

Test/Cyber Requirements and Capability Gaps Abstract

The use of cyberspace operations to defend supported networks and project power through the digital domain is at the leading edge of new age warfare. DoD agencies are working feverishly to define doctrine, tactics, techniques, procedures and materiel requirements to enable the employment of cyberspace operations in support of national, strategic, operational and tactical objectives. Development of tools and technology to test and verify effectiveness of weapon systems is critical for success in the cyberspace domain. In addition, unique technical knowledge and lessons learned from the test community provide an excellent launch point for the development of training systems simulating cyberspace effects.

The Test/Cyber Requirements and Capability Gaps Panel brings together key Government, Industry and Academic experts to discuss current and future initiatives to ensure weapon systems and platforms are tested within a realistic cyberspace operating environment. The panel will present user requirements, proposed science and technology needs, and current industry and academic perspectives on implementation of cyber testing. The panel will also address the "Shift Left" paradigm which provides greater emphasis on cyber testing during program development versus only at an operational test. The panel will discuss opportunities for the community build training capabilities leveraging knowledge gained from cyber-related testing.

This panel is for those interested in gaining a better understanding of cyberspace activities within the test and training communities. Project managers, engineers, technology managers, and business development personnel should attend this interactive session. The panel will provide presentations and will interact through real time questions from the audience.

Test-Cyber Panel



Colonel Mike Flanagan, USA Ret'd
Moderator
18 June 2015



Test-Cyber Panel



1. Mr. Rick Copeland, Acting PM ITTS
2. Mr. Joshua Miller, Senior Evaluator, Survivability Evaluation Directorate, Army Test and Evaluation Command/Army Evaluation Center
3. Ms. Cisca Vuong, PM ITTS Chief Engineer
4. Mr. Mike Aldinger, Northrop Grumman IS, Manager, LVC Mission Integration
5. Mr. Jon Callahan, General Dynamics Mission Systems, Deputy Program Manager
6. Dr. Fred Wright, Deputy Director and Chief Engineer, Cyber Technology and Information Security Laboratory, Georgia Tech Research Institute
7. Mr. Jason Wonn, CGI-Federal, Director, Cyber Engineering & Consulting Services

Moderator: COL Mike Flanagan, USA Ret'd, Vice President, CACI-Fed





Mr. Joshua Miller (ATEC)



- Senior Evaluator, Survivability Evaluation Directorate, Army Test and Evaluation Command/Army Evaluation Center
- Cybersecurity Test and Evaluation: The Army Perspective





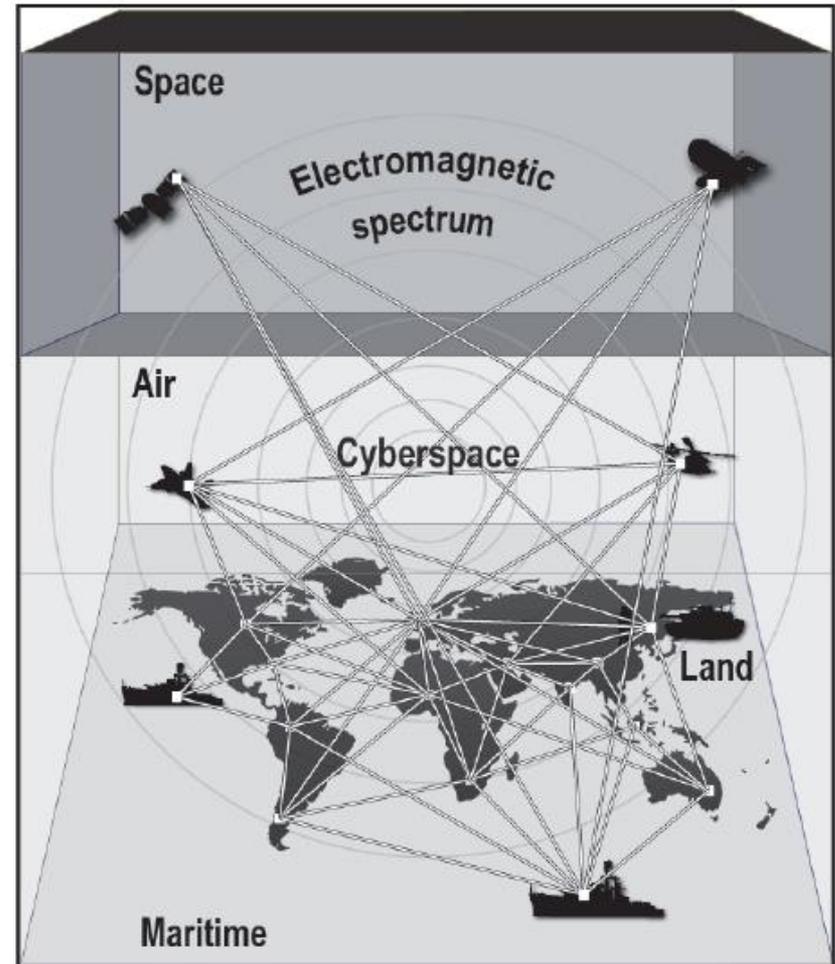
Operational Environments

Operational Environment domains:

- Air (naturally occurring)
- Land (naturally occurring)
- Maritime (naturally occurring)
- Space (naturally occurring)
- Cyberspace (manmade)

DoD Reliance on Cyberspace for:

