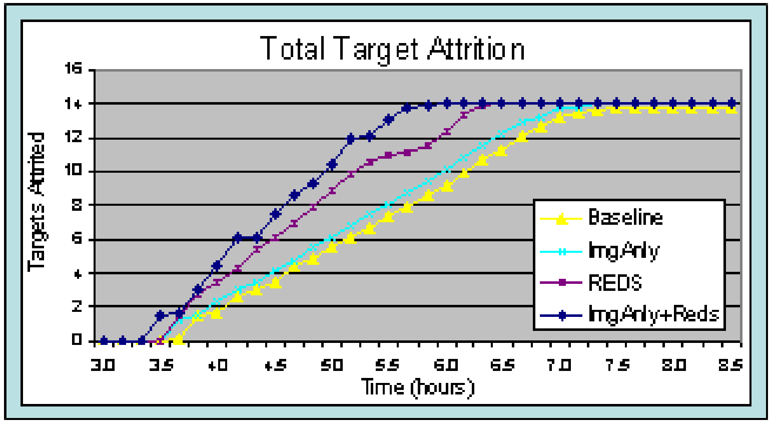
```
Scenario Event Time:         DAY 0 03:16:50.14
[DATA FUSION EVENT]          Track Update

Summary
Actual Target:               EE-9 1-A #1
Fusion Center Locat...       Nimitz
Fusion Center Name:          DEFAULT FUSION
Target Track ID:             Warfare Commander
                             Targeting Commander

Perceived Target
Perceived Identific...       VEHICLE - APC
```

Naval Simulation System (NSS)

Quantitative Assessment

- **<u>Study Mode:</u> Used to set up and execute production simulation runs, given baseline and excursion scenarios.**
- **<u>Monte Carlo Replications:</u> Users specify the number of simulation replications for each simulation run plus platform variations and parameter ranges for each run.**
- **<u>Metrics:</u> Users select from 100+ pre-defined metrics in the categories of C3, surveillance and tracking, engagement, and resources.**
- **<u>Outputs:</u> Metrics are automatically collected during execution. NSS supports scenario excursion analysis, parameter sensitivity analysis, cause-and-effect analysis, and statistical hypothesis testing techniques.**
- **<u>Formatting:</u> Microsoft Excel is used for graphical data display and post-processing.**

