

Cross Domain Maritime Surveillance and Targeting (CDMaST)

Industry Day

16 November 2015

Welcome!!



UNCLASSIFIED – Approved for Public Release



Agenda



Start	End	Topic	Presenter
08:00	08:10	Intro / Safety / General Security	R. Neidlinger / A. Boyd
08:10	08:30	Programmatics / Program Security	R. Neidlinger / A. Boyd
08:30	08:40	DARPA STO Overview	N. Sandell, STO Director
08:40	09:30	CDMaST Program Overview	J. Galambos, DARPA PM
09:30	9:45	Break	
9:45	10:15	LVC Testbed Overview	L. Nguyen, NAWC TSD
10:15	10:30	Question Submission	
10:30	10:45	Break	
10:45	11:30	Address submitted questions	J. Galambos, DARPA PM
11:30	12:45	Lunch- Unclassified session adjourned	
12:45	13:30	Classified Scenario Briefing	S. Robertson
13:43	14:30	Technology Program Briefings	Drs Patt, Littlefield, Kamp, Haas
14:30	14:45	Break	
14:45	15:30	Technology Program Briefings	Drs Krolik, Wichowski, Sullivan
15:30	15:40	Closing Remarks	J. Galambos, DARPA PM

CDMaST

Industry Day Safety and Security Briefing

Mark Doody

Program Security Officer

703-526-2687

Adam Boyd

Program Security Representative

(703) 812-1985

Adam.Boyd.CTR@darpa.mil





General and Safety Overview



- Ground Rules
- Public Release
- Emergency Procedures



Electronic Devices



- All electronic devices (two way pagers, cell phones, cameras, recording devices, laptop computers, etc.) are prohibited.
- These must be left with the technical office representative during registration, in the containers or checked-in with the Visitor Control Center.
- Use of recording devices is prohibited at all times.
- Access to any DARPA wired internet connections is prohibited without explicit permission from the DARPA/STO PSO



DARPA Conference Center Badges



- DCC white badges will grant you access to the authorized first floor areas ONLY (breakout conference rooms, lobby areas, café, restrooms).
- DCC badges must be clearly displayed at all times.
- If leaving the building during breaks, please conceal your DCC badges. If done for the day, please return DCC badge to registration staff member.
- If you misplace or lose your badge notify DARPA staff immediately.
- Only individuals with the proper badge will be admitted into the classified portion of the brief.
- Turn in all badges to DARPA staff prior to departing for the day.



Today's Session



- Morning Session will be UNCLASSIFIED
 - Note taking will be permitted during the unclassified portion of the briefing.
 - **NO NOTE TAKING DURING THE CLASSIFIED PRESENTATION!**
 - **NOTEBOOKS AND NOTEPADS MUST BE LEFT OUTSIDE OF THE CONFERENCE CENTER DURING THE CLASSIFIED PORTION.**
- CLASSIFIED level one-on-one meetings with PM



Public Release Information



- Proposed public disclosures of unclassified information regarding CDMaST will be processed for approval by DARPA prior to publication or distribution.
- One paper copy and one electronic copy on CD/DVD must be submitted at least 20 working days prior to the requested date to:

DARPA's Technical Information Office
675 North Randolph Street
Arlington, VA 22203



Proposal / Program Security Overview



- Proposals
- Security Overview
- Security Incidents



Classified Proposals



- Planning to submit a classified Proposal
 - To request the SCG and DD254 you must submit the formal request sheet via BAA mailbox DARPA-BAA-16-01@darpa.mil. Please specify in your email which documents you are requesting. Files that are sent will be sent via the AMRDEC SAFE site.
 - In order to request the classified briefing, please CLEARLY specify that you desire to receive the SECRET presentation shown at Industry Day.
 - **Only released to companies with SECRET FCLs and SECRET safeguarding**
 - Security Classification Guide & DD254 will be released to performers who meet the proper security requirements and complete the BAA 16-01 data request form
 - If you are planning on couriating classified from/to DARPA you must have courier approval issued by your security officer at time of arrival.
 - Mark classified proposals in accordance with the DoD Manual 5200.01 Vol. 2



Security Overview



- Unauthorized disclosure of SECRET Classified Information could be expected to cause serious damage to national security that the original classification authority is able to identify or describe.
- **Defense Security Service (DSS) is the Cognizant Security Office for Collateral Program Spaces and Automated Information Systems (AIS).**
- The DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) is the guide in which each performer will be required to adhere to with regards to protection of program information (safeguarding), facilities, and AIS.
- DARPA is the approval authority for actions involving SAP Testing (Collateral SECRET- DSS), Public Release, Contracting, etc.



Security Incidents or Concerns



- When reproducing , transmitting or conducting classified work, ensure that it occurs on appropriately cleared approved system at the appropriate level.
- Be aware of the classification level of your material. Data spills occur frequently due to lack of attention to detail.
- Be aware of the classification level when having discussions.
- Ensure all FOUO emails are encrypted
 - CAC card encrypted emails
 - Use the below link to send encrypted FOUO files;
<https://safe.amrdec.army.mil/safe/Welcome.aspx>



Security Incidents or Concerns Continued



- Ensure that all questions concerning the BAA are sent using the proper channels (NIPR, SIPR, etc.)
- Must notify DSS within 24 hour of any security issues! (even for potential incidents). Additionally notify DSS Rep/DARPA security if classified material was inadvertently emailed to DARPA.



Thank You



Agenda



Start	End	Topic	Presenter
08:00	08:10	Intro / Safety / General Security	R. Neidlinger / A. Boyd
08:10	08:30	Programmatics / Program Security	R. Neidlinger / A. Boyd
08:30	08:40	DARPA STO Overview	N. Sandell, STO Director
08:40	09:30	CDMaST Program Overview	J. Galambos, DARPA PM
09:30	9:45	Break	
9:45	10:15	LVC Testbed Overview	L. Nguyen, NAWC TSD
10:15	10:30	Question Submission	
10:30	10:45	Break	
10:45	11:30	Address submitted questions	J. Galambos, DARPA PM
11:30	12:45	Lunch- Unclassified session adjourned	
12:45	13:30	Classified Scenario Briefing	S. Robertson
13:43	14:30	Technology Program Briefings	Drs Patt, Littlefield, Kamp, Haas
14:30	14:45	Break	
14:45	15:30	Technology Program Briefings	Drs Krolik, Wichowski, Sullivan
15:30	15:40	Closing Remarks	J. Galambos, DARPA PM

CDMaST Programmatics Overview

Rick Neidlinger

CDMaST Industry Day Brief

16 November 2015





Program Overview

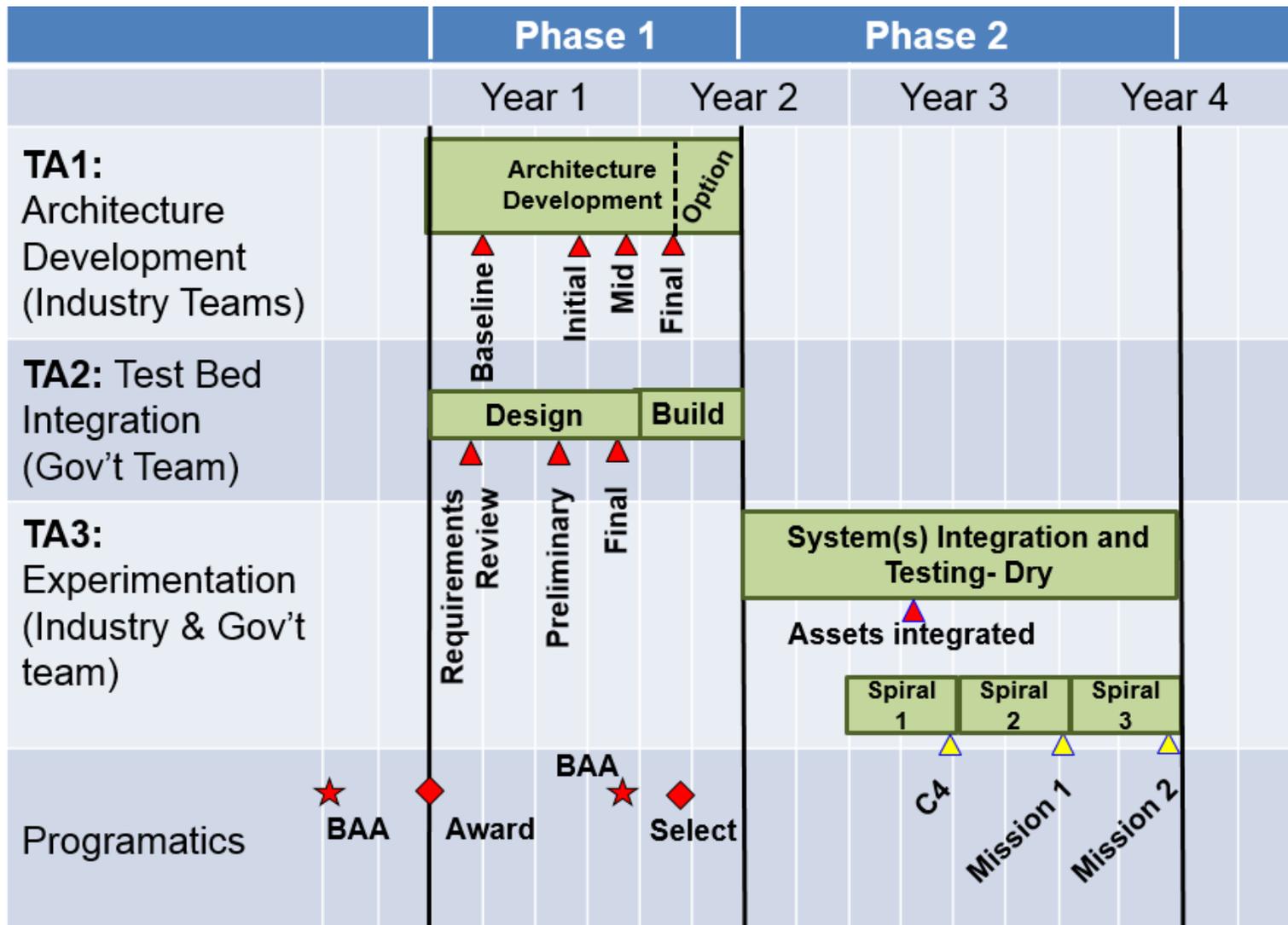


- The Cross Domain Maritime Surveillance and Targeting (CDMaST) program will develop “System of Systems” architectures for wide-area, cross-domain (under, on, and over the sea) surveillance and targeting of adversary ships and submarines in contested environments
- A test/demonstration environment with live/virtual/constructive segments will demonstrate the newly developed integrated “System of Systems” architecture.
- Program is divided into two Phases.
 - **Phase 1:** Develop “System of Systems” architectures which distribute functionality across networks of manned and unmanned platforms, sensors, weapons and mission systems (a 14 month base effort, with a four month option)
 - **Phase 2:** Exercise proposed “System of Systems” architecture using live/virtual/constructive segments, both to reduce technical risk and demonstrate to transition partners. (a 24 month effort, to be awarded under future BAA)

This BAA covers only Phase 1



CDMaST: Program Schedule





PHASE 1

Phase 1, Thrust Area 1

- Industry teams:
 - Baseline Scenario Evaluation
 - Architecture Development
 - Develop Technology Enablers to TRL 4
 - Interact with LVC Testbed team (Government)

Phase 1, Thrust Area 2

- Government team
 - LVC testbed integration

PHASE 2

(Not a part of this BAA)

Phase 2, Thrust Area 3

- Industry team:
 - Architecture Implementation
 - Mature Technology Enablers to TRL 5
 - Experiment/Demonstrate using LVC Testbed and at-sea exercises
- Government team:
 - Coordinate between other Government entities for “live, at-sea” portions of testing

The objective of the program is to define innovative architectures, conduct experiments, and demonstrate effective military capabilities



CDMaST: Award Information



- ***This BAA covers only Phase 1, with up to \$14,000,000 designated for performer teams.***
- ***Phase 1:***
 - Period of performance: 14 months + 4 month option
 - Number of anticipated awards: Up to 3 teams
 - Teaming is encouraged in order to satisfy BAA
 - Partial proposals for contracts will not be awarded.
- ***Phase 2:***
 - Separate BAA will be published for Phase 2 proposals
 - Period of performance: 24 months
 - Number of anticipated awards: Up to 1 team

A superior architecture and proposed integration and experimentation plan is the basis for Phase 2 award



- ***Conceive and model your architecture, then.....***
- ***Use Department of Defense Architecture Framework (DoDAF) version 2.02 to document your architecture***

DoDAF Conformance

“DoD Components are expected to conform to DoDAF to the maximum extent possible in development of architectures within the Department. Conformance ensures that reuse of information, architecture artifacts, models, and viewpoints can be shared with common understanding.

DoDAF conformance is achieved when:

- The data in a described architecture is defined according to the DM2* concepts, associations, and attributes.
- The architectural data is capable of transfer in accordance with the PES*.”

The screenshot shows the official website for the DoDAF Architecture Framework Version 2.02. The header includes the U.S. Department of Defense logo and the title 'CHIEF INFORMATION OFFICER U.S. DEPARTMENT OF DEFENSE'. A search bar is located in the top right. The main navigation menu includes links for HOME, ABOUT DOD CIO, TOP PRIORITIES, IN THE NEWS, OPPORTUNITIES, LIBRARY, and CONTACT US. The central content area features the DoDAF logo and the text 'DoD Architecture Framework Version 2.02 DoD Deputy Chief Information Officer'. A sidebar on the left lists various sections: DODAF Home, Background, Architectural Development, Meta Model (Conceptual, Logical, PES, IDEAS Foundation Ontology), Viewpoints & Models (All Viewpoint, Capability Viewpoint, Data and Information Viewpoint, Operational Viewpoint, Project Viewpoint, Services Viewpoint, Standards Viewpoint, Systems Viewpoint), Models, Model Categories, Levels of Architecture, Architecture Interrogatives, and Architecture Modeling Primitives. The main content area contains a welcome message and a 'DoDAF Conformance' section. The 'DoDAF Conformance' section states: 'DoD Components are expected to conform to DoDAF to the maximum extent possible in development of architectures within the Department. Conformance ensures that reuse of information, architecture artifacts, models, and viewpoints can be shared with common understanding. Conformance is expected in both the classified and unclassified communities, and further guidance will be forthcoming on specific processes and procedures for the classified architecture development efforts in the Department. DoDAF conformance is achieved when:' followed by two bullet points: 'The data in a described architecture is defined according to the DM2 concepts, associations, and attributes.' and 'The architectural data is capable of transfer in accordance with the PES.'