- Military Command and Control
- Intelligence
- Business Operations



Reference: FM 3-38: Cyber Electromagnetic Activities





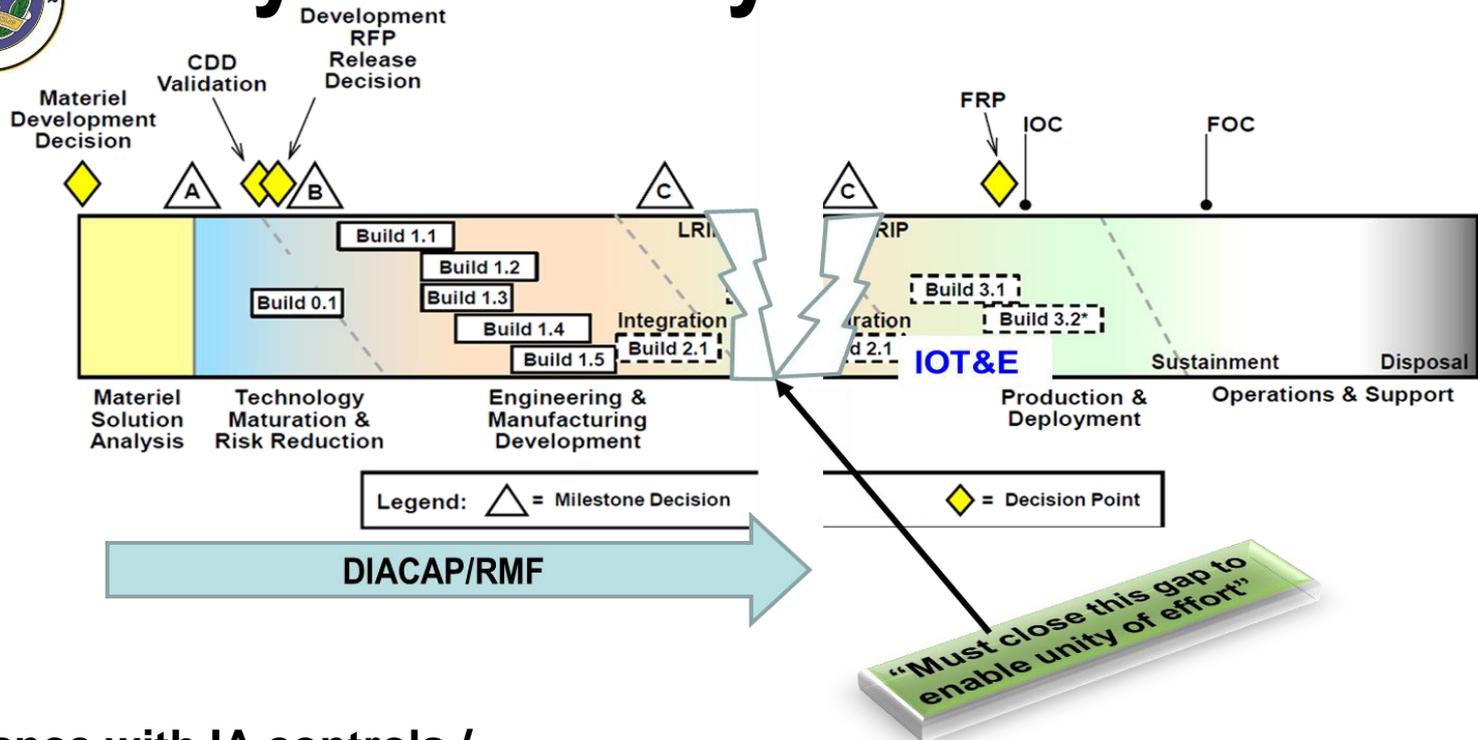
ATEC Initiatives

- **Shift Left**
- **Earlier Developmental T&E for Cyber Security – Cooperative Vulnerability and Penetration Assessments (CVPA) to Prepare Systems for Record Test**
- **Test & Evaluation Program Synchronization (TEPS)**
 - **Early communication on Test and Evaluation metrics**
 - **The Cybersecurity Scorecard**
- **EW - investments in signals collection and automation**
- **Realistic Threat Portrayals**
- **Metrics Study**
 - **Effort in partnership with MIT – Lincoln Labs**
 - **Examine the application of continuous monitoring**





Cybersecurity "Shift Left"



Compliance with IA controls / standards and profiles are necessary but not sufficient

Fielded systems found to have novice IA vulnerabilities during OT, which is problematic and costly.

Shift Left

to discover cybersecurity issues earlier in the acquisition lifecycle.





Effect on Cybersecurity Testing

- Shift Left
 - Formally add cybersecurity DT to the TEMP
- ATEC: Leverage existing test capabilities rather than build new
-
- Build T&E plans starting with Risk Management Framework (RMF) products
 - RMF replaces DIACAP with intent to manage risk over the system's lifecycle





Effect on Cybersecurity Evaluation

- Assess program readiness for major events such as MS C or Initial Operational Test (IOT)
 - AEC cybersecurity scorecard to continually assess
- Incorporate DOT&E 1 August 2014 policy memorandum
 - Protect, Detect, React, Restore

Planning for (event/milestone)

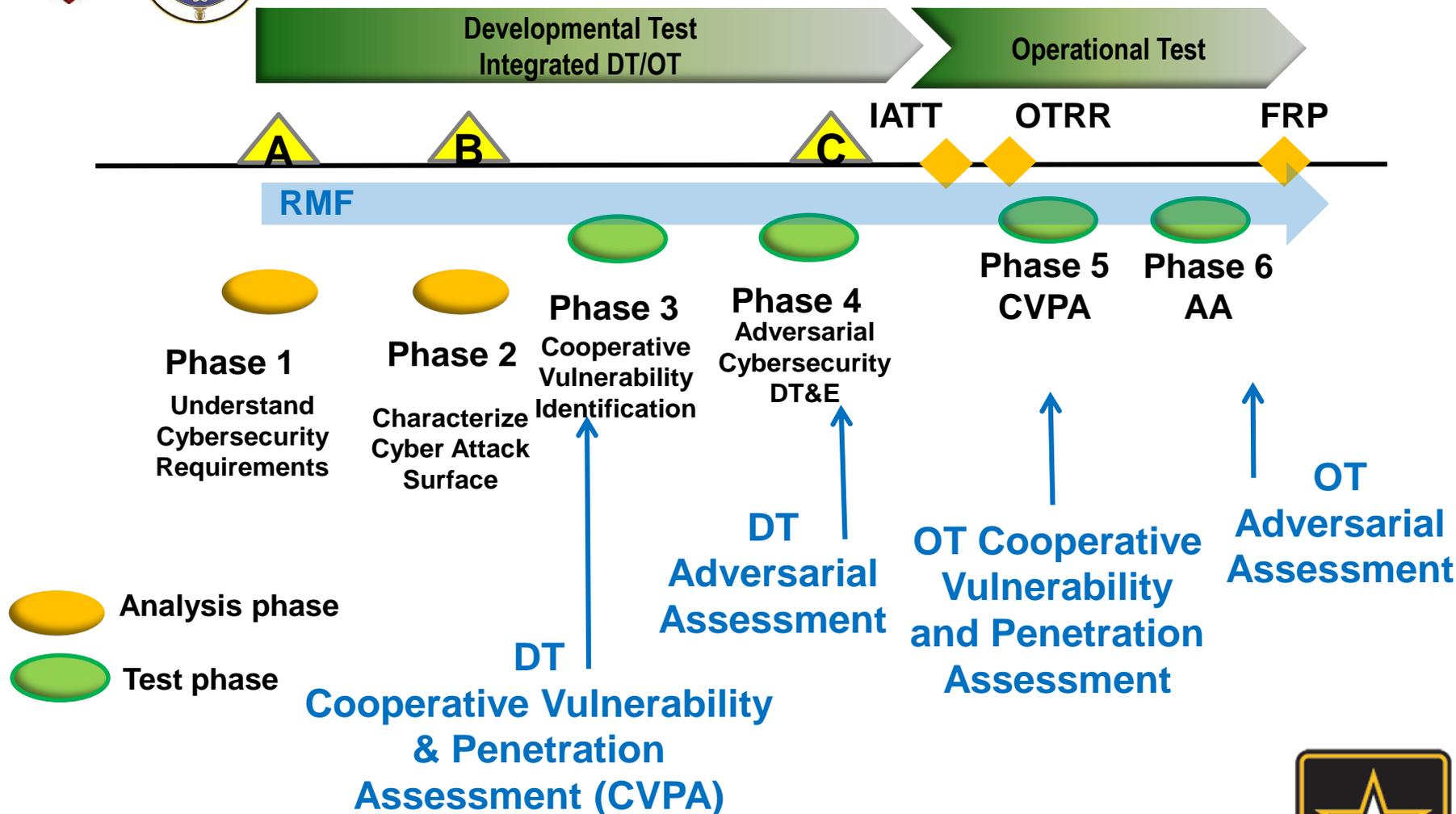
Event	Score	Comments
TEMP	G Y R	Date; Unresolved Issues, related to DOT&E Attachment D
Draft TTSP Part I	G Y R	Date; Unresolved Issues
OTRR 1, T-240	G Y R	Date, Venue, ARL Lead; Unresolved Issues
TAWG	G Y R	Date; Unresolved Issues
Core System Protection, and Core Cyber Defense Performance – Data and Metrics	G Y R	Unresolved Issues, related to DOT&E Attachment C
Operational Test Plan	G Y R	Unresolved Issues, related to DOT&E Attachment E
1 st (DT) Blue Team Assessment	G Y R	Date; Unresolved Issues
1 st (DT) Red Team Assessment	G Y R	Date, Venue, TSMO Lead; Unresolved Issues
OTRR 2, T-60	G Y R	Date; Unresolved Issues
Verification of Fixes	G Y R	Date, Venue, Provider; Unresolved Issues
OTRR 3, T-5	G Y R	Date; Unresolved Issues
2 nd (OT) Blue Team Assessment	G Y R	Date, Venue, ARL Lead; Unresolved Issues
2 nd (OT) Red Team Assessment	G Y R	Date, Venue, TSMO Lead; Unresolved Issues



