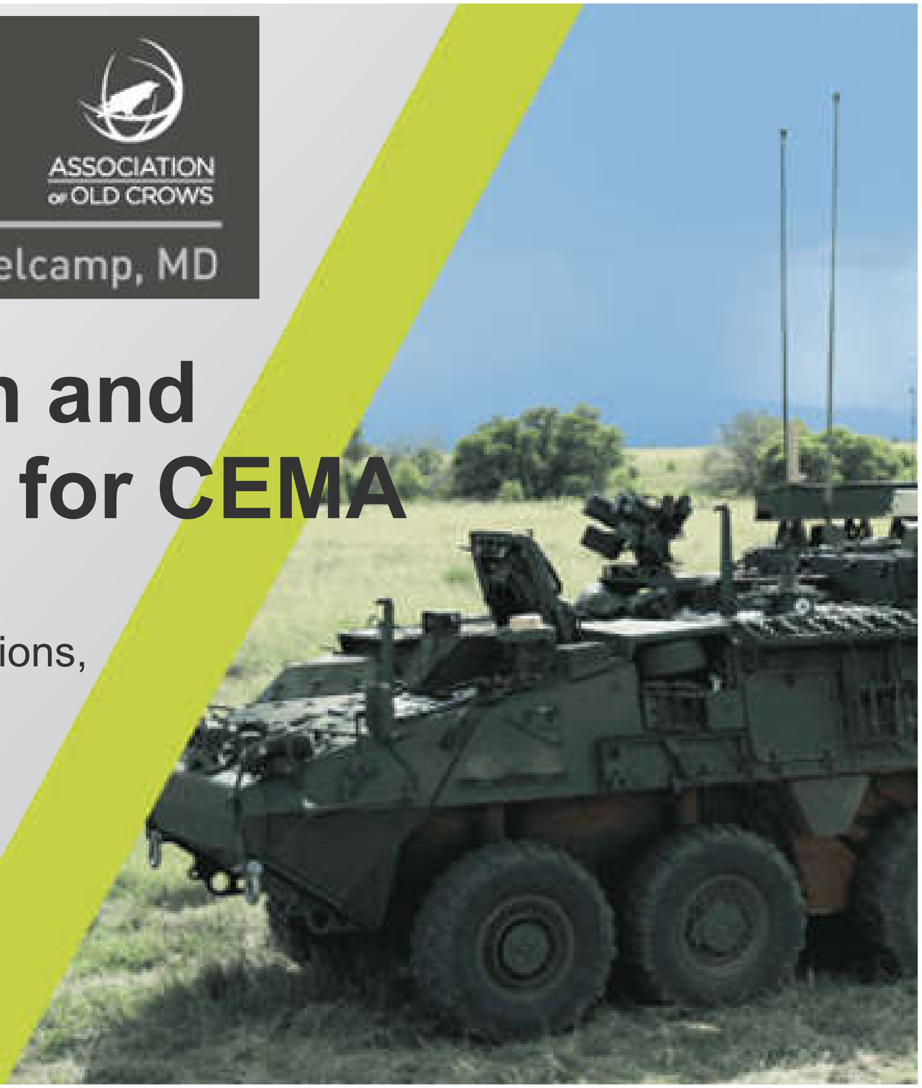
Cyber Electromagnetic Activity (CEMA) 2022

ASSOCIATION of OLD CROWS

MAY 3-4 Belcamp, MD

Distributed Data Fusion and Resource Management for CEMA

- **David McDaniel**
  - Principal Engineer, Silver Bullet Solutions, Inc.
  - davem@silverbulletinc.com



Acknowledgements

David M. McDaniel
Silver Bullet Solutions, Inc.
Arlington, VA, U.S.A.
davem@silverbulletinc.com

Todd Kingsbury
Silver Bullet Solutions, Inc.
San Diego, CA, U.S.A
todd.kingsbury@silverbulletinc.com

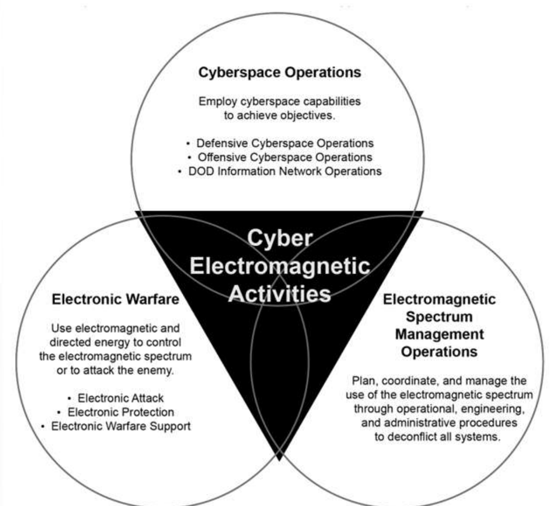
Ken Hintz
Associate Professor (Emeritus), Electrical and Computer Engineering, George Mason University / Perquire Research
Savannah, GA, U.S.A
ken.hintz@perquire.com