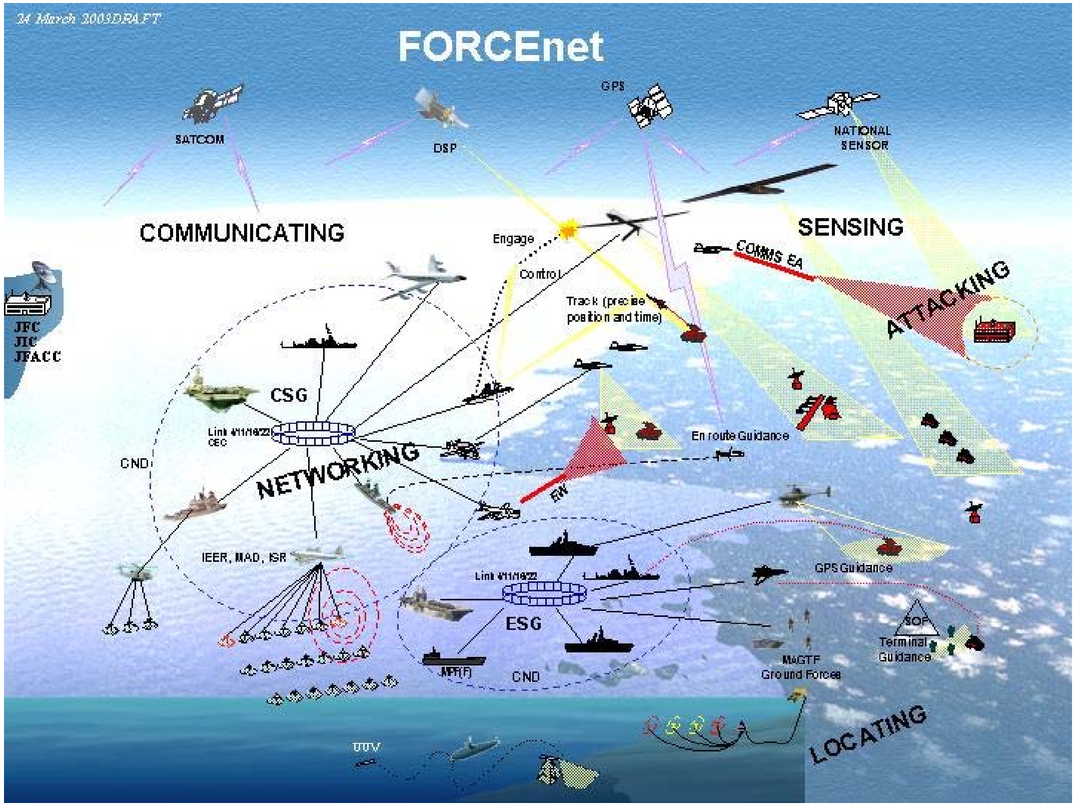




Naval Simulation System (NSS)

Representation of FORCEnet Systems and CONOPs

- **Explicit simulation of IT infrastructure upgrades including communications and networking.**
- **Explicit simulation of sensor architecture upgrades and resulting enhanced info flows.**
- **Explicit simulation of prosecution architecture upgrades and resulting faster accomplishment of warfighting goals.**
- **Explicit simulation of FORCEnet-driven mission level CONOPs alternatives and resultant impact on force-level outcomes.**



Naval Simulation System (NSS)

Current Applications

- CNO N70/N61F/N81 POM-06 Campaign Assessment. Assessment of FORCEnet value-added in an Amphibious Assault TACSIT.
- CNO N76 Surface Warfare (SUW) Phase II Capstone Requirements Study.
- COMPACFLT OPLAN review and evaluation, CONOPs development support to subordinate commands, and Fast Track system analysis.
- AF Space Command Ground Moving Target Indication (GMTI) radar analysis of alternatives (AoA).
- NAVAIR Multi-Mission Aircraft (MMA) program analyses.
- Joint Warfare Analysis Center (JWAC) analysis of IW/IO systems and concepts.
- Industry analyses in support of the Navy LCS and DD(X), USCG Deepwater, and various US and Foreign UAV/UCAV programs.

OUTLINE

- FORCEnet
  - Definitions
  - Modeling and Simulation (M&S) Roles
  - Key M&S Challenges
- Naval Simulation System (NSS)
  - Modeling Overview
  - Representation of FORCEnet
  - Current Applications
- **POM-06 Campaign Assessment**
  - **Objectives**
  - **Approach**
- Summary

POM-06 Campaign Assessment

Scenario/OPSIT and Key Questions

Objective:

Evaluate FORCEnet warfighting value-added.

Scenario:

Scenario: MTW-W 2012, Assault Operations OPSIT
Baseline: Programmed Systems (PB-04) in 2012.
Excursion: Additional (PB-04+) Systems and CONOPs (e.g. TCA).

Key Questions to be Addressed:

Q1: What is the relationship between improved connectivity and the speed/quality of decision-making and the successful outcome of combat operations?

Q2: What is the relationship between improved COP and the quality of decision-making and the successful outcome of combat operations?

Q3: How much bandwidth, and over what transmission modes 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?