Cybersecurity T&E Scorecard Presented at Each PEO Executive Test Day



Proposed Cybersecurity T&E Events



Events derived from draft DASD(DT&E) DoD Cybersecurity Test and Evaluation Guidebook, and DOT&E Cybersecurity Operational Test and Evaluation Guidance Memo (01 August 2014)





Challenges

- **Cybersecurity as Systems Engineering Discipline**
- **Contractual Language for systems with IT**
- **Cyber Test Ranges – “Plug and Play” Tactical Network**
- **M&S – Virtual Machine Emulation & Simulation**
 - **System of Systems Risk Assessment for Investment Decisions**
- **Operational Requirements**
 - “If there is a computer in something, it *can* be [cyber-attacked](#), and we need to be able to harden it and defend it,” the Pentagon’s [Deputy Chief Information Officer for Cybersecurity](#) Mr. Richard Hale
 - “The Joint Staff has recently put out a formal requirement document that includes cybersecurity as a key part of the survivability key performance parameter [KPP]” for every new system”
- **Addressing DOTMLPF-P**
- **Metrics**

**Defensible
Systems**





Ms. Cisca Vuong (PEO STRI)



- Chief Engineer for Project Manager, Instrumentation, Targets & Threat Simulators (PM ITTS)

- PM ITTS S&T/Capability Gaps





PM ITTS Strategic Focus Areas



- **Support Army Capabilities as Material Developer for Test**
 - Validated Cyber and Electronic Warfare Threats, Targets, and Test Range Instrumentation
- **Training Material Developer**
 - Special Operations Forces (including 160th SOAR), Intelligence, and Fires
- **Emerging Test Capabilities**
 - Integrated Live Virtual Constructive Test Environment
 - Warrior Injury Assessment Manikin
- **Stakeholders**
 - Combatant Commands
 - Army G2, INSCOM and TRADOC Centers of Excellence
 - Army Test and Evaluation Command and Army Test Centers
 - OSD Director, Operational Test & Evaluation
 - OSD Director, Developmental Test & Evaluation





S&T for Test & Evaluation



- PM ITTS leverages primarily DoD Test Resource Management Center (TRMC) T&E/S&T
 - S&T requirements submitted through established T&E Reliance Panel Needs and Solutions Process
- TRMC strategic focus on eight Test Technology Areas (TTA)
 - Advanced Instrumentation Systems Technology (AIST)
 - Cyberspace Test Technology (CTT)
 - Directed Energy Test (DET)
 - Electronic Warfare Test (EWT)
 - High Speed Systems Test (HSST)
 - C4I and Software Intensive Systems Test (C4T)
 - Spectrum Efficient Technology (SET)
 - Unmanned and Autonomous Systems Technology (UAST)
- Emphasis on efficiency and commonality
 - Minimize duplication of effort





Test / Cyber S&T Research Areas



TSIS S&T #	S&T Focus Area	Research Areas	Target Program of Record	Estimated Current TRL	Program Need Date		
					Near Term (2016-2020)	Mid Term (2020-2030)	Far Term (2030-2040)
1	Threat cyber capabilities	Enhance threat Computer Network Operations	Various	Various	X	X	X
2		Threat Computer Network Attack & Computer Network Defense	Various	Various	X	X	X
3		Remote mission command of multiple cyber platforms;	Various	Various	X	X	X
4		Modeling & execution of cyber activities	Various	Various	X	X	X
5		Virtualization of threat networks	Various	Various	X	X	X
6		Threat cyber tools developed as Software as a Service (SaaS)	Various	Various	X	X	X





Current Cyber T&E/S&T Efforts



- TSMO cyber threat environments
 - Automated Cyberspace Threat Representation (ACTR)
 - S&T effort executed under TRMC CTT
 - Potential S&T insertion/transition to TSMO Network Operations Security Center (NOSC)
 - Framework for Automated and Verified Sanitization (FAVS)
 - S&T effort executed under TRMC CTT
 - Potential S&T insertion/transition to TSMO NOSC, National Cyber Range (NCR)
- Work collaboratively with CERDEC Intelligence and Information Warfare Directorate (I2WD) and SMEs to shape/address Army S&T needs for threat cyber T&E





Mr. Rick Copeland (PEO STRI)