Rakesh Nagi
Donald Biggar Willett Professor of Engineering
University of Illinois
Urbana-Champaign, U.S.A
rakeshnagi@gmail.com

James Llinas
Research Professor (Emeritus), Executive Director
Center for Multisource Information Fusion
State University of New York at Buffalo
Buffalo, NY, U.S.A.
llinas@buffalo.edu

CEMA DDFRM Landscape on the Tactical Edge

1. Denied, Disrupted, Intermittent, and Limited (DDIL) and Anti-Access Area Denial (A2/AD) conditions
2. Coordinated CEMA attack
3. Attack on specialized tactical Industrial Control Systems (ICS), Supervisory Control and Data Acquisition (SCADA), and Internet of Things (IoT) equipment
4. Local-only network attack

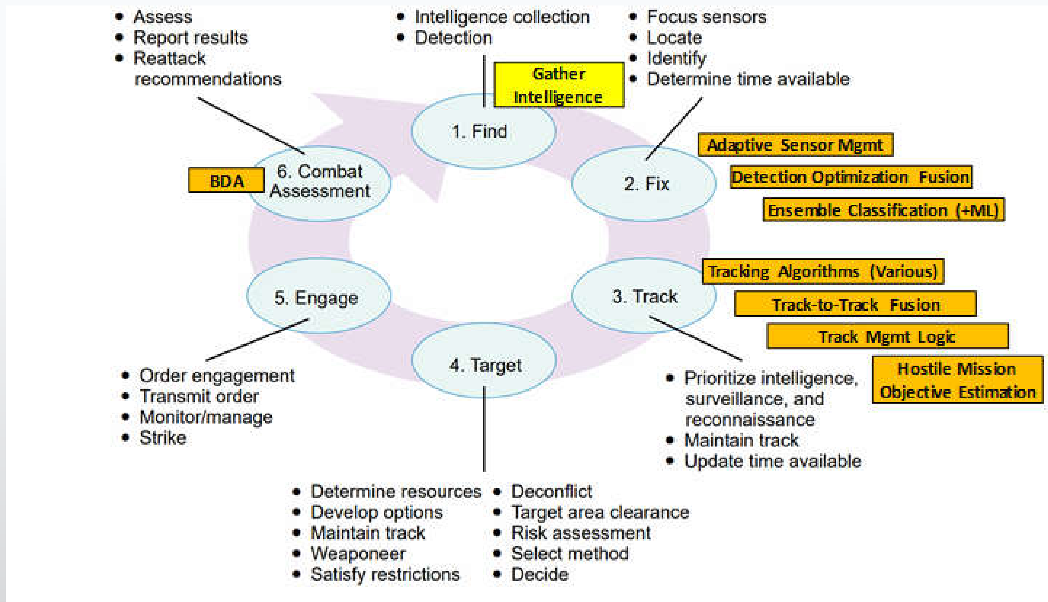


FM 3-38, Cyber Electromagnetic Activities, February 2014

		CEMA Activities		
Cyberspace Layers	**OSI/TCP Layers**	**Cyberspace**	**EW**	**EMSO**
Physical	1.Physical Layer	◔	●	●
Logical	2.Data Link Layer	◑	◕	◔
	3.Network Layer	◕	◑	
	4.Transport Layer	●	◔	
	5.Session Layer	●		
	6.Presentation Layer	●		
	7.Application Layer	●		
Persona		●		
Individual criminal		●		
Organized criminals		●	◔	
Non-nation state		●	◕	◔
Nation state		◕	●	●

Data Fusion (DF) and Resource Management (RM) Frameworks in Kill Chains

- Correlated DF functions in orange boxes support:
  - Hostile mission and intent assessment
  - Optimal weapon assignment and precise designation
  - Weapon operations e.g.,
    - Offensive Cyber Ops (OCO) / Electronic Warfare (EW)
    - Defensive Cyber Ops (DCO) / Electronic Counter Measures (ECM)
    - Network / EM maneuver
    - Endpoint reconfiguration
  - Battle Damage Assessment (BDA)
  - Possibly re-targeting
- Cyber kill chain
  - Reconnaissance
  - Weaponization
  - Delivery
  - Exploitation
  - Installation
  - Command & Control
  - Actions on Objectives