*DM2-DoDAF Meta Model

*PES- Physical Exchange Specification



CDMaST: Proposal Evaluation Criteria



- ***Overall Scientific and Technical Merit:*** Approach is feasible, achievable, complete, supported by a technical team with the requisite expertise
- ***Potential Contribution and Relevance to the DARPA Mission:*** Contributions of the proposed effort are relevant to the national technology base
- ***Proposer's Capabilities and/or Related Experience:*** Proposer's ability to deliver products relevant to CDMaST on schedule and budget
- ***Cost Realism:*** Costs are realistic for the technical and management approaches offered, and demonstrate the proposer understands the effort

***Further details are provided in the BAA
Contracts are awarded based on these criteria***



Agenda



Start	End	Topic	Presenter
08:00	08:10	Intro / Safety / General Security	R. Neidlinger / A. Boyd
08:10	08:30	Programmatics / Program Security	R. Neidlinger / A. Boyd
08:30	08:40	DARPA STO Overview	N. Sandell, STO Director
08:40	09:30	CDMaST Program Overview	J. Galambos, DARPA PM
09:30	9:45	Break	
9:45	10:15	LVC Testbed Overview	L. Nguyen, NAWC TSD
10:15	10:30	Question Submission	
10:30	10:45	Break	
10:45	11:30	Address submitted questions	J. Galambos, DARPA PM
11:30	12:45	Lunch- Unclassified session adjourned	
12:45	13:30	Classified Scenario Briefing	S. Robertson
13:43	14:30	Technology Program Briefings	Drs Patt, Littlefield, Kamp, Haas
14:30	14:45	Break	
14:45	15:30	Technology Program Briefings	Drs Krolik, Wichowski, Sullivan
15:30	15:40	Closing Remarks	J. Galambos, DARPA PM

CDMaST

Program Security Brief

Mark Doody
Program Security Officer
(703) 526-2687

Adam Boyd
Program Security Representative
(703) 812-1985
adam.boyd.ctr@darpa.mil





Program Overview



- Cross Domain Maritime Surveillance and Targeting (CDMaST) program will develop “System of Systems” architectures for wide-area, cross-domain (under, on, and over the sea) surveillance and targeting of adversary ships, and submarines in contested environments
- A test/demonstration environment with live/virtual/constructive segments will demonstrate the newly developed integrated “System of Systems” architecture.
- Program is divided into two Phases.
 - **Phase 1:** Develop “System of Systems” architectures which distribute functionality across networks of manned and unmanned platforms, sensors, weapons and mission systems
 - **Phase 2:** Exercise proposed “System of Systems” architecture using live/virtual/constructive segments, both to reduce technical risk and demonstrate to transition partners.

This BAA covers only Phase 1.



Thrust Area 1 (TA 1)



- ***Phase 1, Thrust Area 1: Architecture Development and Analysis***
 - Develop concepts for future distributed architectures to achieve wide area war-fighting effectiveness in highly contested areas based on Government Furnished Mission scenario
 - Use mission level modeling/simulation/analysis tools to run baseline scenario and advanced concepts to hold adversary ships and submarines at risk.
 - Coordinate with Government Team performing TA 2 (Test bed integration)
 - Submit proposals for Phase 2.
- ***Security for TA 1***
 - Anticipate work at unclassified, collateral SECRET and TOP SECRET, Special Access Program (SAP), and Sensitive Compartment Information (SCI)
 - Expect Contractor Program Security Officer (CPSO) to be heavily involved in the secure execution of TA-1 mission
 - Program Office expectation of extraction of unclassified and collateral data from overall SAP and or SCI product will necessitate a CPSO review of products prior to submission



Applicants Considering Classified Submissions



- Applicants considering classified submissions must ensure that the necessary personnel, facilities, and security infrastructure are in place at the appropriate level
 - Facility Clearance (FCL)
 - Safeguarding level
 - Automated Information System(s) (AIS)
 - Foreign Ownership Control and Influence (FOCI)
 - Additional information on these subjects can be found at: www.dss.mil
 - DARPA expects proposals for TA-1 will be received at the collateral SECRET level
 - If seeking submission of SAP or SCI data governed by another Original Classification Authority (OCA that is not the Director of DARPA), then this MUST be pre-coordinated and approved with the owning service/agency (also notify Program Security Representative (PSR)) .



SECURITY REQUIREMENTS – TA-1



- Anticipate work at unclassified, collateral SECRET and **TOP SECRET**, Special Access Program (SAP), and Sensitive Compartment Information (SCI)
- The Government anticipates that some architecture development and evaluation will occur at the TS//SCI//SAP level.
 - The TS//SCI//SAP work shall be compiled into a separate addendum to enable distribution of some materials at the UNCLASSIFIED and SECRET levels.
- **Performers should have the personnel and facilities necessary to execute their proposed work at those levels.**
- **Note: per the DARPA Security Classification Guide (SCG) 897 CDMaST architectures will be Collateral SECRET unless elements drive to higher levels**
- For TA1, upon contract award performer teams may be required to nominate personnel for access into Special Access Programs.
 - This would entail that personnel have a final TOP SECRET clearance with a Single Scope Background Investigation (SSBI) completed within the last five (5) years in addition to completion of a Special Access Program Personnel Security Pre-screen Questionnaire (SAPNP).
 - For SCI eligibility, applicants must be able to be adjudicated in accordance with appropriate Intelligence Community Guidance (Intelligence Community Directive 704, dtd October 1, 2008)



Security and Proprietary Issues



- The Government anticipates proposals submitted under this BAA will be submitted at the **SECRET level**.
 - Proposers submitting a classified proposal from other classified sources must first receive permission from the respective Original Classification Authority in order to use their information in replying to this BAA. **Applicable classification guide(s) should also be submitted to ensure the proposal is protected at the appropriate classification level.**
- **The Government anticipates that Volume 1 (technical and management proposals) submitted under this BAA will be classified in accordance with DARPA SCG 897** which will be issued along with a Contract Security Classification Specification (DD254) to those companies electing to propose to the BAA.
 - A formal request the Security Classification Guide and a DD254 “DoD Contract Security Classification Specification,” may be submitted by filling out the SCG/DD254 Request Form (found in APPENDIX 2 of the BAA) and emailing the Request Form to DARPA-BAA-16-01@darpa.mil with subject line titled “Request DARPA-BAA-16-01 SCG\DD254.”



Approved Submission Procedures



- Confidential and Secret – See NISPOM (DoD 5220.22-M) for specifics
 - Marked in accordance with DoD Manual 5200.01 Volumes 1-4
 - Hand carrying to DARPA
 - Mailing via USPS Registered® or Express® Mail
- Top Secret – See NISPOM (DoD 5220.22-M) for specifics
 - Marked in accordance with DoD Manual 5200.01 Volumes 1-4
 - Must be hand carried to DARPA
- SAP
 - Must pre-coordinate with DARPA Strategic Technology Office PSO/PSR
 - 703.812.1985 (PSR) or
 - 703.526.2687 (PSO)
- SCI
 - Must pre-coordinate with DARPA Strategic Technology Office PSO/PSR
 - 703.812.1985 (PSR) or
 - 703.526.2687 (PSO)
- Proprietary Data
 - It is the Proposer's responsibility to clearly define to the Government what is considered proprietary data.



Sending Classified Proposals



- Proposal packages are due **12 JAN 2016**.
- Please forward properly wrapped and marked SECRET package to:
- Inner envelope shall be addressed to:
 - Defense Advanced Research Projects Agency
 - ATTN: STO, Dr. James Galambos
 - PSR, Adam Boyd
 - Reference: DARPA-BAA-16-01
 - 675 North Randolph Street
 - Arlington, VA 22203-2114
- Outer envelope shall be sealed with no identification as to the classification of its contents and addressed to:
 - Defense Advanced Research Projects Agency
 - Security & Intelligence Directorate, Attn: CDR
 - 675 North Randolph Street
 - Arlington, VA 22203-2114



Security and Proprietary Issues (continued)



- Proposers must have **existing and in-place prior to execution of an award, approved capabilities (personnel and facilities)** to perform research and development at the classification level they propose.
- It is the policy of DARPA to treat all proposals as competitive information, and to disclose their contents only for the purpose of evaluation. **Proposals will not be returned.**



Evaluation Criteria



- The proposer will describe their security approach to protecting the technical objectives, internal security practices, and internal contracting practices to support their proposal.
 - Relevant security disciplines include but are not limited to:
 - Operations Security (OPSEC), SAP security, SCI security Personnel Security, Physical Security, Test and Transportation Security, Program Security, and Information/Cyber Security.
- The proposal provides details on the adequacy and depth of security handling procedures and staff to administer security activities **of all proposed and anticipated team members including subcontractors, vendor purchase strategies, and potential consultants.**
- The proposal must convey the proposer's adequacy, availability, and commitment of cleared personnel, required facilities, Automated Information Systems (AIS), and communications to support the program in a timely and acceptable level at the appropriate level of classification upon potential contract award.
 - **The proposal shall provide a security architecture chart that adequately depicts all relationships of subcontractors as it relates to overall program acquisition strategy.**



Security Overview



- Unauthorized disclosure of SECRET Classified Information could be expected to cause serious damage to national security that the original classification authority is able to identify or describe.
- **Defense Security Service (DSS) is the Cognizant Security Office for Collateral Program Spaces and Automated Information Systems (AIS).**
- The DoD 5220.22-M National Industrial Security Program Operating Manual (NISPOM) is the guide in which each performer will be required to adhere to with regards to protection of program information (safeguarding), facilities, and AIS.
- DARPA is the approval authority for actions involving TS//SAP//SCI Testing (DSS has cognizance over Collateral SECRET testing only), Public Release, Contracting, etc...



Security Overview – SAP/SCI



- Unauthorized disclosure of Special Access Program (SAP) or Sensitive Compartmented Information (SCI) data could be expected to cause loss of strategic advantage for U.S. military systems or intelligence assets
- **DARPA is the Cognizant Security Office for Special Access Program Spaces and Automated Information Systems (AIS)**
- **Defense Intelligence Agency (DIA) is the Cognizant Security Office for Sensitive Compartmented Information Facilities (SCIFs) and AIS**
- Revision 1 of the DoD Overprint to the NISPOM Supplement (dtd April 1, 2004) is the DARPA SAP security guidebook
- DARPA follows the ICD 705 standard for physical security of both SAPFs and SCIFS
- A CD is provided with your package that includes relevant templates and policy applicable to security at all levels in support of DARPA programs



Security Incidents or Concerns



- When reproducing, transmitting or conducting classified work, ensure that it occurs on DSS approved systems for collateral and appropriately cleared systems for FOUO or Unclassified.
- Be aware of the classification level of your material when processing. Data spills occur frequently and will impact a programs ability to continue to work while clean-up operations are on-going.
- Be aware of the classification level when having discussions and ensure to set the level of the room.
- Ensure all FOUO emails are encrypted
 - CAC card encrypted emails
 - Use the below link to send encrypted FOUO files;

<https://safe.amrdec.army.mil/safe/Welcome.aspx>



Security Incidents or Concerns Continued



- Ensure that all questions concerning the BAA are sent using the proper channels (NIPR, SIPR, etc.)
- In the event of a security incident ensure that your organization notifies DSS within 24 hour of any security issues! (even for potential incidents). Additionally notify DARPA security if classified material was inadvertently emailed to DARPA PSO/PSR and resides on our unclassified systems.
- SAP/SCI security incidents must be reported to your cognizant security authority (CSA) and the DARPA PSO as applicable
 - After contract award all security incidents regarding the CDMaST effort must be reported to the DARPA/STO PSO



DARPA Key Security References



- Executive Order 13526, “Classified National Security Information”
 - December 29, 2009
- DARPA Security Classification Guide 897 – CDMaST
- National Industrial Security Program Operating Manual (NISPOM)
 - DoD Manual 5220.22-M incorporating change 1, dtd March 28, 2013
- Information Assurance Workforce Program Improvement
 - DoD Manual 8570.01-M incorporating change 3, dtd January 24, 2012
- DoD Information Security Program: Overview, Classification, and Declassification
 - DoD Manual 5200.01 Volumes 1-4 incorporating change 1, dtd March 21, 2012
- Distribution Statements on Technical Documents
 - DoD Directive 5230.24, dtd August 13, 2012
- Freedom of Information Act (FOIA) Program
 - DoD 5400.7-R, September 4, 1998, (Incorporating Change 1, April 11, 2006).
- Withholding of Unclassified Technical Data from Public Disclosure
 - DoD Directive 5230.25, dtd November 6, 1984, (Incorporating Change 1, August 18, 1995).