- Acting Project Manager, Instrumentation, Targets & Threat Simulators (PM ITTS)

- PM ITTS Support/Mission in Test and Cyber





PM ITTS Strategic Focus Areas

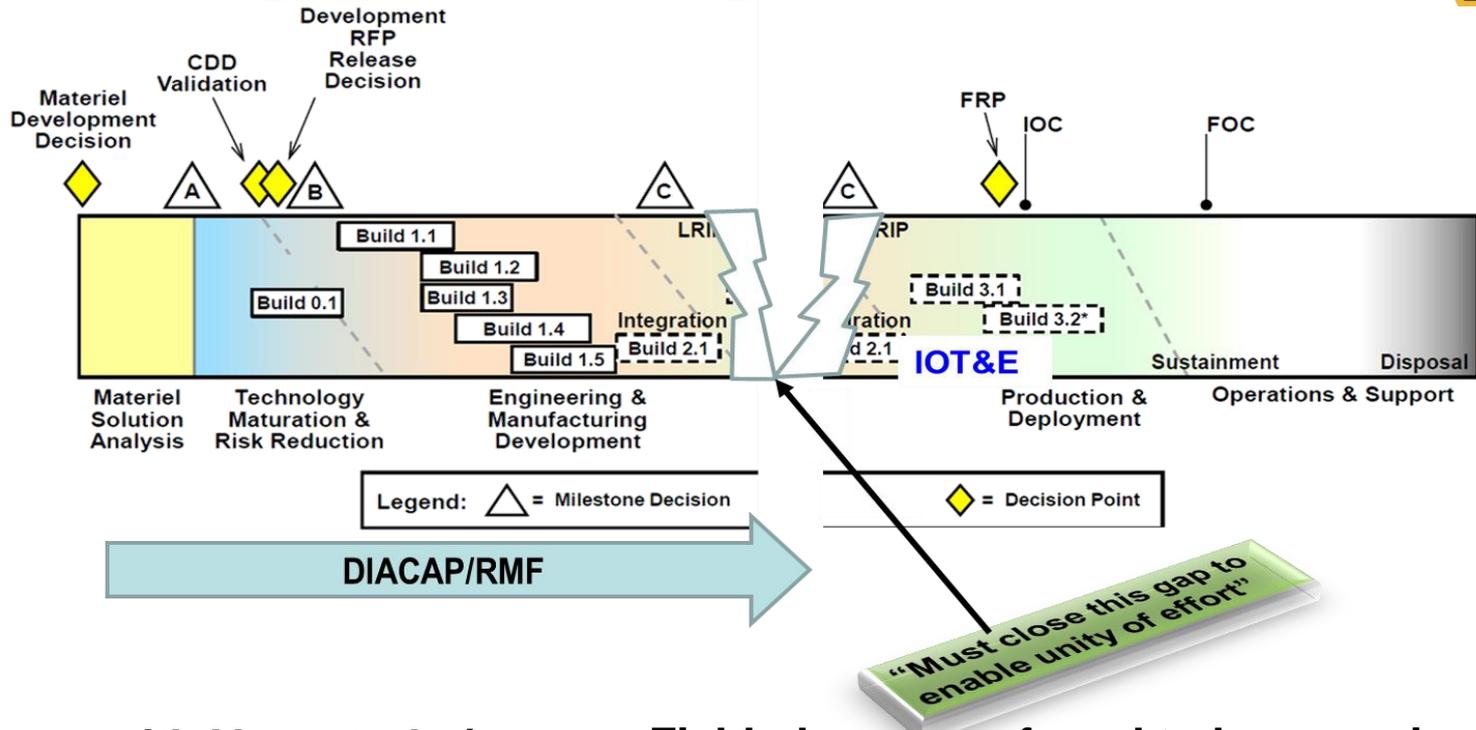


- **Support Army Capabilities as Material Developer for Test**
 - Validated Cyber and Electronic Warfare Threats, Targets, and Test Range Instrumentation
- **Training Material Developer**
 - Special Operations Forces (including 160th SOAR), Intelligence, and Fires
- **Emerging Test Capabilities**
 - Integrated Live Virtual Constructive Test Environment
 - Warrior Injury Assessment Manikin
- **Stakeholders**
 - Combatant Commands
 - Army G2, INSCOM and TRADOC Centers of Excellence
 - Army Test and Evaluation Command and Army Test Centers
 - OSD Director, Operational Test & Evaluation
 - OSD Director, Developmental Test & Evaluation





Cybersecurity “Shift Left”



Compliance with IA controls / standards and profiles are necessary but not sufficient

Fielded systems found to have novice IA vulnerabilities during OT, which is problematic and costly.