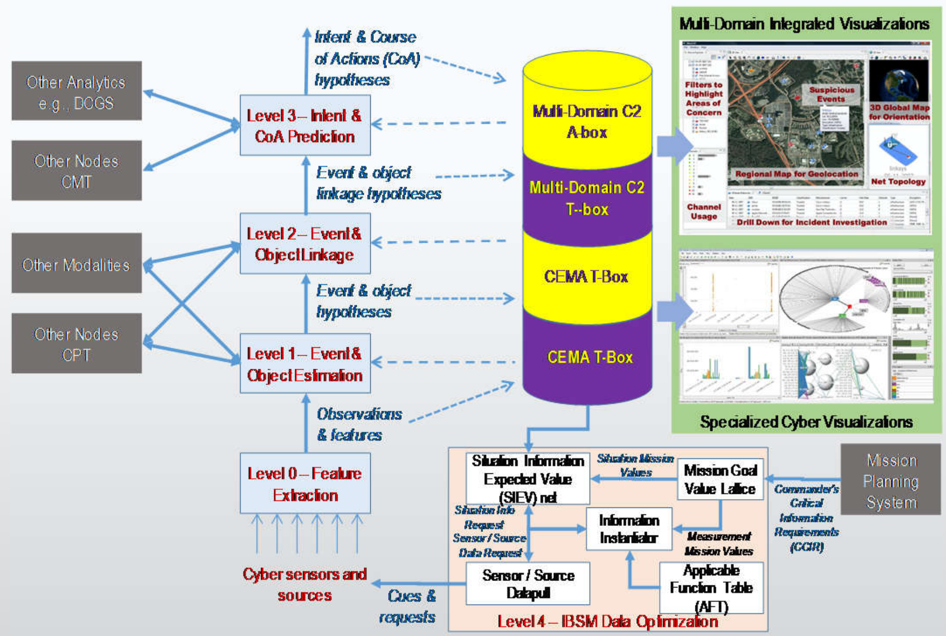


Background is Joint Publication 3-60, Joint Targeting, 28 September 2018

Cyber Electromagnetic Activity (CEMA) 2022
MAY 3-4
Belcamp, MD

DDFRM-CEMA Architecture Major components

- Ontology
  - Formal and extensible ontology that can go from CEMA modalities to real-world behaviors
  - A-box and T-box (assertional and terminological components)
- Distributed Data Fusion
  - Directed Acyclic Relationship Graph (DARG) makes inferences (hypotheses and likelihood ratios) from sensor and data sources to objects and events and linkages-between and predictions-about them.
  - Other nodes and modalities
- Resource Management
  - Adapts the data fusion system to CEMA sensors and data sources using a situation dependent lattice of mission goals valuing optimal information-gathering observations and indicators.



CEMA Ontology has Disparate Layers

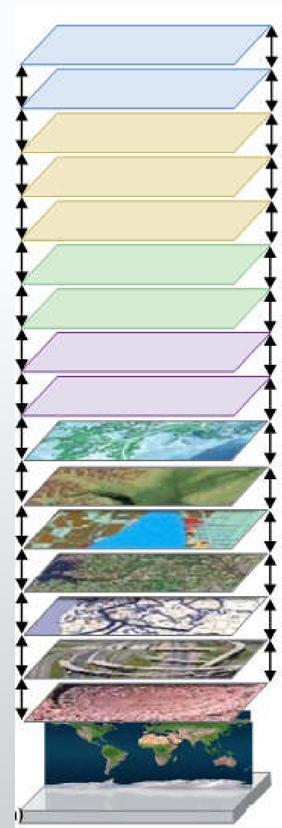
- Many data layers typically considered in CEMA contexts
- Upper layers could include:
  - Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time (PMESII-T),
  - Diplomatic, Information, Military, and Economic (DIME)
  - Areas, Structures, Capabilities, Organization, People and Events (ASCOPE)
- Layers are "disparate",
  - essentially different in kind
  - do not easily allow comparison or synthesis
- Three major challenges:
  - Alignment and normalization
  - Association to create a complete evidential picture of the operational domain
  - Exploitation to extract/assess the existence of Commander's Critical Information Requirements (CCIR) or Priority Intelligence Requirements (PIR)

Non Realtime (NRT) Feeds
- Message (e.g., USMTF, AMHS)
- RSS
- Weather

Intelligence Layers
- Threats
- AOB / GOB / NOB / EOB
- Assessments
- Targeting
- Cyberspace Order of Battle

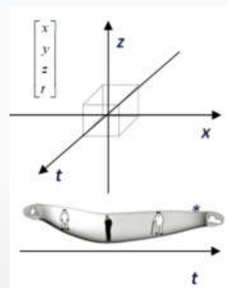
Cross-Functional Data Layers
- UN, host nation, NGO
- Regional cooperation relationships
- Mission Partners
- Climate, ecosystem applications
- Demographic, human geography
- Logistics plans and operations
- Operation/concept plans
- Checkpoints, MSRs, LOCs

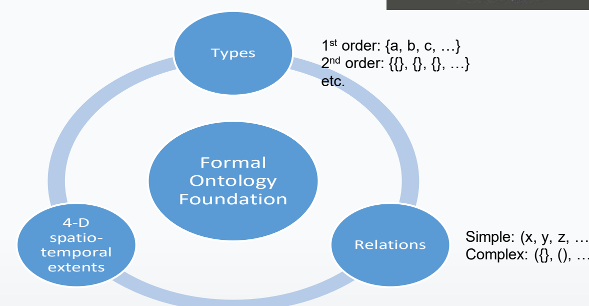
Shared Foundation Databases
- Map, topographic data
- Imagery data
- EMOE, EMS
- Cyberspace Terrain and Topography