DARPA Key Security References – SAP/SCI



- SAP Security Oversight
 - In accordance with DoD Overprint to the NISPOM Supplement Revision 1, dtd April 1, 2004
- SAP Personnel Security Eligibility
 - In accordance with USD Memorandum – “Special Access Nomination Process”, dtd May 20, 2013
 - DARPA SAPCO Memorandum – “New Special Access Program (SAP) Nomination Process (SAP NP), dtd August 29, 2013
- SCI Eligibility
 - In accordance with Intelligence Community Directive (ICD) 704, dtd October 1, 2008
- SAP/SCI Physical Security
 - In accordance with Intelligence Community Directive (ICD) 705
 - Intelligence Community Standards 705-1 and 705-2
 - Technical Specifications for Construction and Management of SCIFs, dtd April 23, 2012
 - SCIF accreditations/co-utilization requests must be coordinated through the Defense Intelligence Agency (DIA); plan accordingly



DARPA Key Security References – SAP/SCI (continued)



- SAP Information Assurance
 - In accordance with “Joint Special Access Program (SAP) Implementation Guide”, dtd October 9, 2013
 - National Institute of Standards and Technology (NIST) Special Publication 800-37 Revision 1, “Guide for Applying the Risk Management Framework to Federal Information Systems”, dtd February 2010
- SCI Information Assurance
 - In accordance with “Department of Defense Intelligence Information System (DoDIIS) – Joint Security Implementation Guide (DJSIG)”, dtd August 2011
- Operations Security (OPSEC)
 - In accordance with DoD 5205.02-M – “DoD Operations Security (OPSEC) Program Manual”, dtd November 3, 2008



Agenda



Start	End	Topic	Presenter
08:00	08:10	Intro / Safety / General Security	R. Neidlinger / A. Boyd
08:10	08:30	Programmatics / Program Security	R. Neidlinger / A. Boyd
08:30	08:40	DARPA STO Overview	N. Sandell, STO Director
08:40	09:30	CDMaST Program Overview	J. Galambos, DARPA PM
09:30	9:45	Break	
9:45	10:15	LVC Testbed Overview	L. Nguyen, NAWC TSD
10:15	10:30	Question Submission	
10:30	10:45	Break	
10:45	11:30	Address submitted questions	J. Galambos, DARPA PM
11:30	12:45	Lunch- Unclassified session adjourned	
12:45	13:30	Classified Scenario Briefing	S. Robertson
13:43	14:30	Technology Program Briefings	Drs Patt, Littlefield, Kamp, Haas
14:30	14:45	Break	
14:45	15:30	Technology Program Briefings	Drs Krolik, Wichowski, Sullivan
15:30	15:40	Closing Remarks	J. Galambos, DARPA PM

DARPA Strategic Technology Office Contested Environment Strategy and Plans

Dr. Nils Sandell, STO Director

16 November 2015



Distribution Statement "A" (Approved for Public Release, Distribution Unlimited)



Strategic Technology Office (STO) Contested Environment Thrust



STO Systems and Technologies: Core Competencies

- Battle Management/Command and Control (BMC2)
- Communications (C)
- Intelligence, Surveillance and Reconnaissance (ISR)
- Electronic Warfare (EW)
- Positioning, Navigation and Timing (PNT)
- System-of-Systems Integration

STO Contested Environment Thrust: Focus Areas

- Air Dominance against Peer Threat
- Undersea Dominance against Peer Threat
- Spectrum Dominance against Peer Threat

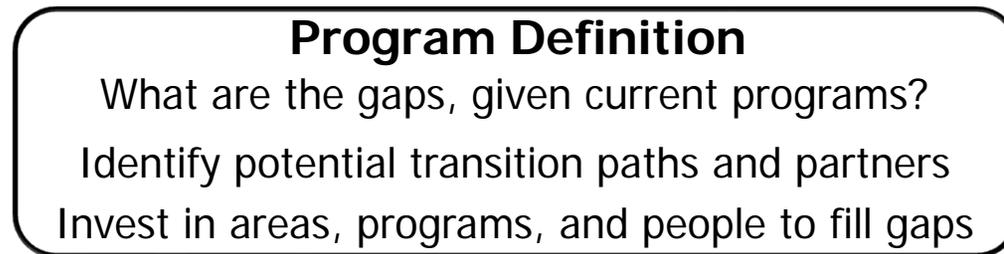
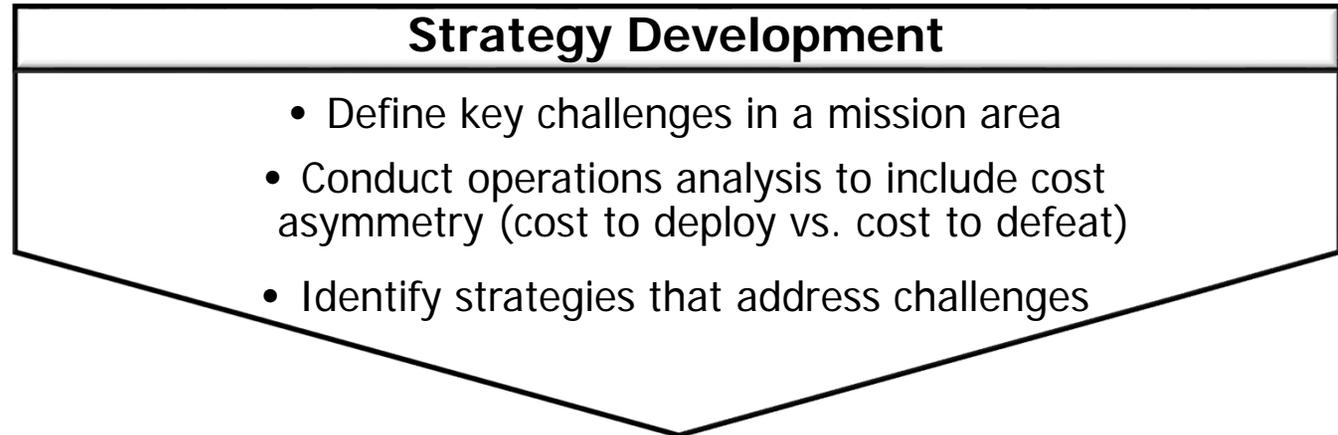
***Fighting as a Network to Increase
Military Effectiveness, Cost Leverage, and Adaptability***



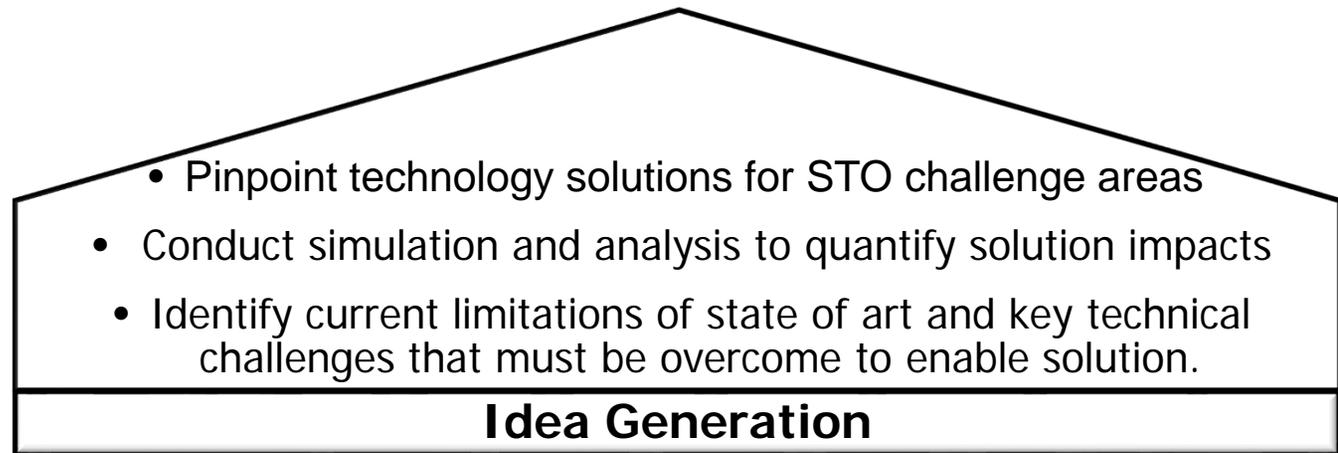
Program Definition Combines Strategy Development (Top Down) with Idea Generation (Bottom Up)



- National, Defense Strategies
- COCOM, Service Needs
- DARPA Investment Themes
- AEO, Liaison Staff, Special Assistant Input, ADI



- DSO, I2O, MTO, TTO
- Universities
- Industry
- Government Labs and FFRDCs





Contested Environment Thrust Goals and Potential Approaches



- Goals: Technologies to Help Enable
 - Air, Undersea and Spectral Dominance* Against Peer Threat
 - Agile Insertion of New Technology
 - Positive Cost Leverage
- Potential Approaches
 - Networking of Low Cost Autonomous Platforms with Manned Platforms
 - Electronic Warfare and Electronic Counter-Counter Measures
 - Electro-Optical (EO) Systems
 - Agile, Jam-Resistant Sensing and Navigation
 - Low Probability of Detection/Anti-Jam Communications
 - Distributed, Deep Ocean Active and Passive Sonar
 - Underwater Operations

*Dominance limited in time and space



Contested Environment Challenges and Strategies – System of Systems



- System of Systems Challenges:
 - Increasing costs and schedule to develop major defense systems with decreasing defense budgets
 - Need systems that cost more to defeat than to deploy
 - Long schedules result in obsolete technology
 - Traditional top down systems engineering failing for system-of-systems: no one is in-charge and too complicated anyway
- System of System Strategies:
 - Leverage commercial components and development processes
 - Development process schedule- and not requirements-driven
 - Use government-owned reference implementations
 - Use simpler, disaggregated, heterogeneous platforms that achieve desired effects by coordinated action
 - Build on successful models (Internet, Microsoft driver development process) to develop system-of-systems integration technology
 - Dual-purpose demonstrations: demonstrate system-of-systems operational capability and the process for developing it



Agenda



Start	End	Topic	Presenter
08:00	08:10	Intro / Safety / General Security	R. Neidlinger / A. Boyd
08:10	08:30	Programmatics / Program Security	R. Neidlinger / A. Boyd
08:30	08:40	DARPA STO Overview	N. Sandell, STO Director
08:40	09:30	CDMaST Program Overview	J. Galambos, DARPA PM
09:30	9:45	Break	
9:45	10:15	LVC Testbed Overview	L. Nguyen, NAWC TSD
10:15	10:30	Question Submission	
10:30	10:45	Break	
10:45	11:30	Address submitted questions	J. Galambos, DARPA PM
11:30	12:45	Lunch- Unclassified session adjourned	
12:45	13:30	Classified Scenario Briefing	S. Robertson
13:43	14:30	Technology Program Briefings	Drs Patt, Littlefield, Kamp, Haas
14:30	14:45	Break	
14:45	15:30	Technology Program Briefings	Drs Krolik, Wichowski, Sullivan
15:30	15:40	Closing Remarks	J. Galambos, DARPA PM

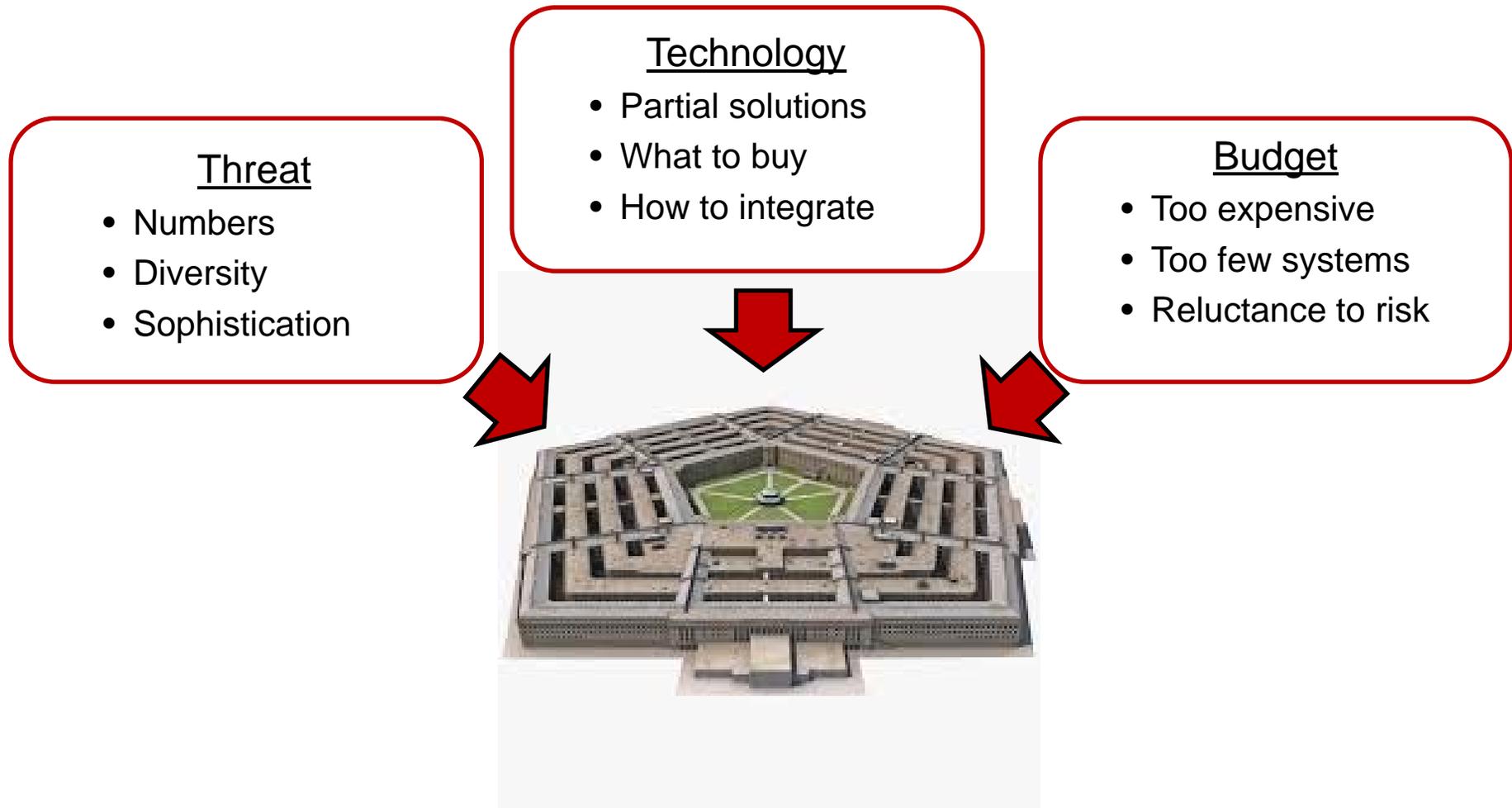
Cross Domain Maritime Surveillance and Targeting (CDMaST) Program Overview

Dr. Jim Galambos

CDMaST Industry Day Brief

16 November 2015





Program born as a new System of Systems approach to impose cost and rapidly, affordably apply technology to address evolving threats

THINK

BIG!