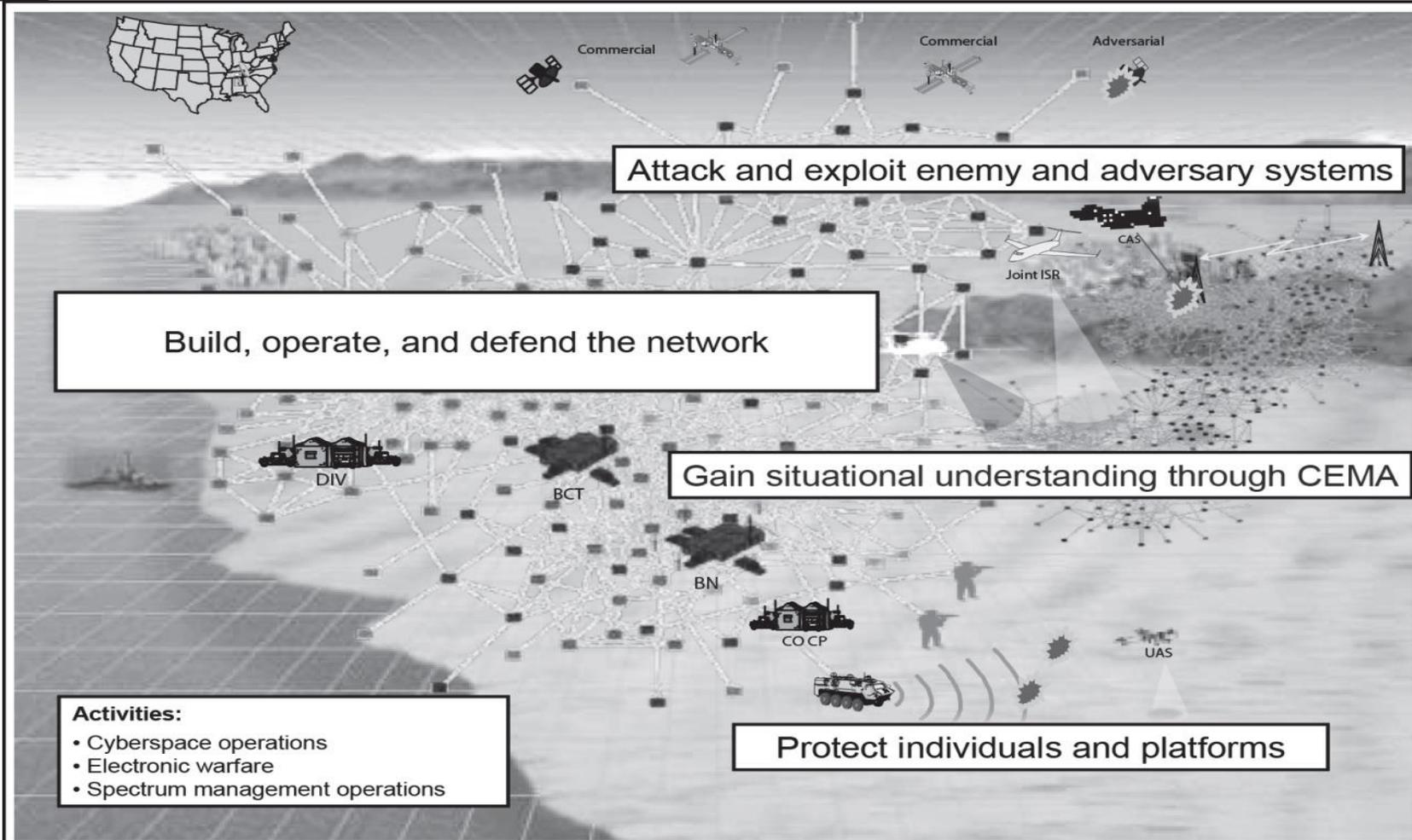
Shift Left

to discover cybersecurity issues earlier in the acquisition lifecycle.





Cyber Electromagnetic Activities



BCT	brigade combat team	CEMA	cyber electromagnetic activities	ISR	intelligence, support, reconnaissance
BN	battalion	COCP	company command post	UAS	unmanned aerial systems
CAS	close air support	DIV	division		

From FM 3-38; Approved for public release; Field Manual No. 3-38; Headquarters Department of the Army; Washington, DC, 12 Feb 2014





Collective Cyber Training



- Leveraged Threat Computer Networks Operations, Red Team, and Cyber Environments/Range Experience to position PEO STRI as Army Materiel Developer for Collective Cyber Training Systems
- Organized a Consortium of Cyber Stakeholders to understand requirements and identify S&T needs
- Support system and collective training requirements generation process
- Designate PEO STRI as the Materiel Developer for Collective Cyber Training

Goal: PEO STRI Materiel Developer for Collective Cyber Training Systems





Mr. Mike Aldinger (Northrop Grumman)

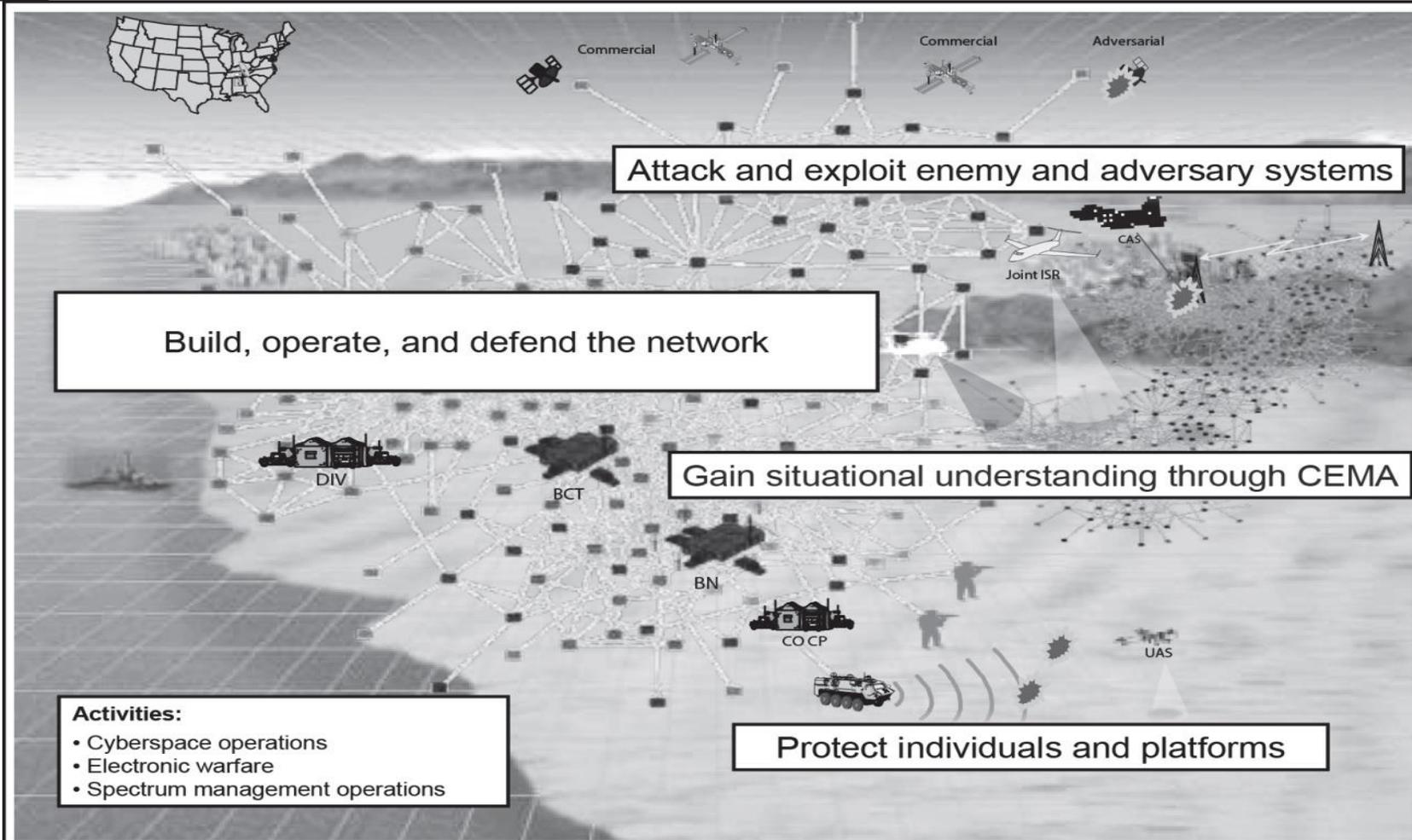


- Northrop Grumman IS, Manager, LVC Mission Integration





Cyber Electromagnetic Activities



BCT	brigade combat team	CEMA	cyber electromagnetic activities	ISR	intelligence, support, reconnaissance
BN	battalion	COCP	company command post	UAS	unmanned aerial systems
CAS	close air support	DIV	division		