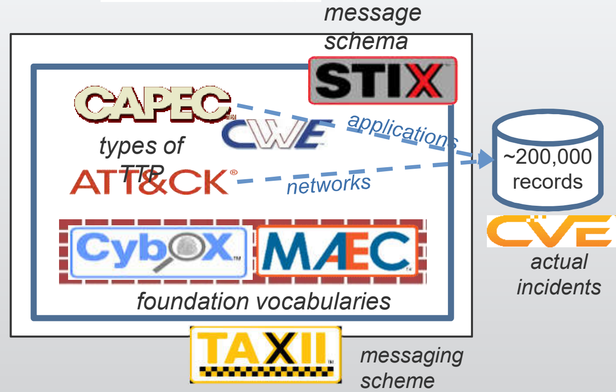


Formal Foundation and Multiple Standards

- Formal means the ontology has a mathematical foundation
  - Set theoretic and higher-order for classification
  - Four dimensional for continuity from past to present to possible futures
  - Mereologic to deal with parts and wholes
  - Mereotopologic to deal with boundaries and borders
- Many inter-related cyberspace data standards and Tbox sources





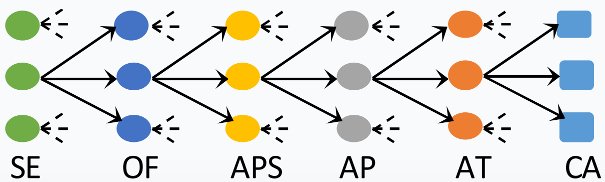


CAPEC™	Common Attack Pattern Enumeration and Classification*
ATT&CK™	Adversarial Tactics, Techniques & Common Knowledge
CWE™	Common Weakness Enumeration
CVE	Common Vulnerabilities and Exposures
CyboX™	Cyber Observable eXpression
STIX™	Structured Threat Information eXpression
TAXII™	Trusted Automated Exchange of Intelligence Information
MAEC™	Malware Attribute Enumeration and Characterization

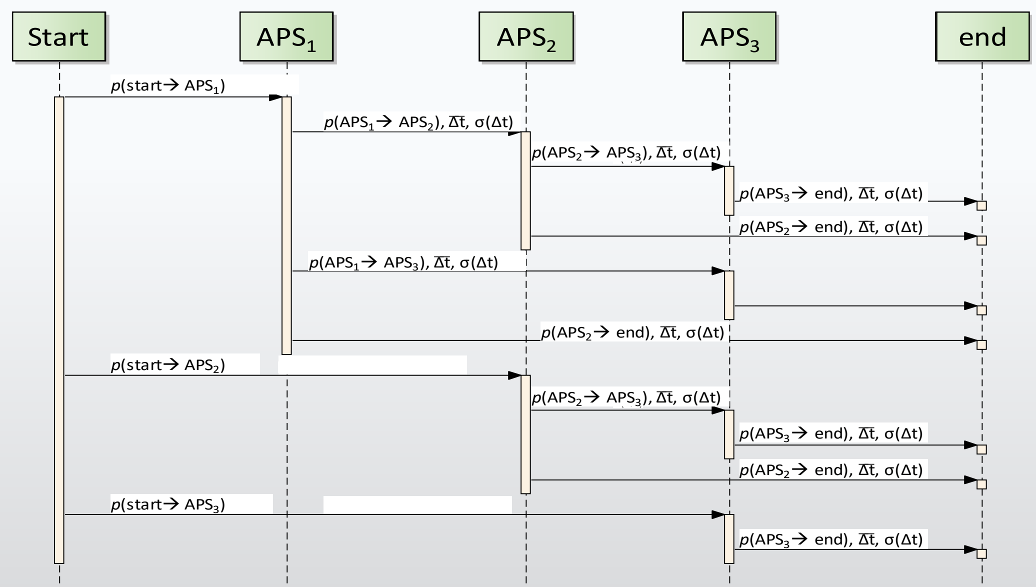
Cyber Electromagnetic Activity (CEMA) 2022