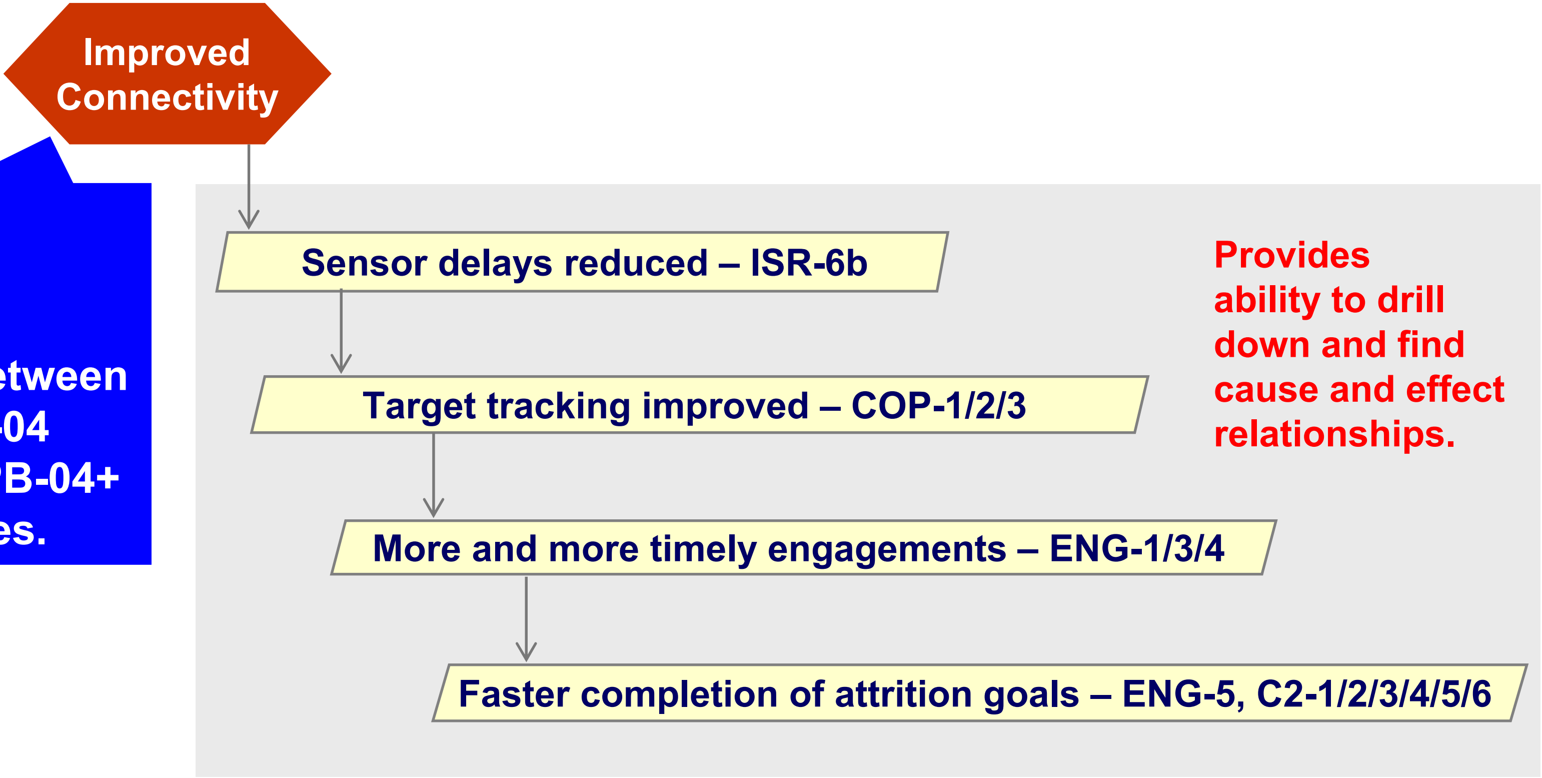
Q4: What is the impact of varying levels of network attacks on the successful outcome of combat operations? What types of redundancy, backups, and alternative paths are necessary to ensure successful warfighting outcomes?

POM-06 Campaign Assessment

Q1 – Improved Connectivity

Q1. Impact of Improved Connectivity on Decision-Making. **What is the relationship between improved connectivity and the speed/quality of decision-making and the successful outcome of naval/joint/coalition combat operations?**

Improved connectivity measured as a comparison between FORCEnet PB-04 baseline and PB-04+ excursion cases.



Improved Connectivity

Sensor delays reduced – ISR-6b

Target tracking improved – COP-1/2/3

More and more timely engagements – ENG-1/3/4

Faster completion of attrition goals – ENG-5, C2-1/2/3/4/5/6

Provides ability to drill down and find cause and effect relationships.

NOTE: ISR-xx, COP-xx, ENG-xx, and C2-xx refer to specific NSS metrics.