From FM 3-38; Approved for public release; Field Manual No. 3-38; Headquarters Department of the Army; Washington, DC, 12 Feb 2014





Mr. Jon Callahan (General Dynamics)

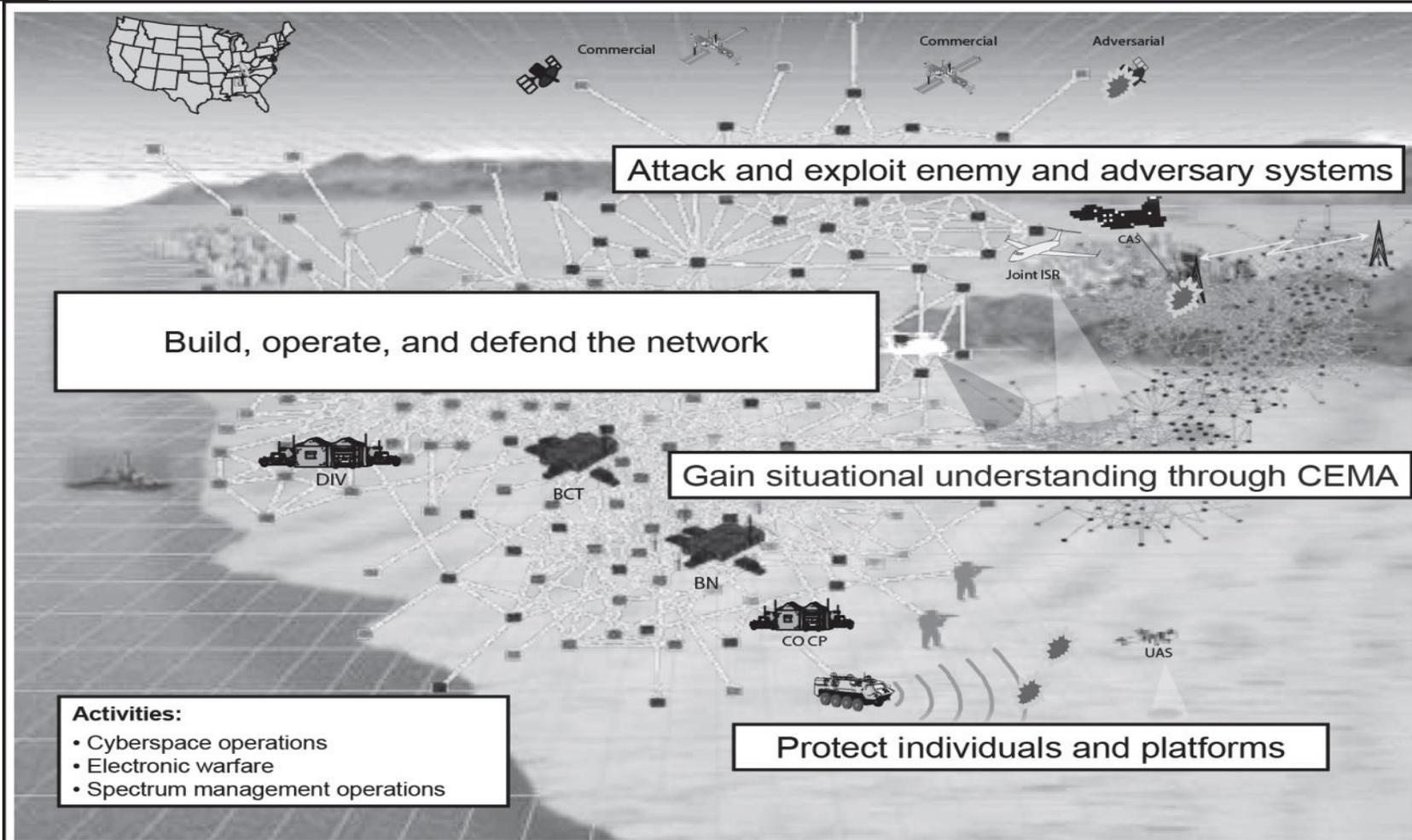


- Deputy Program Manager, General Dynamics Mission Systems





Cyber Electromagnetic Activities



BCT	brigade combat team	CEMA	cyber electromagnetic activities	ISR	intelligence, support, reconnaissance
BN	battalion	COCP	company command post	UAS	unmanned aerial systems
CAS	close air support	DIV	division		

From FM 3-38; Approved for public release; Field Manual No. 3-38; Headquarters Department of the Army; Washington, DC, 12 Feb 2014





Dr. Fred Wright (Georgia Tech)