MAY 3-4
Belcamp, MD

CEMA Data Fusion

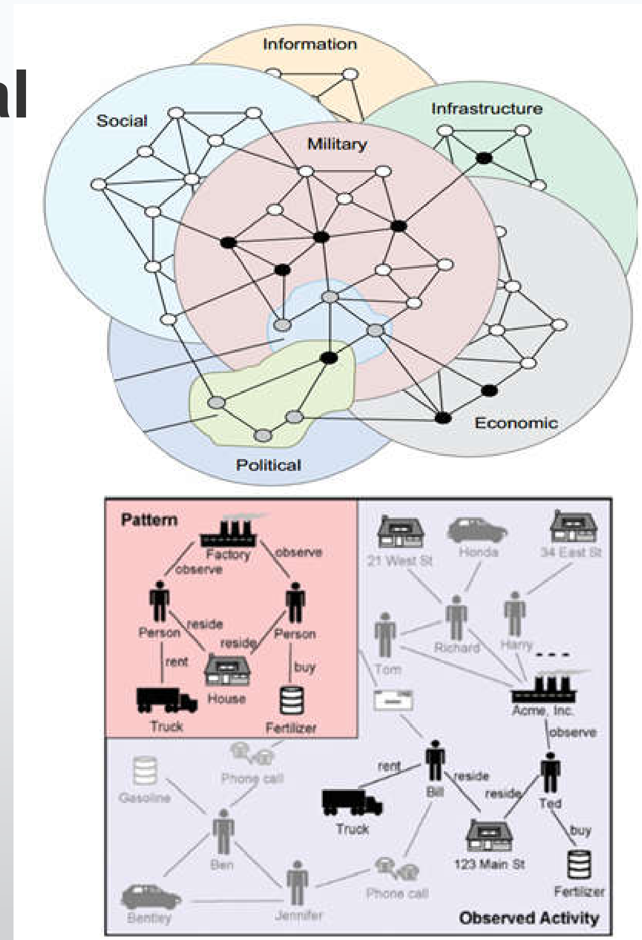


Legend:
SE Combat System Sensor Events
OF CAPEC Observations and Features
APS Attack Pattern Steps
AP Attack Pattern
AT Attacker Type
CA Candidate Attacker



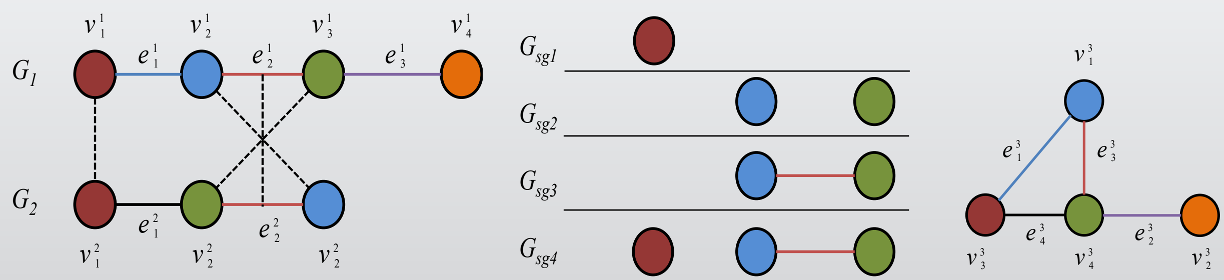
Directed Attributed Relational Graphs (DARG)

- Graphical-based analysis with nodal and edge-wise relationships represents layered data
- Cross-layer (graph) association and associated evidence-to-PIR/COP queries by graph-matching
- Bomb attack example shows template (pattern) and application to disparate data



Graph Association

- (A) G_1 and G_2, share some similarities
- (B) Common subgraphs between the two graphs
- (C) Maximum common subgraph (MCG)

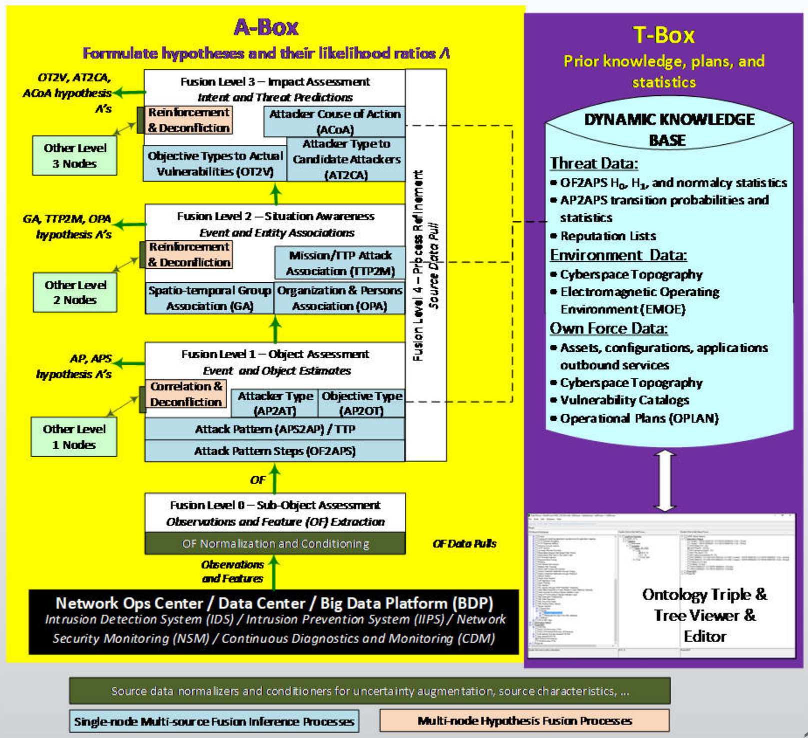


(A) (B) (C)