Peer Contested Maritime Environments

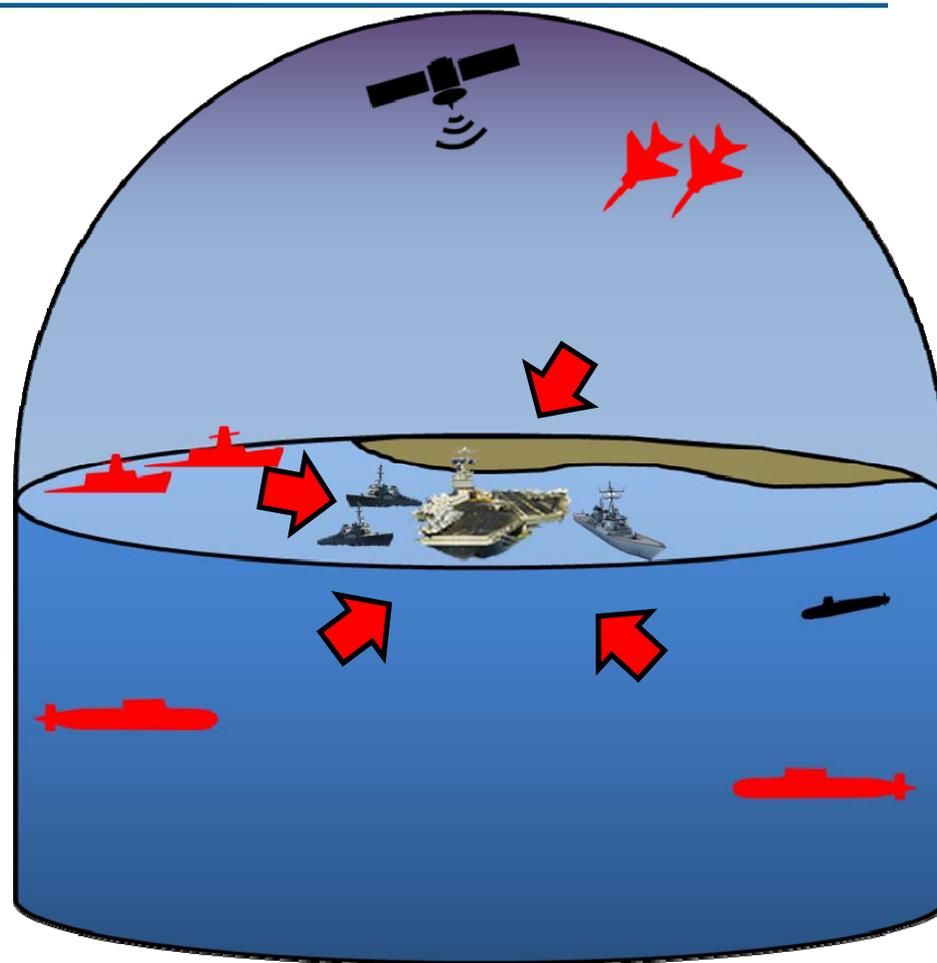


Today

- Operate far forward in vast operating areas
- Missions heavily based on carriers
- High value units concentrated for mutual defense
- Targeted from variety of sources with links to multiple platforms with long range weapons

Issues

- Adversaries have significant cost advantage engaging HVU
- Defensive posture
- Poor coordination with undersea
- Finite magazine



We want to go on offense and impose asymmetry on adversary



CDMaST: Approach

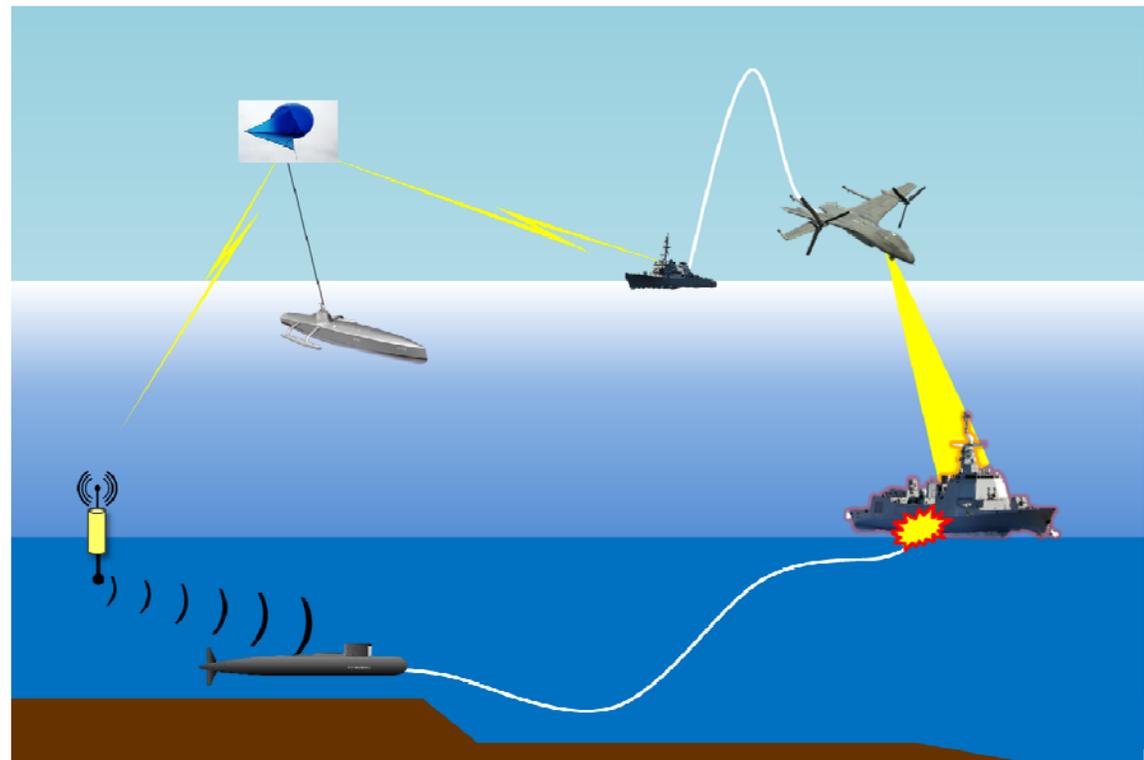


Hypothesis: Combining distributed manned and unmanned systems and exploiting all domains we can:

- Deliver much greater military effectiveness at lower cost
- Impose greater cost on the adversary to counter than for us to field

Attributes

- Wide Area
- Disaggregated
- Cross-Domain
- Adaptable
- Resilient



Hold adversary ships and submarines at risk over ~1,000,000 km²



CDMaST System of Systems

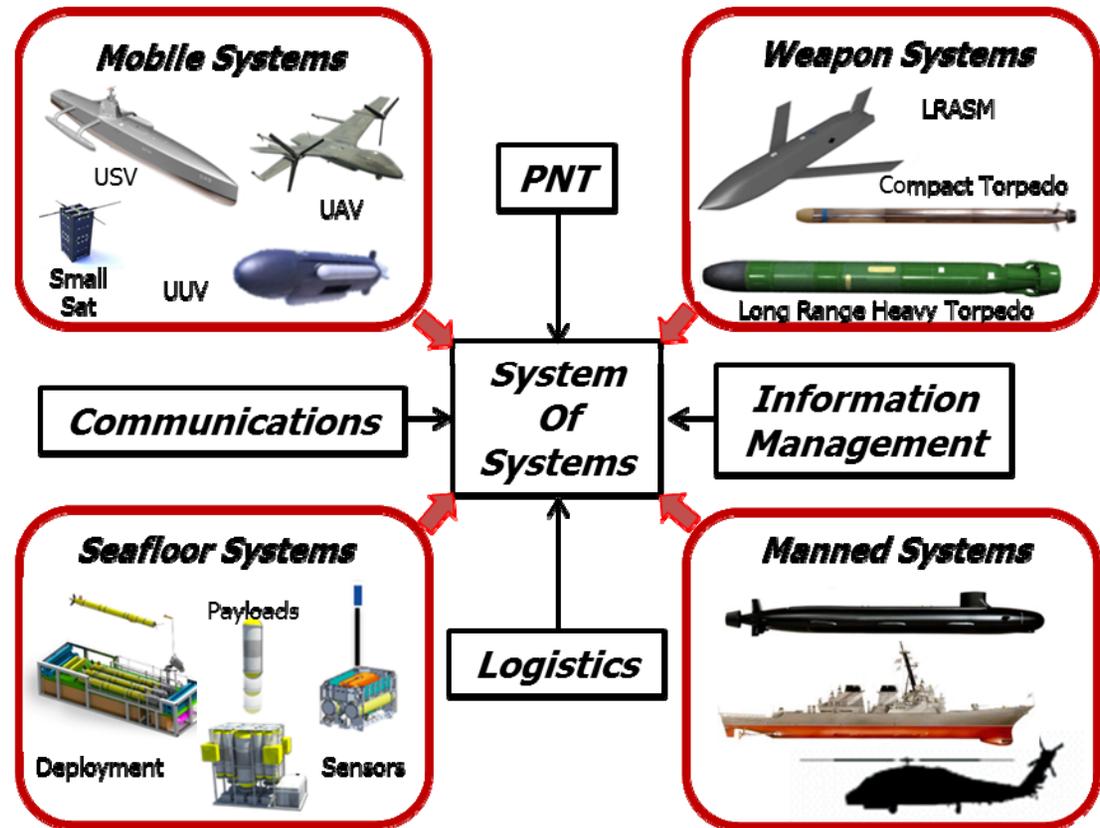


Applications

- Weapon systems
- Unmanned mobile systems
- Unattended fixed systems
- Manned systems

Services

- Communications
- Energy (power)
- Information management
- Position, navigation and timing

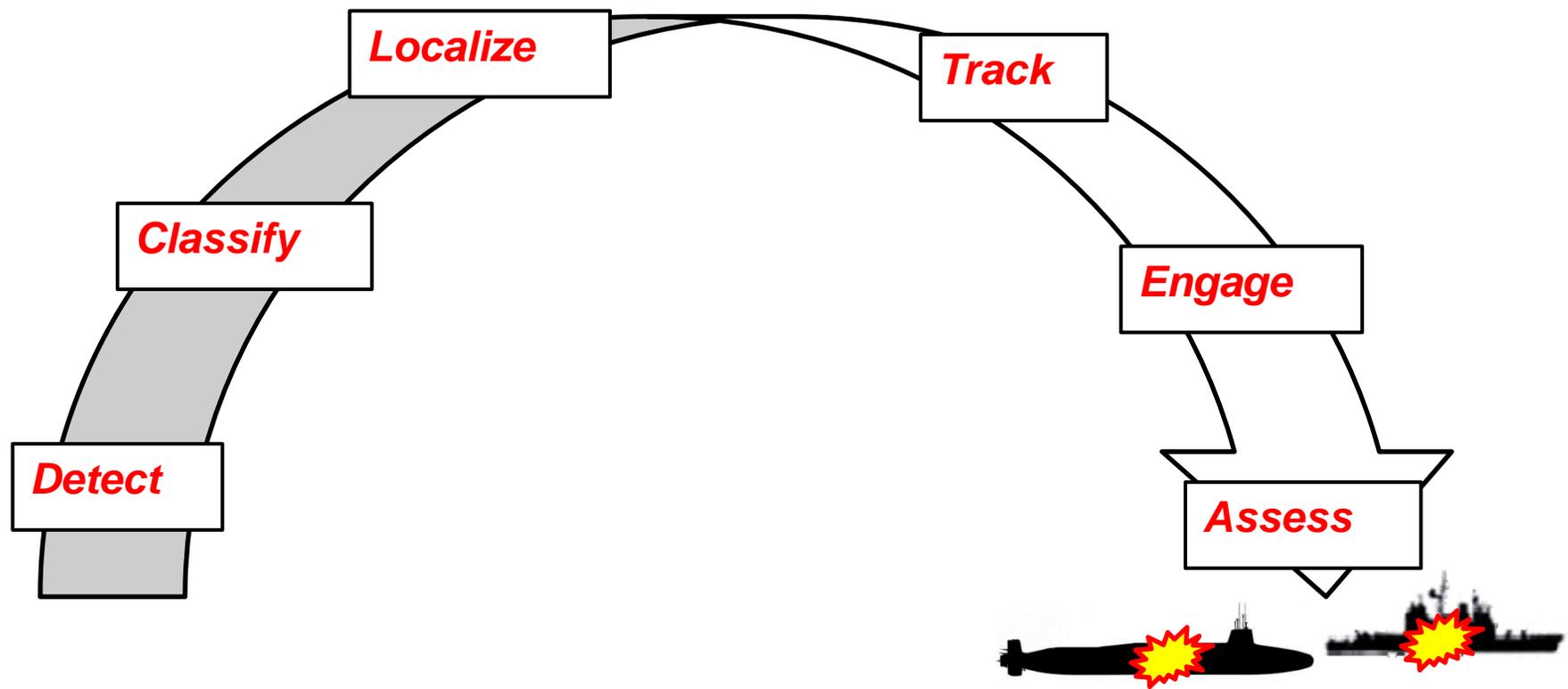


USV Unmanned Surface Vehicle
 UAV Unmanned Aerial Vehicle
 UUV Unmanned Undersea Vehicle
 PNT Position, Navigation, and Timing
 LRASM Long-Range Anti-Ship Missile

Successful architectures must be effective, affordable, deployable, sustainable, and adaptable