POM-06 Campaign Assessment

Q1 – Improved Connectivity

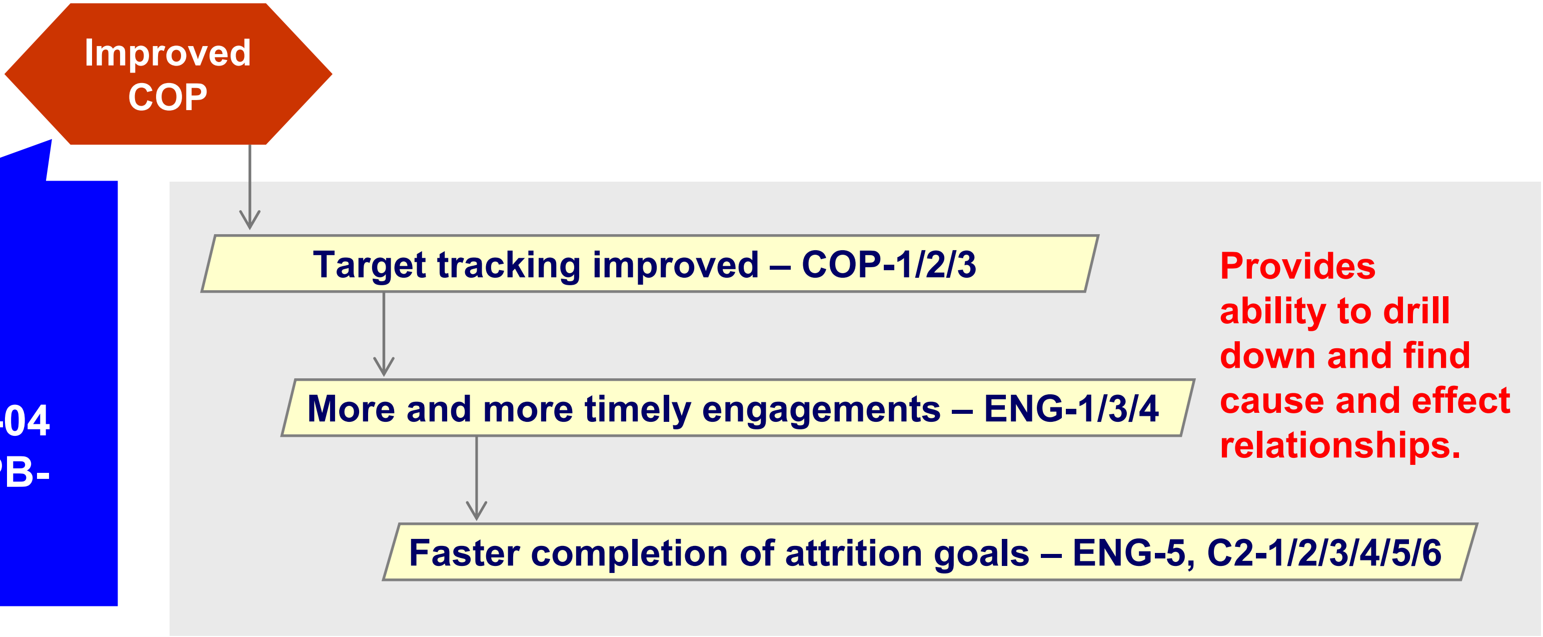
- Improved connectivity excursion cases to be addressed include:
  - Transformational Communications Architecture (TCA),
  - Greater reliance on pull vs. push communications plans.
- Improved connectivity analysis to include consideration of mission-level CONOPs alternatives designed to leverage connectivity enhancements, e.g.:
  - **Distributed Picture Management:** Given improved connectivity, enable all levels of command to participate in COP management. E.g. a tactical unit with a visual on a critical target should be enabled to update the COP. This results in a COP = union of the tactical knowledge held at all levels of command.
  - **Advanced Data Fusion:** Given improved connectivity, employ advanced data fusion techniques. Processing of both positive and negative search information; track targets as well as "cleared" areas. Historical tracking based on known target behaviors, known hiding locations, etc. Advanced analysis and prosecution of lost tracks, e.g. MTI lost track analysis. Intelligent agent tactical triggers and pre-planned responses.