Cyber Electromagnetic Activity (CEMA) 2022
MAY 3-4
Belcamp, MD

CEMA Distributed Data Fusion

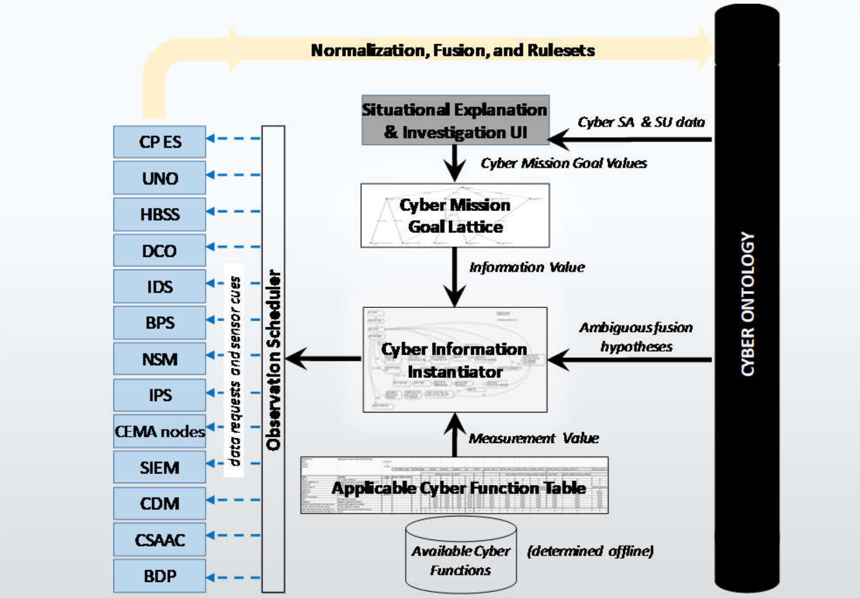
- T-Box on right:
  - Attack data
    - Patterns and their steps, a type of TTP
    - Known or suspected threats
  - Cyberspace topography and Electromagnetic Operating Environment (EMOE)
  - Ownforce data
    - Vulnerabilities
    - Plans
- A-Box on left: JDL levels for CEMA
  - Level 0: Normalize Observations and Features (OF) from many sources
  - Level 1, objects and events
    - Hypothesize Attack Pattern Steps (APS) and Attack Patterns
    - Infer Attacker Type and Objective Type
  - Level 2, associations and linkages
    - Spatio-temporal groups
    - Critical ownforce capability to AP
    - Missions from attack patterns
  - Level 3, predictions
    - Attacker type
    - Objectives to vulnerabilities
    - Attacker CoA
  - Multi-node at every level



Cyber Electromagnetic Activity (CEMA) 2022
MAY 3-4
Belcamp, MD

DDFRM-CEMA Resource Management

- *Information Based Sensor/Source Management (IBSM)*
- Level 4 data fusion process that is a holistic information satisficing solution
  - Transfer information not just data
  - Mission valued information
  - Maximize the probability of obtaining that information
  - Obtain the information in a timely manner
- *Situation Assessment Situation Information Expected Value (SIEV)* net measures information by the expected decrease in uncertainty in the Commander's Critical Information Requirements (CCIR) value such as to disambiguate fusion hypotheses
- Uses a situation *dependent lattice of mission goals* mission goals in the mathematical form of a lattice and then adjoin to each of the goals a computed mission value, we have a goal lattice and an ordering relation, considered to be is necessary for the accomplishment of
- Assign relative values to relevant information-gathering actions to maximize the *Expected Information Value Rate (EIVR)* - utilize the change in entropy as a measure of information
- Cues sensors to collect additional data (e.g., detailed logs) and pulls information from data sources (e.g., Big Data Platform) using *Applicable Function Table* that are impractical to push to the node (e.g., PCAPs)



Legend:

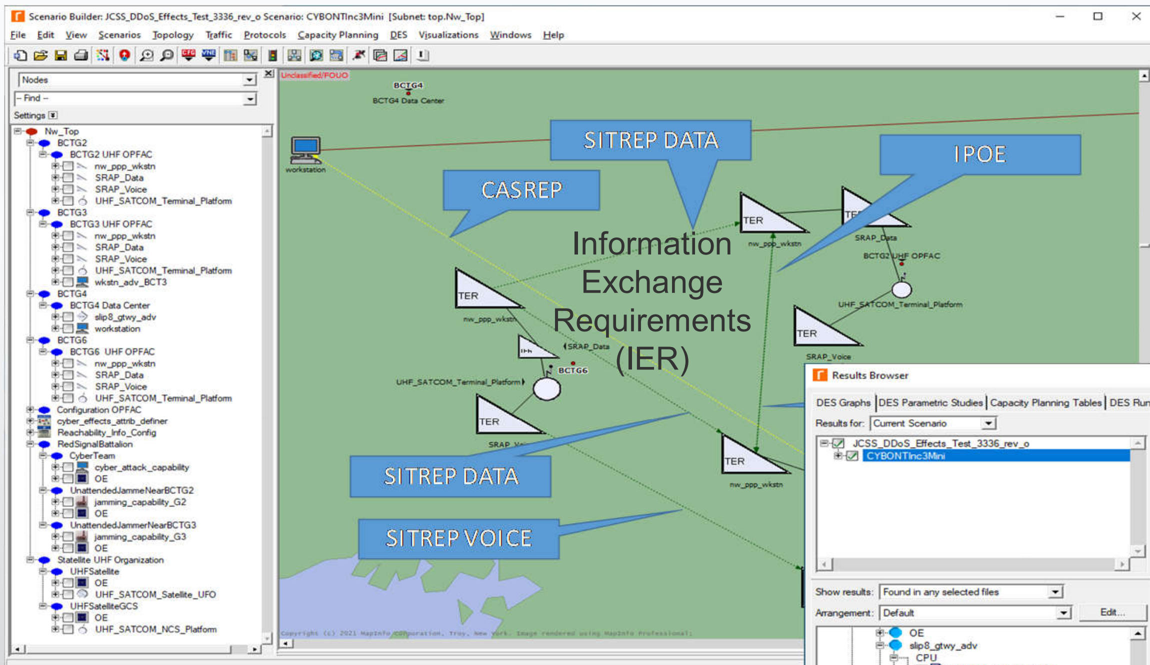
BDP	Big Data Platform	IDS	Intrusion Detection System
BPS	Boundary Proxy Service	IPS	Intrusion Protection System
DCO	Deployable DCO System	NSM	Network Security Monitoring
ES	Endpoint Security (e.g., HBSS)	SIEM	Security Information & Event Management Service
HBSS	NOSC Host Based Security Service	UAM	User Activity Monitoring
UNO	Unified NetOps	CSAAC	Cyber Situational Awareness Analytic Capabilities