CDMaST Mission Elements



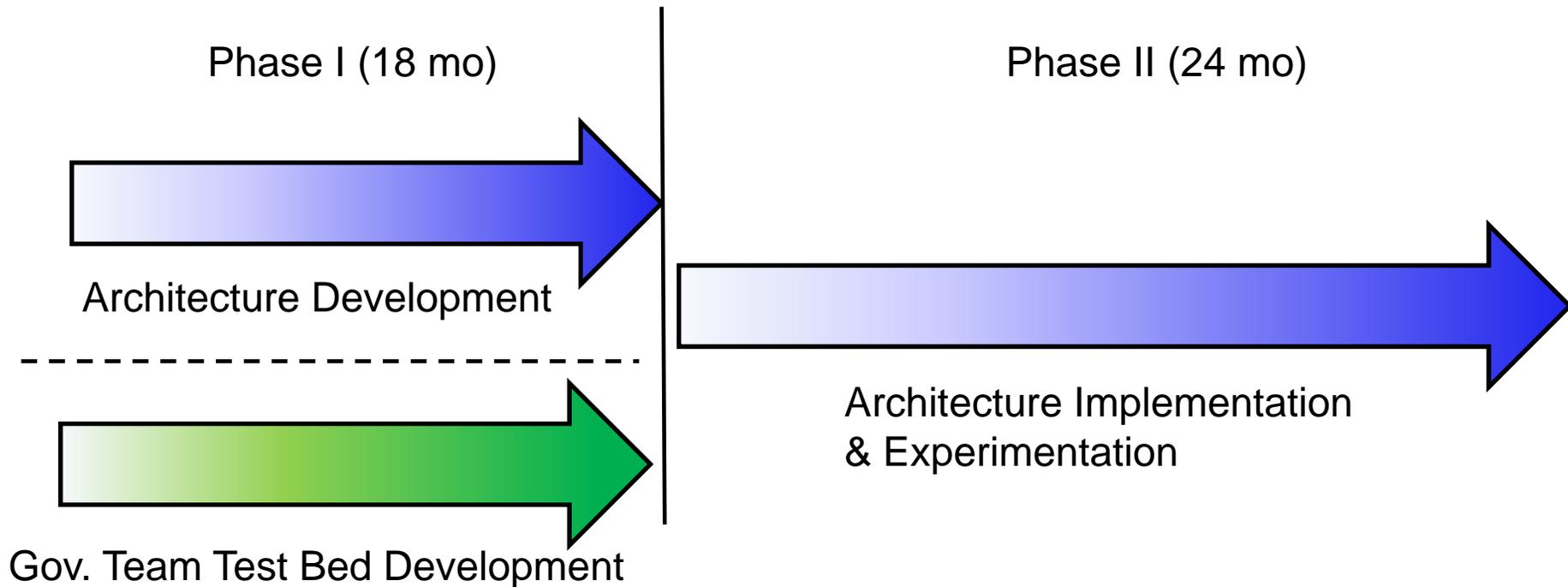
Architecture solutions must address all elements of kill chain



CDMaST: Program Information



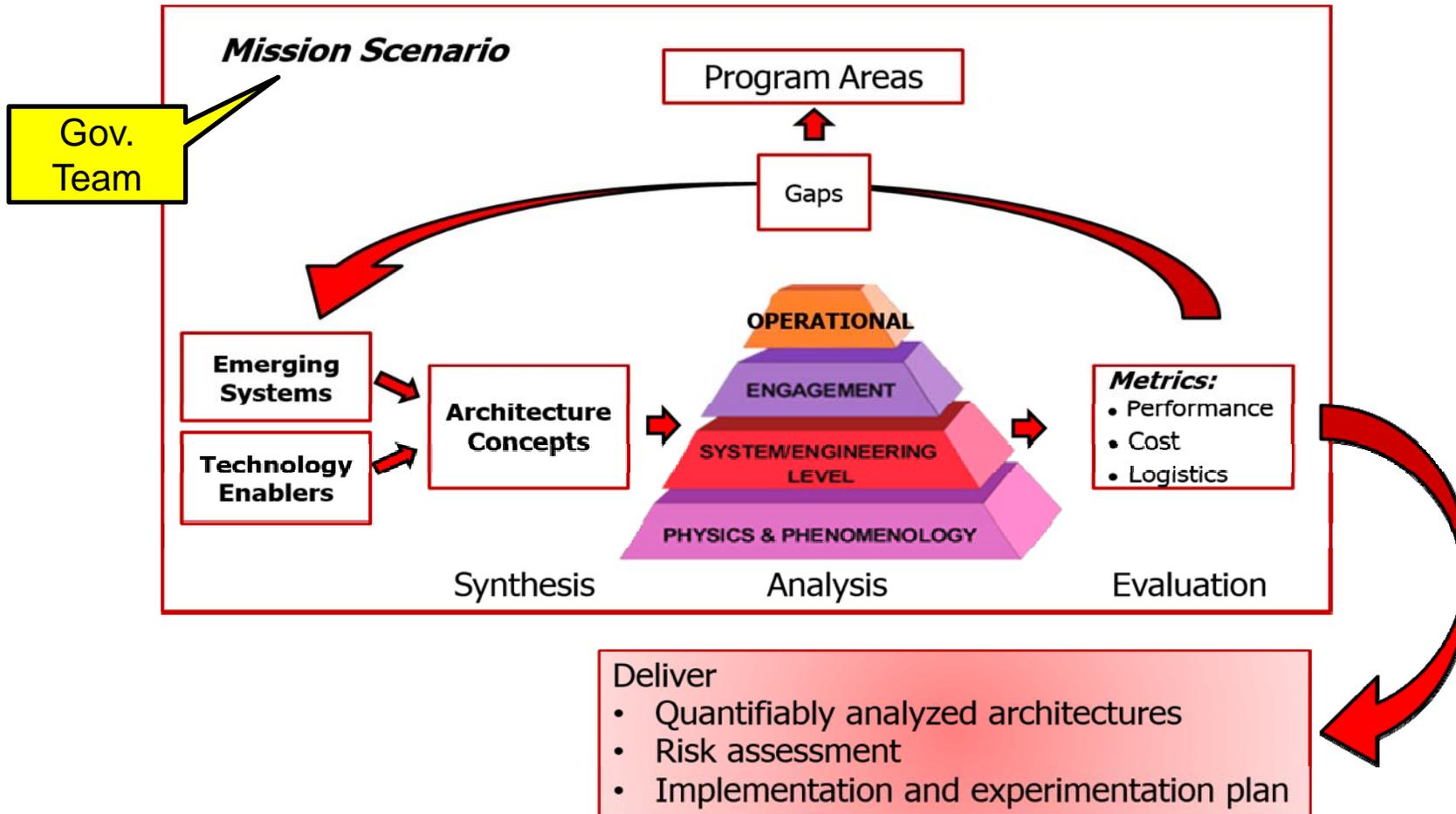
The CDMaST program will develop and demonstrate “System of Systems” architectures for wide-area, cross-domain (under, on, and over the sea) surveillance and targeting of adversary ships, and submarines in contested environments



Deliver analyzed, documented, and tested architecture solutions



Phase I: CDMaST Architecture Development Process



Analysis and modelling leads directly into plan and proposal for implementation and experimentation in Phase II



- ***Military Effectiveness:***

- Area Domination: Number of square miles where a Probability of Kill (Pk) greater than 0.9 has been achieved, divided by the cost to field the Proposer's SoS architecture
- Probability of Survivability: Personnel, manned and unmanned systems, sensors, and communication links. Greater weight will be applied to preservation of manned assets.
- Promptness: Time required to achieve "Area Domination" and time to eliminate all adversarial targets from area.

- ***Cost:***

- System Cost: Deploy (procure, field) and sustain (operate, maintain) SoS architecture
- Cost Imposition: SoS architecture cost vs. Cost to adversary due to SoS architecture.

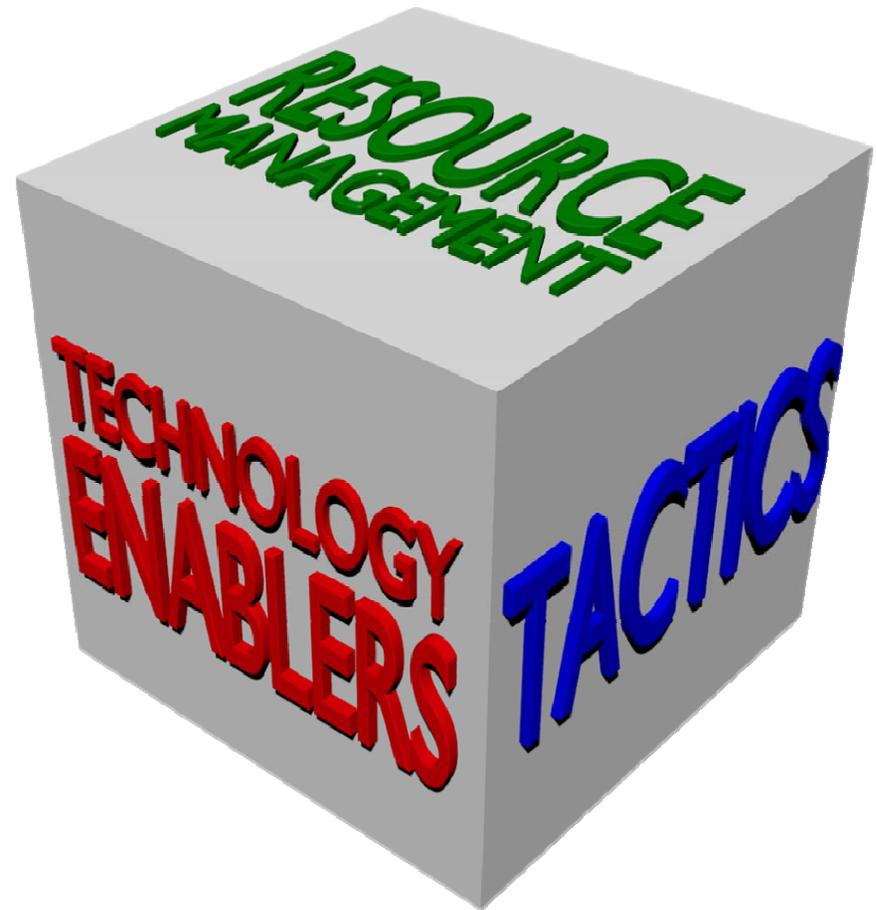
Hold ships and subs at risk over wide areas while minimizing own cost and risk while driving up adversary cost



Innovation opportunities



- Technology Innovation
- Tactics Innovation
- Resource management innovation



More than just technology...SoS involves combining clever manipulation of resources along with innovative tactics to win the day



CDMaST: Technology Enablers Examples

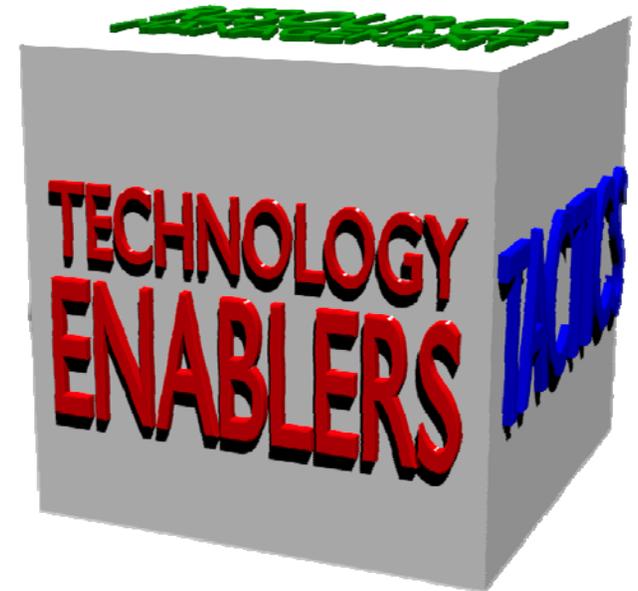


Sensor-platform innovation opportunities

- Platforms...UxVs, Kites, balloons, small satellites, etc.
- Sensors...RF, Acoustic, passive, active, non-acoustic, lasers, etc.

Services innovation opportunities

- Communications...modems, waveforms, LED's, etc.
- Data networking...distributed battle management, Self-forming ad-hoc undersea networks, data fusion
- Deployment/sustainment...docking stations, energy harvesting, snorkeling, etc.
- PNT...off-board systems, clocks, algorithms



Not developing new...but looking for innovative use of technologies and systems to be combined, re-purposed, and packaged in effective SoS



Sensor platform innovation opportunities

- Platforms
 - Cross-domain fixed – mobile collaboration for 3rd party targeting
 - Positioning in all domains to optimize performance
- Sensing and targeting
 - Environmental monitoring and dynamic planning
 - Active and multi-static sensing

Services innovation opportunities

- Communications and networking
 - Unmanned comms relays
 - Rapid deployment
 - Data mules
- Deployment/sustainment and PNT
 - Autonomous replenishment...fixed/mobile
 - Pre-positioned systems
 - Collaborative navigation using follower - leader



Seeking innovative operational concepts that trade basic characteristics (speed, cost, energy, range, risk,...etc.) to optimize performance



CDMaST: Resource Management



- Complex analysis environment
 - Sensor performance
 - Platform positions
 - Balance communications, energy, data, navigation
 - Changing environment
 - Equipment failures
- Exploit
 - Motion
 - Temporal history
 - Domain characteristics
 - Collaborative behaviors
 - Planning and dynamic re-allocation



Must go beyond single vehicle autonomy and incorporate collaborative system behavior to optimize performance and minimize cost



Seedling Example: UUV Submarine Search

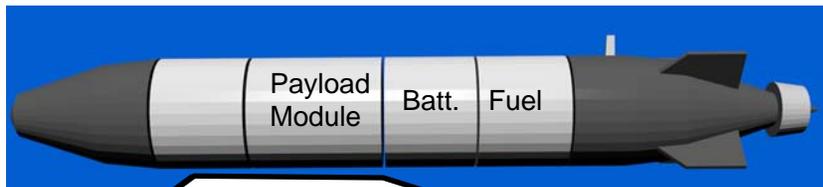


Mission:

- Self deploy and transit 800 nm
- Search and track all subs in op area 1,000,000 km² using UUVs
- Sustain for months