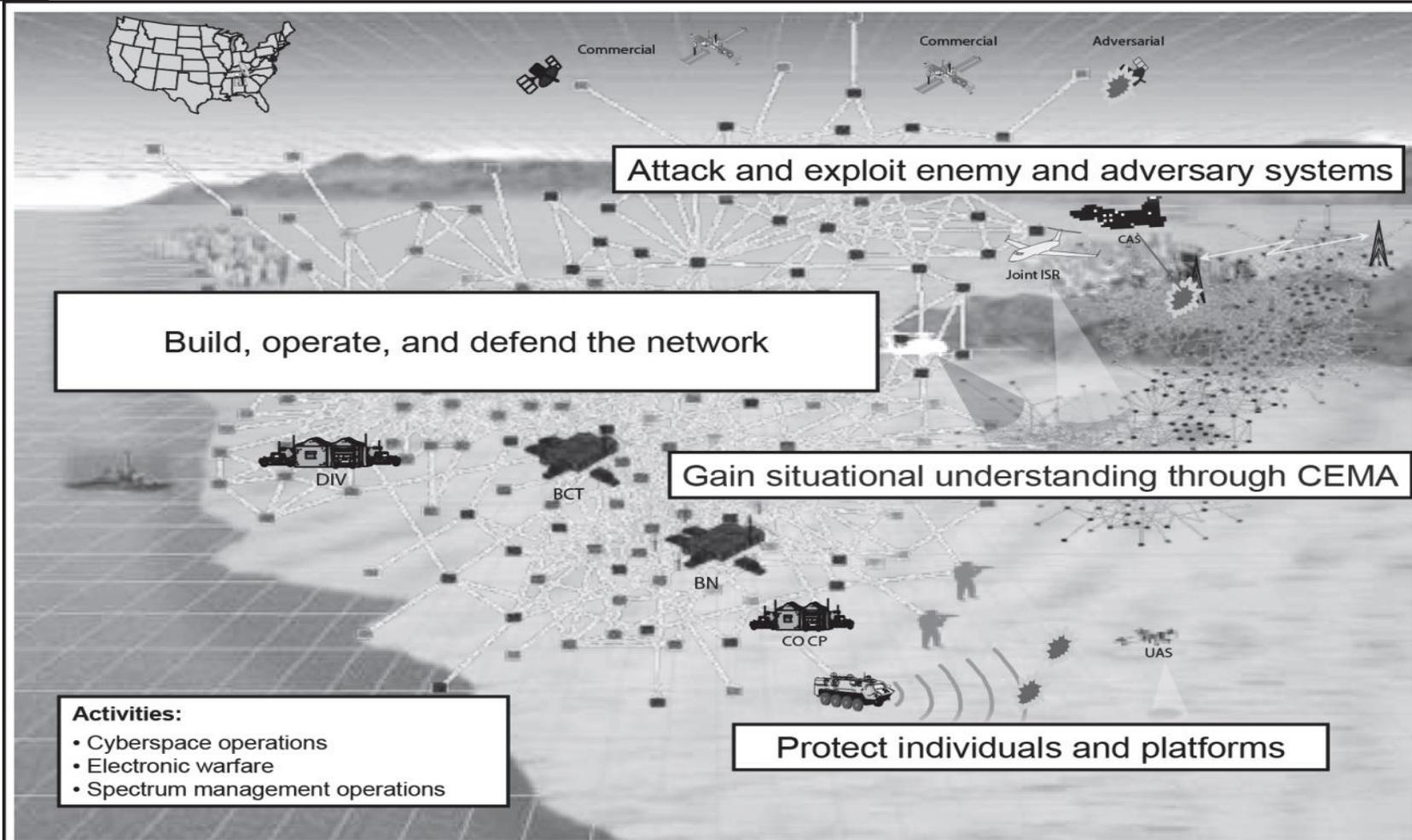


- Deputy Director and Chief Engineer, Cyber Technology and Information Security Laboratory, Georgia Tech Research Institute





Cyber Electromagnetic Activities



BCT	brigade combat team	CEMA	cyber electromagnetic activities	ISR	intelligence, support, reconnaissance
BN	battalion	COCP	company command post	UAS	unmanned aerial systems
CAS	close air support	DIV	division		

From FM 3-38; Approved for public release; Field Manual No. 3-38; Headquarters Department of the Army; Washington, DC, 12 Feb 2014





Mr. Jason Wonn (CGI-Federal)

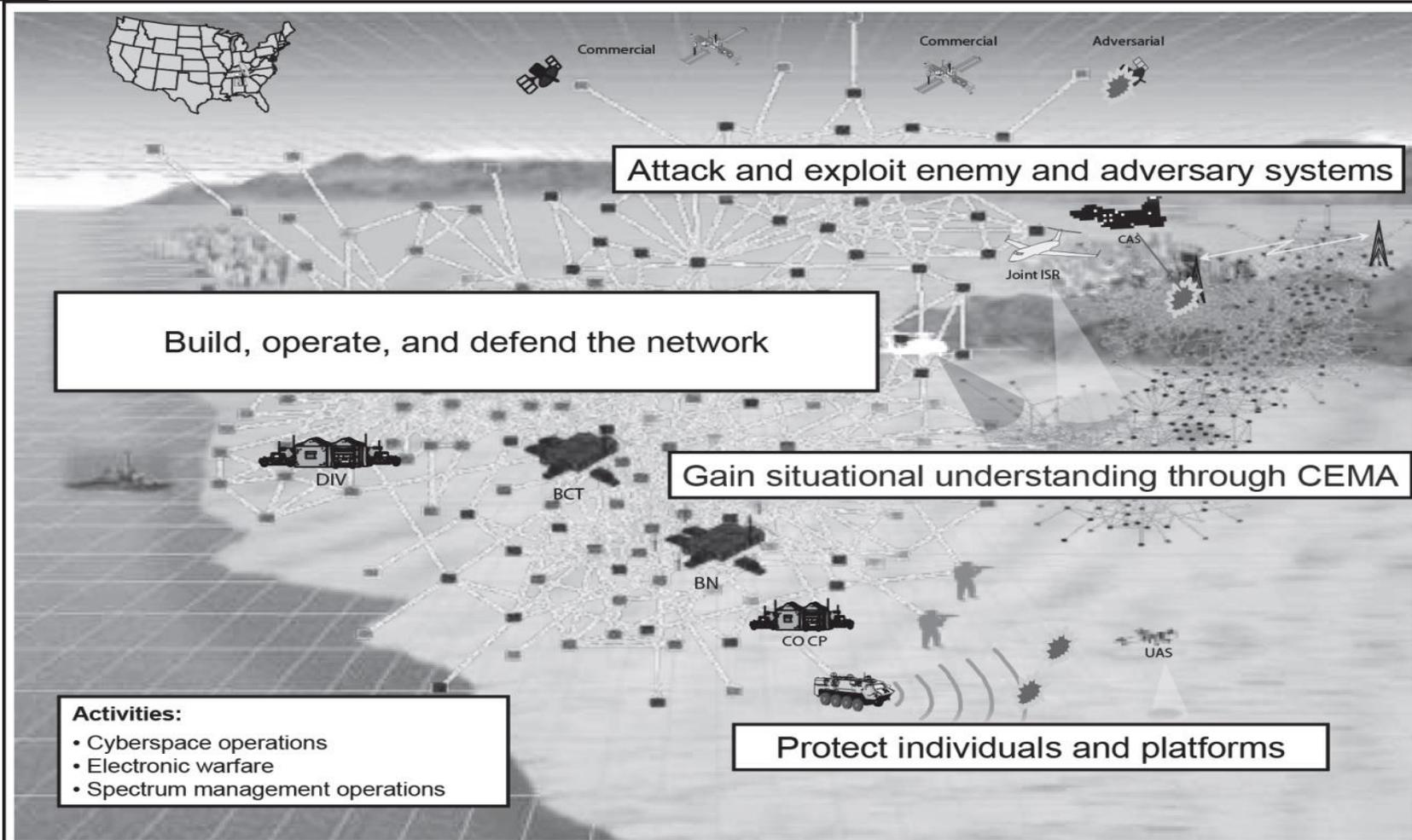


- Director, CGI-Federal Cyber Engineering & Consulting Services





Questions and Answers



BCT	brigade combat team	CEMA	cyber electromagnetic activities	ISR	intelligence, support, reconnaissance
BN	battalion	COCP	company command post	UAS	unmanned aerial systems
CAS	close air support	DIV	division		