POM-06 Campaign Assessment

Q2 – Improved COP

Q2. Impact of Improved COP on Decision-Making. **What is the relationship between improved common operational and tactical picture and the quality of decision-making and the successful outcome of naval/joint/coalition combat operations?**

Improved COP measured as a comparison between FORCEnet PB-04 baseline and PB-04+ excursion cases.


Improved COP
Target tracking improved – COP-1/2/3
More and more timely engagements – ENG-1/3/4
Faster completion of attrition goals – ENG-5, C2-1/2/3/4/5/6

Provides ability to drill down and find cause and effect relationships.

NOTE: COP-xx, ENG-xx, and C2-xx refer to specific NSS metrics.

POM-06 Campaign Assessment

Q2 – Improved COP

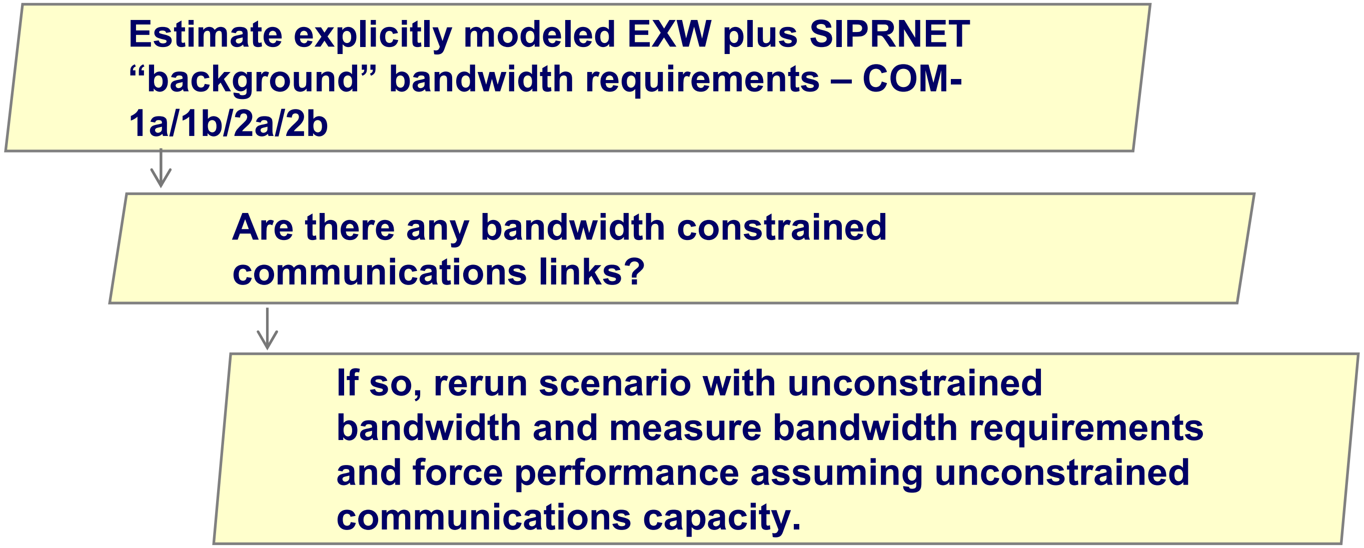
- Improved COP analysis to include consideration of mission-level CONOPs alternatives designed to leverage COP enhancements, e.g.:
  - **Minimization of Time-Distance Constraints:** Given the improved COP, examine surveillance and engagement asset stationing schemes that result in maximum numbers of tactical assets as close as possible to likely locations of pop-up time critical targets.
  - **Self-Synchronization:** Enable surveillance and engagement assets with commander's guidance, the improved COP, and the authority to act.
  - **Advanced Resource Allocation Schemes:** Employ mathematical optimization, along with improved COP and advanced data fusion techniques, to make more effective resource allocations. Design algorithms that work in a "power-to-the-edge" fashion, i.e. that can be executed at any level of command and produce globally optimal allocation recommendations.
  - **High Risk Maneuvers:** Given the improved COP, it might become feasible to maneuver forces without the risk of encountering threat forces and to hence conduct operations with a lighter, more nimble execution force.