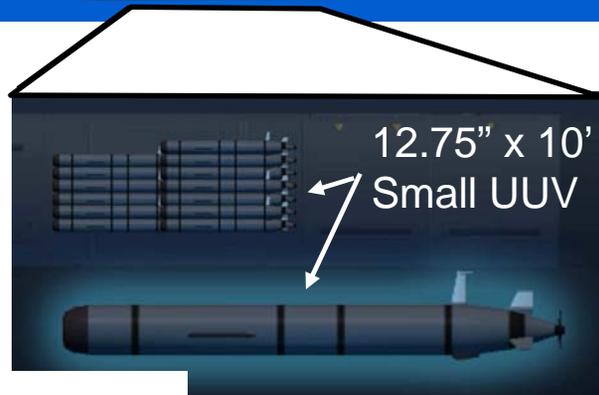
Approach

- Employ large UUVs to deploy and sustain small UUV sensing/communication nodes
- Passive sensors with nominal 2km detect



Technology Enablers

- Hybrid electric/diesel energy source
- Autonomous deploy and mobile recharge
- Collaborative mission autonomy





Seedling Results: Sustainment



Available Resources:

- Small UUVs (12.75" diam x 14 ft)
- Large Modular UUVs (12' diam x 85')

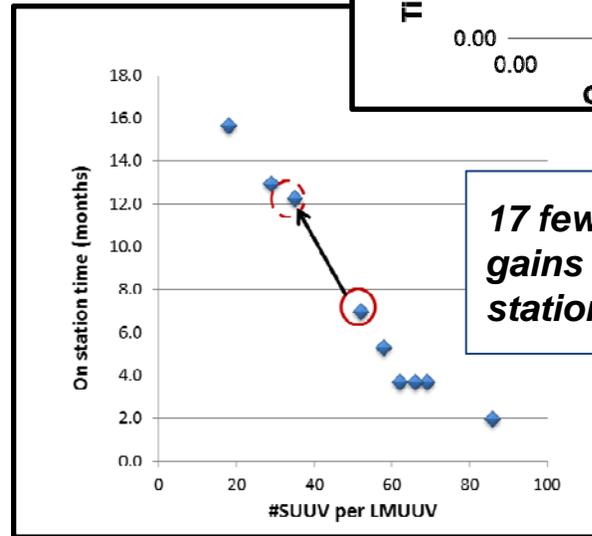
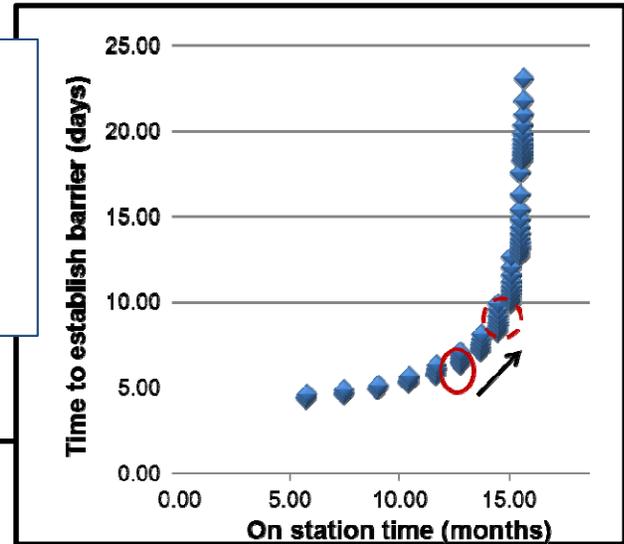
Trade variables

- Speed (transit/search)
- Vehicle size
- Ratio of small to large

Metrics

- Time to clear area and establish barrier
- Endurance
- Number of vehicles

28 days on station gained by slowing transit speed by 1 kt at the cost of 16.5 extra hours



17 fewer SUUV/LMUUV gains 5 months of on station time

Months on station feasible via snorkeling and combining small and large UUVs





Seedling Results (Con't)



• Resource allocation

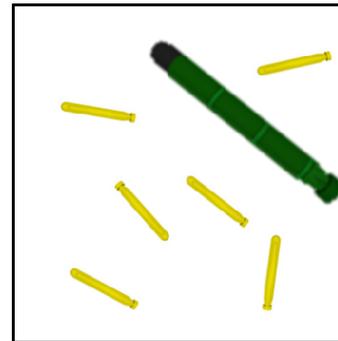
- “Brute force” cover entire area
- Expanding perimeter

• Trades

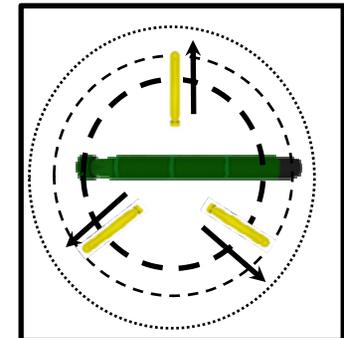
- Time required to initially clear area
- Number of assets required to clear area
- Total fiscal expense for acquisition and fielding system

• Issues

- Brittle...Resilience to failure
- Ability to react to intruder



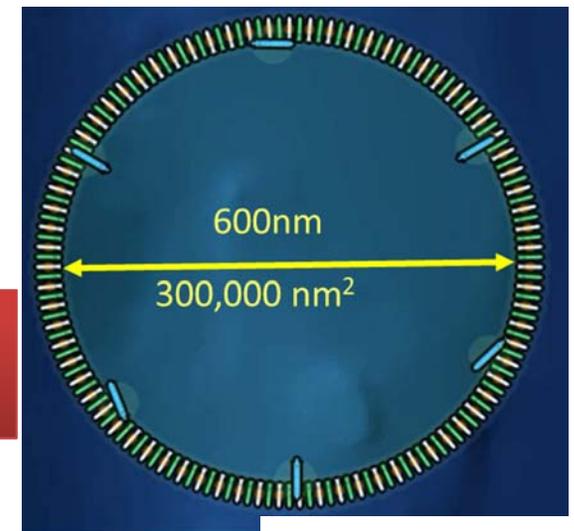
Random 'brute force' fill the area ~>2000 SUUVs



Expanding search



Expanding perimeter <500 SUUVs



SONALYSTS

Assets required reduced by factor of 4 through intelligent search tactics





General BAA Comments



Cross domain System of Systems Test Bed



Approach: Use architectures to drive design and leverage existing simulation capabilities

- Government led warfare center team
- Develop initial test bed concept, ready for kick-off with selected TA1 performers
- Gov team will interact with TA1 performers to understand architectures and develop Interface Control Documents (ICD)s
- Hold Design Reviews with TA1 Performers to ensure understanding of the test bed.

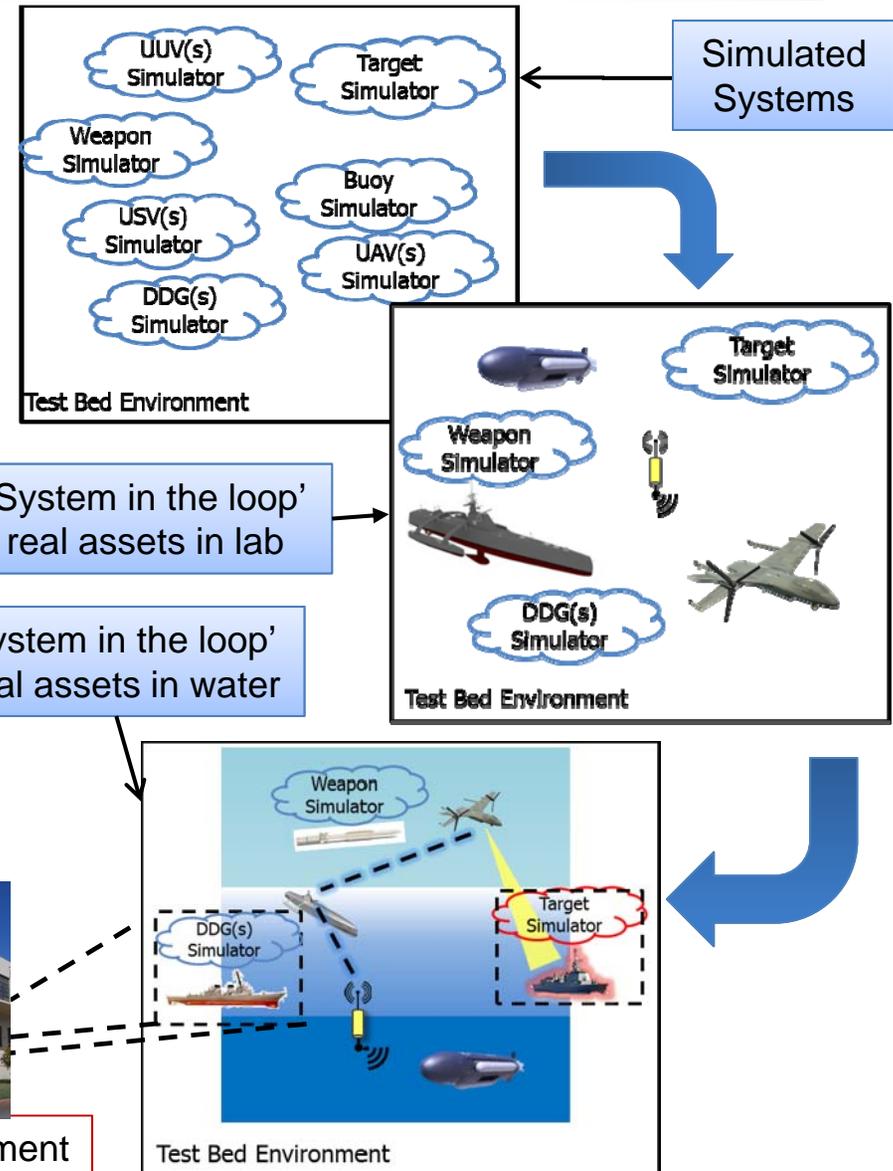
Provide:

- Final test bed design and ICDs to Phase 2 bidders
- Tested environment for Phase 2 LVC

Live: Human Operator controlling physical hardware
Virtual: Human Operator controlling simulated hardware
Constructive: Simulated Operator controlling simulated hardware



Simulation Environment





SoS approach has risks the CDMaST program will address

- Architecture Development and Analysis
 - Architecture too complex to work reliably in combat
 - Architecture too dependent on fragile communications links
 - Platforms design for low cost turn out to be costly
 - Level of autonomy needed is beyond state-of-art
 - Low cost platforms lack reach/persistence to be effective in contested environments
 - Low cost platforms lack size/weight/power to carry necessary mission systems
- Integration Technology Development
 - SoS integration costly and slow
 - Platforms and subsystems from different contractors are incompatible
- Adoption
 - Services buy and Congress allocates budgets for platforms - not Systems of Systems



CDMaST: Scientific/Technical Ingredients for Proposers



Industry team proposals should incorporate the following:

- Knowledge of the problem: Risk should be recognized and technical solutions should be physics based and incorporate realistic CONOPs
- Innovative combinations and components to construct new System of Systems architectures
- Innovative tactics to exploit opportunities created by System of Systems architectures
- Methods for efficient and innovative resource allocation
- Maturity in systems hardware/software integration (for Phase 2 performance)



Document these Industry team capabilities in your proposal:

- Modeling and simulation analysis capability, from physical level to engineering to mission level operations over large areas to include
 - Military effectiveness
 - Communications
 - Information management (command & control, networking, information assurance)
 - Position, timing, and navigation
 - Deployment and sustainment
- Ability to estimate system costs and conduct “Red Team” analysis to estimate cost imposition on adversary
- Expertise in systems engineering and the Department of Defense Architecture Framework (DoDAF) version 2.02
- Ability to implement multi-element architecture concepts and conduct experimentation in phase II program
- Experience in Live/Virtual/Constructive (LVC) Training, Test and Evaluation



Agenda



Start	End	Topic	Presenter
08:00	08:10	Intro / Safety / General Security	R. Neidlinger / A. Boyd
08:10	08:30	Programmatics / Program Security	R. Neidlinger / A. Boyd
08:30	08:40	DARPA STO Overview	N. Sandell, STO Director
08:40	09:30	CDMaST Program Overview	J. Galambos, DARPA PM
09:30	9:45	Break	
9:45	10:15	LVC Testbed Overview	L. Nguyen, NAWC TSD
10:15	10:30	Question Submission	
10:30	10:45	Break	
10:45	11:30	Address submitted questions	J. Galambos, DARPA PM
11:30	12:45	Lunch- Unclassified session adjourned	
12:45	13:30	Classified Scenario Briefing	S. Robertson
13:43	14:30	Technology Program Briefings	Drs Patt, Littlefield, Kamp, Haas
14:30	14:45	Break	
14:45	15:30	Technology Program Briefings	Drs Krolik, Wichowski, Sullivan
15:30	15:40	Closing Remarks	J. Galambos, DARPA PM



Agenda



Start	End	Topic	Presenter
08:00	08:10	Intro / Safety / General Security	R. Neidlinger / A. Boyd
08:10	08:30	Programmatics / Program Security	R. Neidlinger / A. Boyd
08:30	08:40	DARPA STO Overview	N. Sandell, STO Director
08:40	09:30	CDMaST Program Overview	J. Galambos, DARPA PM
09:30	9:45	Break	
9:45	10:15	LVC Testbed Overview	L. Nguyen, NAWC TSD
10:15	10:30	Question Submission	
10:30	10:45	Break	
10:45	11:30	Address submitted questions	J. Galambos, DARPA PM
11:30	12:45	Lunch- Unclassified session adjourned	
12:45	13:30	Classified Scenario Briefing	S. Robertson
13:43	14:30	Technology Program Briefings	Drs Patt, Littlefield, Kamp, Haas
14:30	14:45	Break	
14:45	15:30	Technology Program Briefings	Drs Krolik, Wichowski, Sullivan
15:30	15:40	Closing Remarks	J. Galambos, DARPA PM