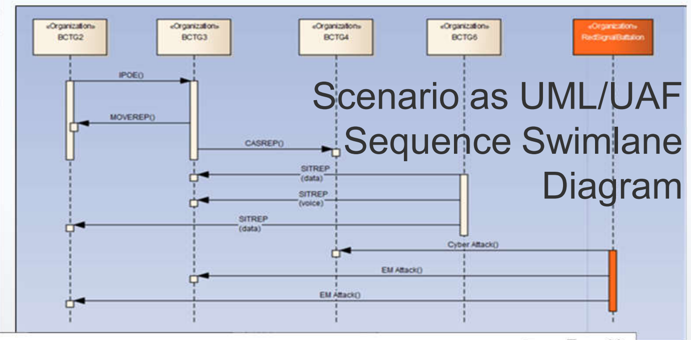
Information Exchange Requirements (IER)

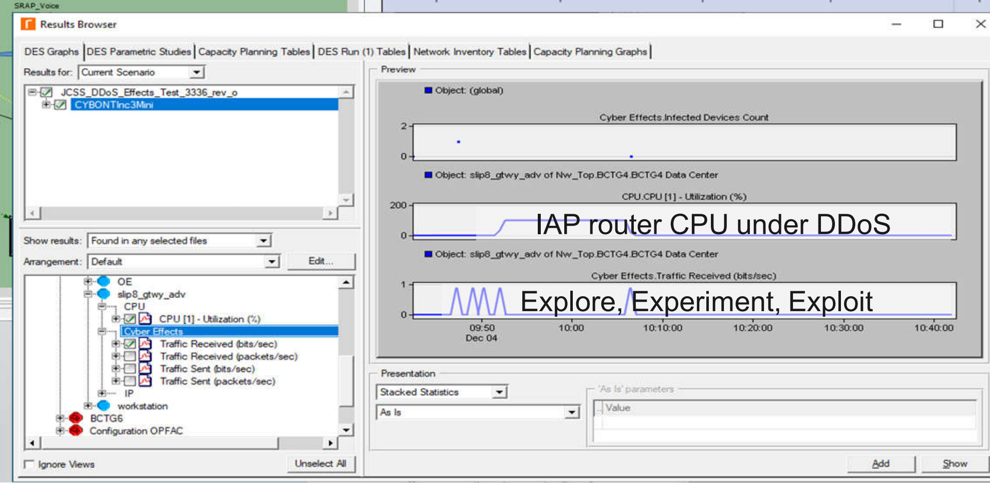
Coordinated CEMA Simulations for DDFRM Lab Testing

Cyber Electromagnetic Activity (CEMA) 2022

MAY 3-4
Belcamp, MD



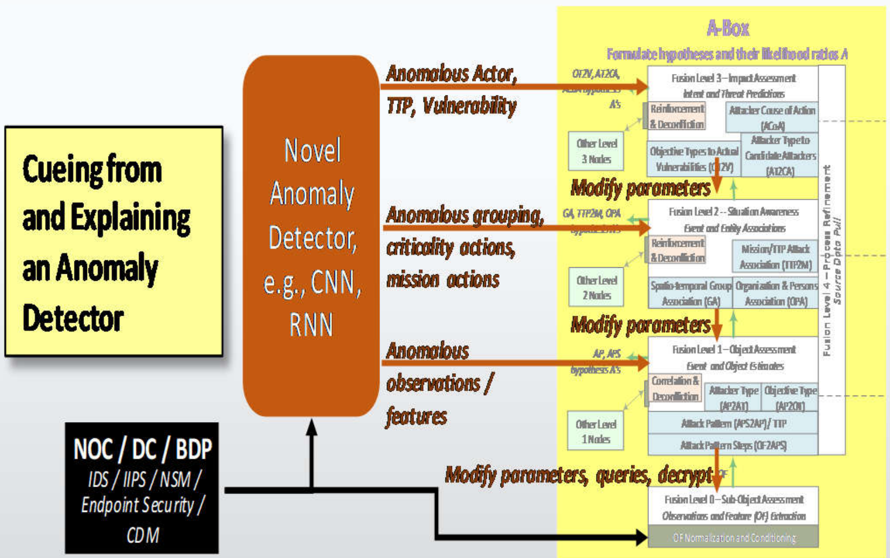




Joint Communications Systems Simulator (JCSS)