REF: *Power to the Edge – Command and Control in the Information Age*, Draft Release, Alberts and Hayes, Command and Control Research Program (CCRP), www.dodccrp.org, ASD(C3I), April 2003.

POM-06 Campaign Assessment

Q3 – Bandwidth Requirements

Q3. Bandwidth Requirements. **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?**



Estimate explicitly modeled EXW plus SIPRNET "background" bandwidth requirements – COM-1a/1b/2a/2b

Are there any bandwidth constrained communications links?

If so, rerun scenario with unconstrained bandwidth and measure bandwidth requirements and force performance assuming unconstrained communications capacity.

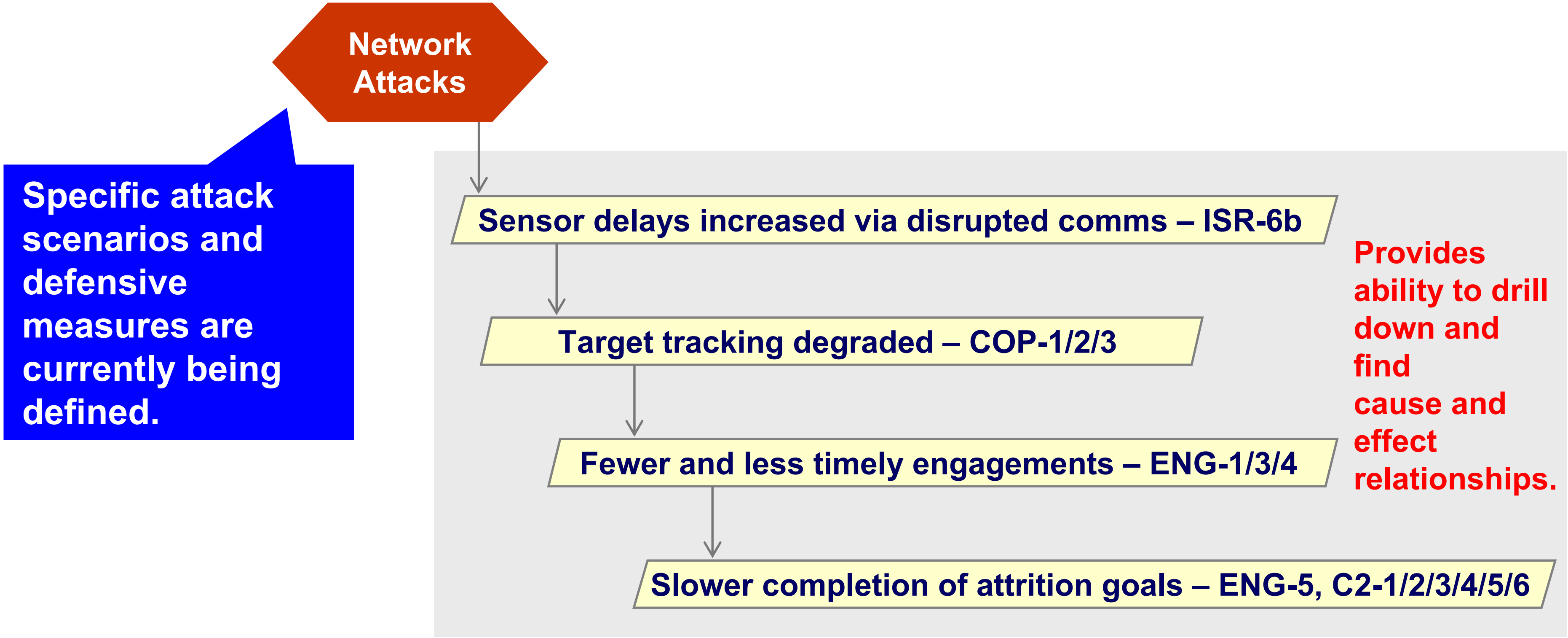
REF: *Analysis of Network Capacity: USS Blue Ridge during Exercise Terminal Fury 03 Phase 2 (U)*, Sunoy N. Banerjee and John A. Bentrup, CNA Report CRM D0007476.A1/Final, January 2003.

NOTE: COM-xx refers to specific NSS metrics.

POM-06 Campaign Assessment

Q4 – Network Attacks

Q4. Susceptibility to Network Attacks. 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?