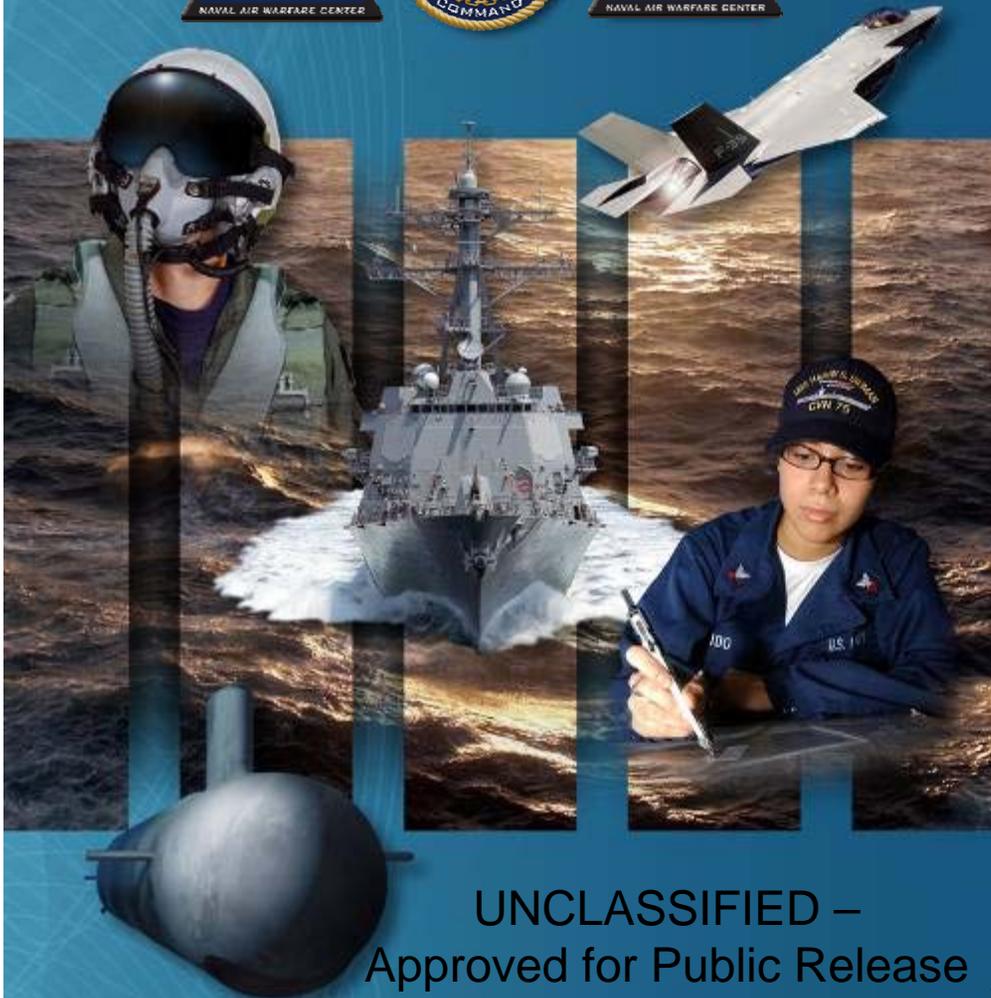


Agenda



Start	End	Topic	Presenter
08:00	08:10	Intro / Safety / General Security	R. Neidlinger / A. Boyd
08:10	08:30	Programmatics / Program Security	R. Neidlinger / A. Boyd
08:30	08:40	DARPA STO Overview	N. Sandell, STO Director
08:40	09:30	CDMaST Program Overview	J. Galambos, DARPA PM
09:30	9:45	Break	
9:45	10:15	LVC Testbed Overview	L. Nguyen, NAWC TSD
10:15	10:30	Question Submission	
10:30	10:45	Break	
10:45	11:30	Address submitted questions	J. Galambos, DARPA PM
11:30	12:45	Lunch- Unclassified session adjourned	
12:45	13:30	Classified Scenario Briefing	S. Robertson
13:43	14:30	Technology Program Briefings	Drs Patt, Littlefield, Kamp, Haas
14:30	14:45	Break	
14:45	15:30	Technology Program Briefings	Drs Krolik, Wichowski, Sullivan
15:30	15:40	Closing Remarks	J. Galambos, DARPA PM

NAVAL AIR WARFARE CENTER
TRAINING SYSTEMS DIVISION
ORLANDO FLORIDA

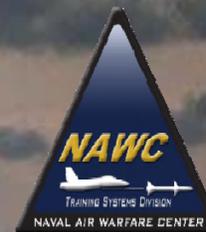


UNCLASSIFIED –
Approved for Public Release

CDMaST
Live Virtual Constructive
(LVC) Testbed

Long Nguyen
16 Nov 2013

Organization



UNCLASSIFIED – Approved for Public Release



- Simulations & Training
- Research Labs, Prototypes, Acquisition



UNCLASSIFIED – Approved for Public Release

NAWCTSD Battle Stations 21 Training System



Live, Virtual, & Constructive (LVC)

Live Exercise (L):

- Natural physical environment where the human operate their operational systems in a specific physical environment for which they were intended.

Virtual System (V):

- Synthetic environment where the human operates simulators, emulators or (stimulated) operational equipment.

Constructive Simulation (C):

- Synthetic environment consisting of simulated participants/platforms/sensors and their corresponding interactions.

LVC Events (LVC):

- At least one Live and one synthetic (Virtual or Constructive) integrated components.

Distributed LVC

Live - Real operators, real systems

Virtual - Real operators, simulated systems

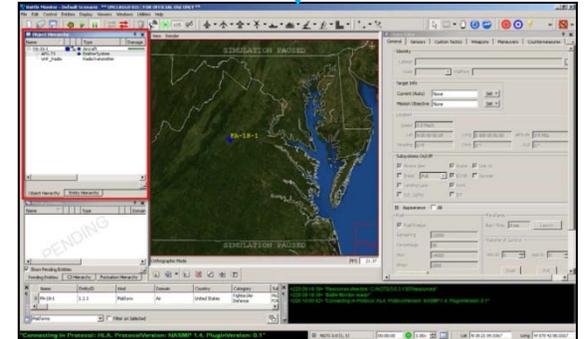
Constructive - Simulated operators, simulated systems



Live Example: A live E-2D providing data to both live and virtual exercise participants



Virtual Example: A P-3 Crew trainer. Real operators, simulated systems.



Constructive Example: Next Generation Threat System (NGTS) providing Air, Surface, Subsurface and Ground entities for an exercise.



LVC – Current State of the Art

- Navy Continuous Training Environment (NCTE)
 - an LVC Infrastructure, employed in the range
- Interservice/Industry Training Simulation & Education Conference – I/ITSEC 2015
 - NAWCTSD is leading a Distributed LVC Demonstration, 30 Nov
- Operations Center and Research Lab
 - an LVC Testbed

UNCLASSIFIED – Approved for Public Release



CDMaST LVC

NAWCTSD – Real-time Simulations & Training

DARPA's Push

- Explore LVC technology in CDMaST's solution space
- LVC testbed for experimentation and demonstration
- Exploit Model and Simulation (M&S) environments
- Engage LVC/Range Community for CDMaST thrust
- Augment physical platforms with LVC, optimize kill chain
- Support CDMaST M&S development
- Parallel CDMaST & LVC test bed architecture development
- CDMaST Interface and LVC Interoperability
- Scalable, persistent LVC/CDMaST architecture and protocols

UNCLASSIFIED – Approved for Public Release



Navy Continuous Training Environment (NCTE)

NCTE: Global infrastructure and system implementation standards supporting Navy distributed synthetic training

Infrastructure includes:

- Navy Enterprise Tactical Training Network (NETTN)
- Network universal translator (JBUS)
- Common Constructive Simulation (Joint Semi-automated Force, JSAF)

System implementation standards build on international, industry, and DoD Standards, e.g., High Level Architecture (HLA), Distributed Interactive Simulation (DIS), TCP/IP, etc.) to ensure interoperability.

Examples include:

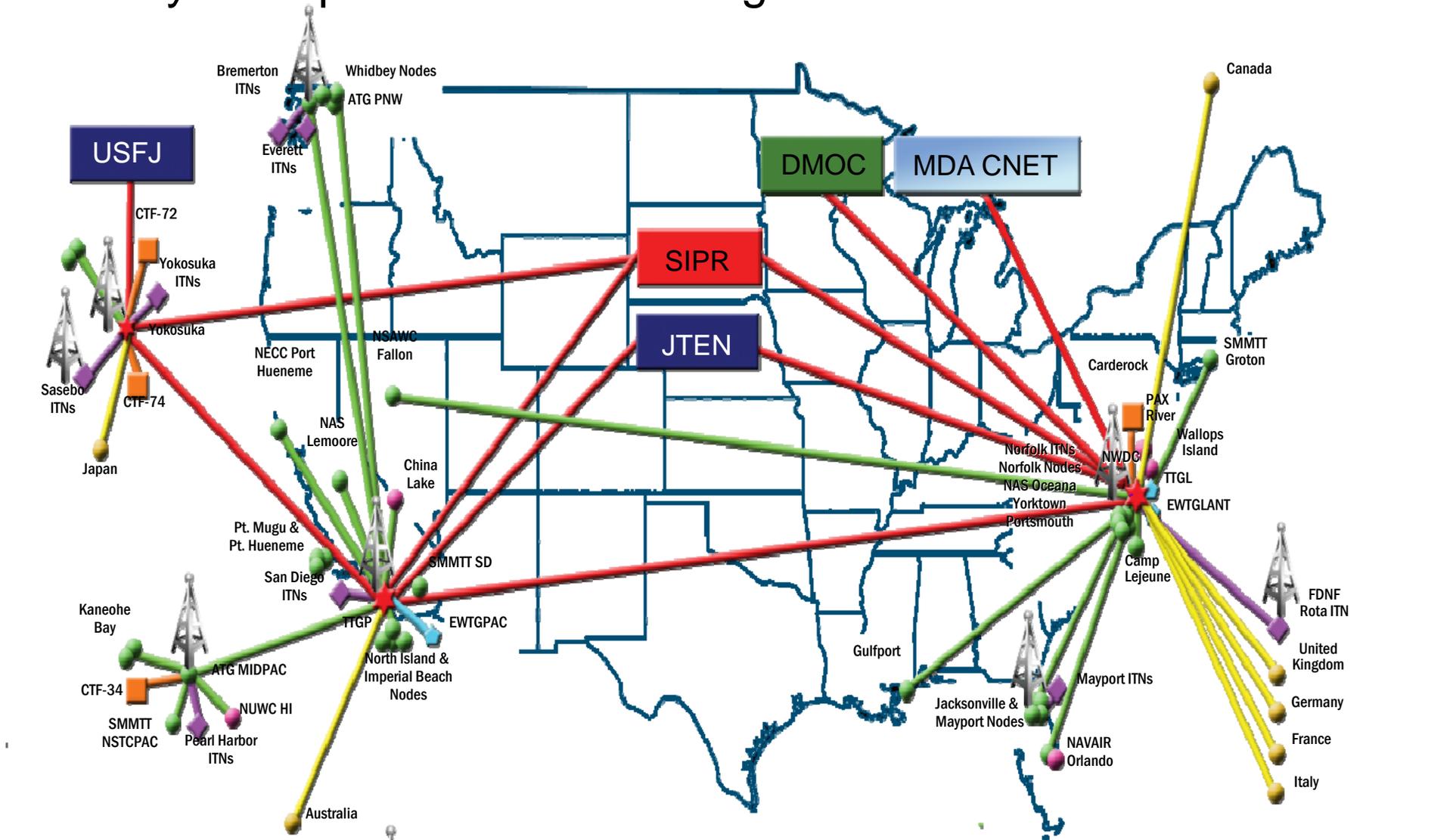
- NCTE Federation Standards
- NCTE Interoperability Guide

Adapt an LVC Infrastructure for CDMaST?

Source: USFF

UNCLASSIFIED – Approved for Public Release

NCTE - Navy Enterprise Tactical Training Network



Digital Radio Management System

Nodes, networks, ranges for CDMAST?