From FM 3-38; Approved for public release; Field Manual No. 3-38; Headquarters Department of the Army; Washington, DC, 12 Feb 2014





Back-Up





PM ITTS Prioritized Capability Gaps



	Technology Area	Programs	Description
1	Threat cyber capabilities	Various	Enhance threat Computer Network Operations, threat Computer Network Attack & Computer Network Defense; Remote mission command of multiple cyber offensive platforms; Modeling & execution of offensive cyber activities providing force multiplier effects; virtualization of threat networks; threat cyber tools developed as Software as a Service (SaaS) available in secure cloud environments
2	Next Generation Tactical Engagement Simulation Systems	ILTE	Capabilities to provide an operationally realistic test environment by generating battlefield effects and cues that will cause Soldiers to act in a tactically correct manner
3	Target Remote Control & Time-Space-Position Information (TSPI) in GPS Denied Env.	Army Ground Aerial Target Control System (AGATCS); ILTE	Capability to calculate and provide reliable & accurate target position to remote target control system in GPS denied environment; Instrumentation required to measure & time tag 3D location of systems under test in operational & urban test events
4	Airborne Threat Jamming	Advanced Jammer Suite; Advanced Electronic Support	Capability to provide live & simulated threat communications and radar electronic attack (EA) systems housed in aviation assets to locate, maneuver to and jam communications and RF signals to include GPS and SATCOM transmissions from space.





Instrumentation Management Office (IMO)

Prioritized Capability Gaps



	Technology Area	Programs	Description
1	Next Generation TESS	ILTE	Capabilities to provide an operationally realistic test environment by generating battlefield effects and cues that will cause Soldiers to act in a tactically correct manner
2	Short Wave Infrared (SWIR) Metric Zoom Lens	Advanced Range Tracking and Imaging System (ARTIS)	Capability required in the SWIR for a continuous motorized zoom electro-optical instrument that changes its magnification to accommodate variations in object distances for tracking objects.
3	Enterprise Architecture and Synthetic Environment	ILTE	Infrastructure approach for service oriented architecture, cloud access to single synthetic environment, point of need, and One-World Terrain
4	Live Architecture	ILTE	Mobile/cloud/distributed computing architecture for Live capabilities deployed during operational tests
5	Time-Space-Position Information (TSPI) in GPS Denied Env.	ILTE	Instrumentation required to measure & time tag 3D location of systems under test involved in operational & urban test events (inside buildings, tunnels, alleys & maneuver area) in the presence of EW jamming & other effects
6	Terrain	ILTE	Correlation of geo-specific terrain with TESS to enable indirect fire weapon simulation and augmented reality of weapon effects.





Target Management Office (TMO) Prioritized Capability Gaps



	Technology Area	Programs	Description
1	Target Remote control in GPS Denied Environments	Army Ground Aerial Target Control System (AGATCS)	Capability to calculate and provide reliable and accurate target position to the remote target control system in GPS denied environment
2	Sophisticated Remote Target Control System (at low cost)	AGATCS, Aerial Flight Target Services (AFTS)	More economical installation, checkout, mission planning, & sustainment to lower total life cycle cost of remotely controlling ground/aerial targets; simultaneous remote control of mixed (manned & unmanned) targets
3	Aerial Targets Launch	MQM-107 Aerial Target Drone	Capability to launch MQM-107 aerial target drone using a safe launching technology other than Rocket Assist Take-Off (RATO) bottle that could potentially reduce operating costs & eliminate explosive items hazards
4	Multi-spectral personnel targets for EO sensor testing	Precision Targets Signature (PTS)	Multi-spectral personnel targets to support T&E of EO sensors & training personnel in detection, tracking & intent assessment. Personnel targets will be integrated into test & training scenarios, presented in different poses & displayed in multi-spectral bands ranging from visible to Long Wave Infrared (LWIR)





Threat Systems Management Office (TSMO)

Prioritized Capability Gaps



	Technology Area	Programs	Description
1	Threat cyber capabilities	Various	Enhance threat Computer Network Operations, threat Computer Network Attack & Computer Network Defense; Remote mission command of multiple cyber offensive platforms; Modeling & execution of offensive cyber activities providing force multiplier effects; virtualization of threat networks; threat cyber tools developed as Software as a Service (SaaS) available in secure cloud environments
2	Airborne Threat Jamming	Various	Capability to provide live and simulated threat communications and radar electronic attack (EA) systems housed in aviation assets to locate, maneuver to and jam communications and RF signals to include GPS and SATCOM transmissions from space.
3	Software Defined Radios (SDR)	Various	Use of SDR/Cognitive Radios/Dynamic Spectrum Assess (DSA) technologies to represent threat faithful representations; spectrum efficient, frequency agile, small form/fit.
4	Digital Radio Frequency Memory (DRFM)	Various	Capability to model both physics & effects of DRFM waveforms and to provide DRFM signal injection for EA simulators.
5	Threat Directed Energy	Various	Capability to provide live and simulated threat of high energy laser, high power microwave transmission in a focused (narrow beam) technique for threat electronic warfare environment





IMO Current T&E/S&T Efforts



- Advanced Range Tracking and Imaging System (ARTIS)
 - Short Wave Infrared (SWIR) Metric Zoom Lens
 - Topic released under AIST
 - Potential S&T insertion during Engineering & Manufacturing Development (EMD) phase
 - Supports objective requirement, not needed for threshold
- Integrated Live-virtual-constructive Test Environment (ILTE)
 - Real-Time Casualty Assessment (RTCA) Shoot through Foliage
 - Topic submitted under AIST
 - Potential S&T insertion during EMD phase
- Pulsed Neutron Environment (PNE)
 - PNE S&T Study conducted under DET
 - S&T insertion/transition to potential PNE Central T&E Investment Program new start
- Work collaboratively with Army test centers, RDECs and SMEs to shape/address Army S&T needs for T&E





DoD TRMC T&E/S&T Needs POAM



Activity	FY13					FY 2014					
	May-13	Jun-13	Jul-13	Aug-13	Sep-13	Oct-13	Nov-13	Dec-13	Jan-14	Feb-14	Mar-14
T&E/S&T Needs process											
Process documented by S&T panel											
Process reviewed by SME's											
Process reviewed by TRAG and BoD Staff											
Process approved											
Needs Call											
Draft Needs Call developed by panel											
Draft Call reviewed by TRAG and BoD Staff											
Needs call Approved by BoD											
Needs call Released											