Network Attacks

Specific attack scenarios and defensive measures are currently being defined.

Sensor delays increased via disrupted comms – ISR-6b

Target tracking degraded – COP-1/2/3

Fewer and less timely engagements – ENG-1/3/4

Slower completion of attrition goals – ENG-5, C2-1/2/3/4/5/6

Provides ability to drill down and find cause and effect relationships.

NOTE: ISR-xx, COP-xx, ENG-xx, and C2-xx refer to specific NSS metrics.

POM-06 Campaign Assessment

Q4 – Network Attack Related Definitions

- **Network Security** includes all measures required to: (1) insure that threat entities cannot extract data from own force networks; (2) insure that threat entities cannot insert data or modify data in own force networks; and (3) insure that threat entities cannot use virus or denial of service attacks to degrade the performance of own force networks.
  - **Threat Capture of Own Force Network Data:** This is the toughest of the three issues to model. It involves modeling how a commander would conduct C2 operations given some level of knowledge of the disposition or intent of the other side. One specific limiting case, the capture of the dispositions and states of threat forces, could be handled in NSS by replacing the commander’s imperfect perception of the other side (i.e. his simulated tactical picture) with ground truth.
  - **Threat Corruption Own Force Network Data:** Some aspects of network data corruption could be easily handled in NSS. This would include any scripted changes to the commander’s tactical picture (e.g. modify track areas of uncertainty, insert or delete tracks, insert or delete contact reports, etc.). Dynamic changes to the commander’s picture, wherein the time and nature of the change is determined based of the tactical situation, would obviously be more involved.
  - **Threat Network Attacks:** Assuming that the impact of a threat network attack would be disabling a node or slowing the response time of a communication link or processing center, this could be handled in a straightforward manner in NSS.

POM-06 Campaign Assessment

Q4 – NSS Network Attack Representations

- **Denial of communications links at specified times, for specified durations**:
  Results will show increased message delays, or lack of message transmission. Will require contingency CONOPs with communications plans including backup routing given loss of links (which would be required in real operations if real attacks on links were anticipated).
- **Denial of a particular sensor or information source**:
  Turn off the sensor at the time of attack. Degradation of the tactical picture will automatically result (e.g., loss of track ID due to loss of a SIGNINT sensor). Effect on target attrition can also be automatically computed in NSS.
- **Denial or destruction of databases or processing capabilities**:
  Suspension of processing capabilities and/or tactical picture at affected commands. Could also include employment of alternative tactics tables, based on pre-planned tactics alternatives that mimic real-world re-assignment of command responsibilities, as would be developed for such contingencies.
- **Insertion of false information into BLUE databases**:
  Degraded force effectiveness results from NSS, reflecting deviation of the perceived tactical picture from ground truth (as corrupted by the attack – e.g., spy on board the ship in the data fusion center). An example would be to falsely tag mobile targets as dead, which are in reality still in operation.

This NSS analysis is to be conducted as a part of the IA Excursion (CLE-7).

OUTLINE

- FORCEnet
  - Definitions
  - Modeling and Simulation (M&S) Roles
  - Key M&S Challenges
- Naval Simulation System (NSS)
  - Modeling Overview
  - Representation of FORCEnet
  - Current Applications
- POM-06 Campaign Assessment
  - Objectives
  - Approach
- **Summary**

SUMMARY

NSS Applicability to NCW and FORCEnet Assessments

- The quantitative assessment of NCW and FORCEnet systems and related CONOPs imposes new challenges for DoD M&S tools:
  - Representations must be information-based vs. attrition-based.
  - Examination of mission-level CONOPs alternatives must be supported.
  - Must be able to reveal detailed C4ISR cause-and-effect relationships.
- The Naval Simulation System (NSS) addresses these new M&S requirements, and has been successfully employed in IT-21, NCW, and FORCEnet analyses.
- NSS is currently supporting the OPNAV POM-06 Campaign Assessment, the OPNAV Phase II SUW Capstone Requirements Study, COMPACFLT OPLAN analyses, AF GMTI analyses, NAVAIR MMA analyses, JWAC analyses, and numerous industry programs.