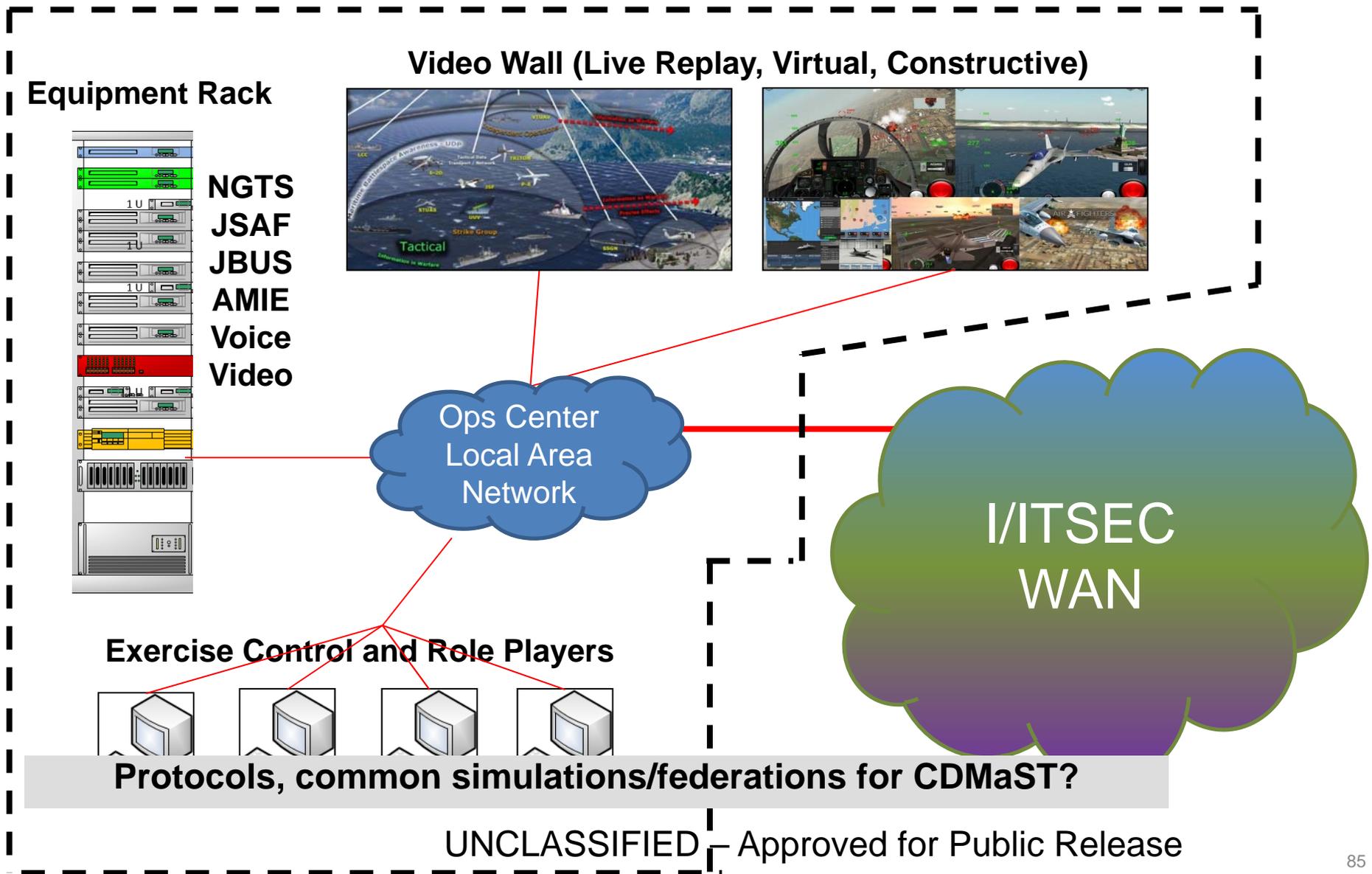
ITNs

Coalition

UNCLASSIFIED – Approved for Public Release

Source: USFF

DIRSAC 2015 LVC Special Event





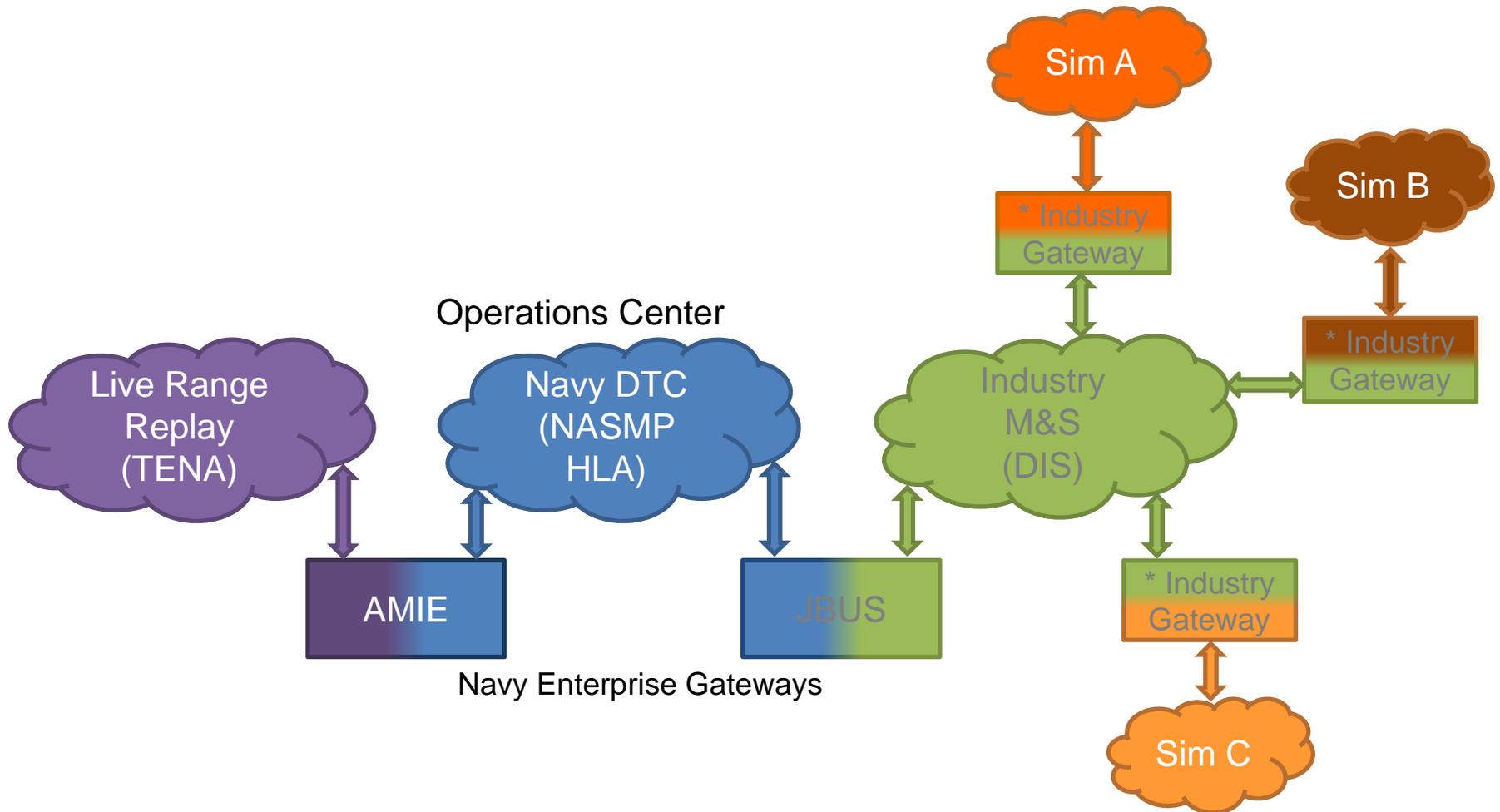
Operations Center:

- Central coordination for all Vignettes
- Role Playing
 - Radio Comms
 - SAF manipulation (NGTS and JSAF)
- Exercise Control/Coordination
 - Exercise Control
 - Scenario Control
 - Exercise Direction
- Technical Oversight Capability
 - DTC JBUS and AMIE configuration
 - Network Control
 - Exercise Troubleshooting
 - Exercise Coordination
- God's Eye View (large video wall)
 - Configurable views (video matrix)

CDMaST Ops Center?



IITSEC Network Architecture

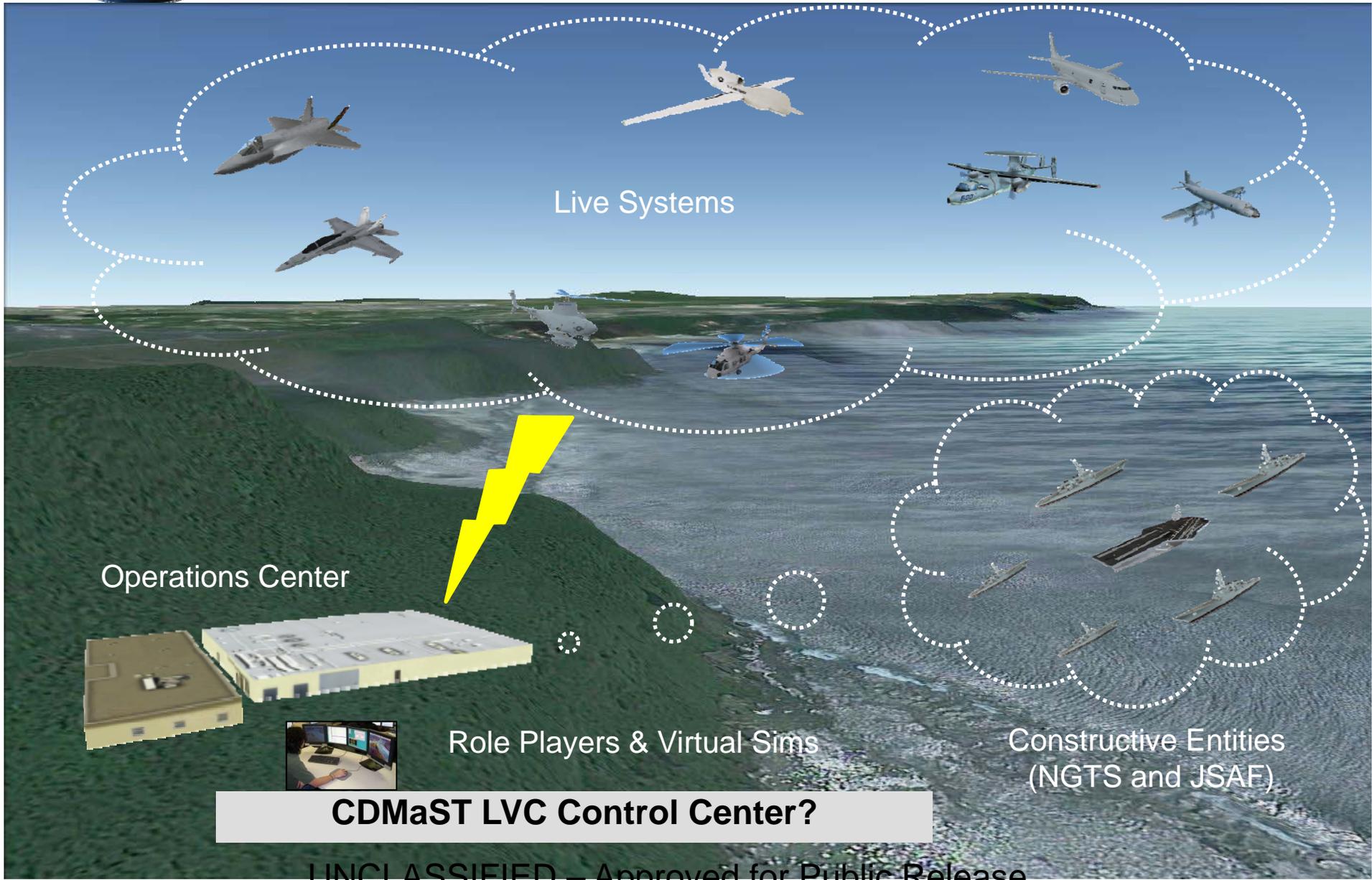


CDMaST LVC Network?

UNCLASSIFIED – Approved for Public Release



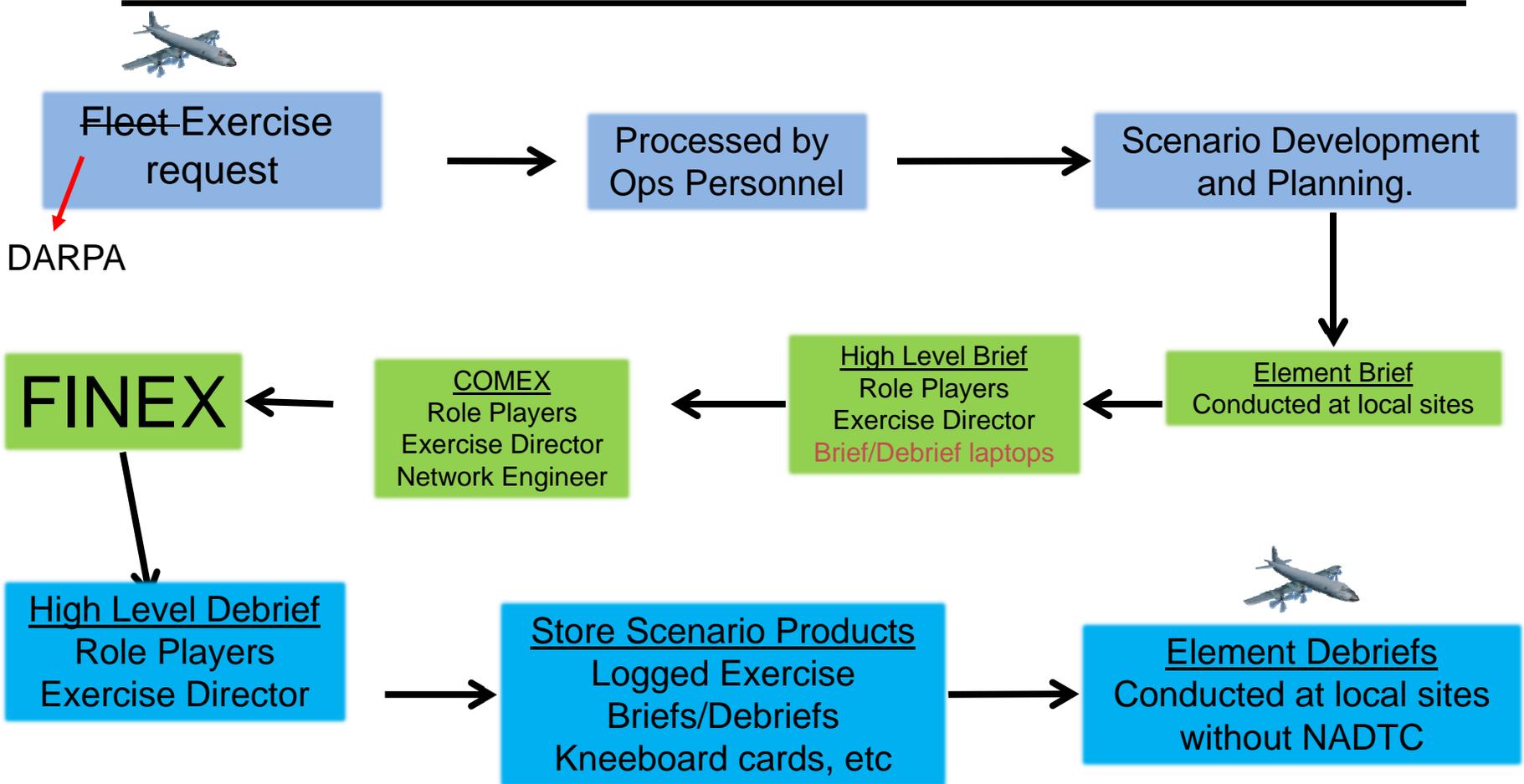
LVC Control Center



CDMaST LVC Control Center?

UNCLASSIFIED – Approved for Public Release

LVC Exercise



CDMaST LVC Scenario, use cases?