Leveraging New AI Technologies

- ***Cueing from and Explaining Anomaly Detector.*** The AI detects an anomaly but cannot understand or explain it. IBSM could pull Observations and Features and cue the DARG to see if weak hypotheses that could explain the anomaly could be strengthened. This would be an example of explainable AI.
- ***Automated Knowledge Base Statistical Learning***. In the first picture, the DF's knowledge base priors (e.g., $p(H_0)$, $p(H_1)$, normalcy statistics, attack pattern step transition probabilities and statistics) are learned in realtime by treating hypotheses confirmations or disconfirmations as accumulations as new samples. A Kalman-like filter could enable their adaptation for temporal drift or process changes over time using a social process.
- ***Automated Attack Pattern Learning and Correla***tion. Types of Observations and Features are clustered to form new provisional Attack Pattern Steps (pAPS). These pAPS and existing APS accumulate into new or variants of existing Attack Patterns (AP).
- ***Disambiguation with Deep Analytics.*** An assistant to the DF process could conduct deeper analysis of fusion hypotheses ambiguities. For example, it could use Power Spectral Densities (PSD) developed from the data lake to understand if there were spurious spectra in the knowledge base statistics that could separate the hypotheses.



References

- Data Fusion
  - Alan N. Steinberg, Christopher L. Bowman, Franklin E. White, "Revisions to the JDL data fusion model," Proc. SPIE 3719, Sensor Fusion: Architectures, Algorithms, and Applications III, (12 March 1999); https://doi.org/10.1117/12.341367
  - J. Llinas, C. Bowman, G. Rogova, A. Steinberg, E. Waltz, F.E. White, Revisiting the JDL data fusion model II, in: Proc. of the International Conference on Information Fusion, 2004, pp. 1218–1230.
  - J. Llinas, "A survey and analysis of frameworks and framework issues for information fusion applications," in Hybrid Artificial Intelligence Systems, ser. LNCS, M. Grana Romay, E. Corchado, and M. Garcia Sebastian, Eds., Springer Berlin Heidelberg, 2010, vol. 6076, pp. 14–23

- Formal Ontology
  - Sidor, T.; Four Dimensionalism; An Ontology of Persistence and Time; Oxford University Press; 2001
  - Smith, B.; "Mereotopology: A Theory of Parts and Boundaries", Data and Knowledge Engineering, 20 (1996),
  - "Church's Type Theory", Stanford Encyclopedia of Philosophy, https://plato.stanford.edu/entries/type-theory-church/
  - De Giacomo, G., Lenzerini, M., "TBox and ABox Reasoning in Expressive Description Logics", Proceedings of the 1996 International Workshop on Description Logics, October 1996

- Level 2 Behavior Fusion
  - T. Coffman, S. Greenblatt, and S. Marcus, "Graph-based technologies for intelligence analysis", Communications of the ACM, 47(3 March):45–47, 2004.
  - Sambhoos, K., Nagi, R., Sudit, M. and Stotz, A. "Enhancements to High Level Data Fusion using Graph Matching and State Space Search," Information Fusion, 2010, Vol. 11(4), pp. 351-364.
  - Gross, G., Nagi, R. and Sambhoos, K. "Soft Information, Dirty Graphs and Uncertainty Representation/Processing for Situation Understanding," 13th International Conference on Information Fusion, Edinburgh, Scotland, 26-29 July 2010.
  - Tauer,G., Nagi, R., Sudit, M.; The Graph Association Problem: Mathematical Models and a Lagrangian Heuristic; Published online in Wiley Online Library (wileyonlinelibrary.com); 2013
  - Gross, G.A., Nagi, R. and Sambhoos, K. "A Fuzzy Graph Matching Approach in Intelligence Analysis and Maintenance of Continuous Situational Awareness," Information Fusion, July 2014, Vol. 18, pp. 43-61.
  - Gross, G.A. and Nagi, R. "Precedence Tree Guided Search for the Efficient Identification of Multiple Situations of Interest – AND/OR Graph Matching," Information Fusion, January 2016, Vol. 27, pp. 240-254.
  - Ogaard, K., Roy, H., Kase, S., Nagi, R., Sambhoos, K. and Sudit, M. "Searching social networks for subgraph pattern occurrences," 2013 SPIE Defense, Security, and Sensing (SPIE, DSS 2013), Baltimore, MD, April-May 2013.
  - Gross, G., Nagi, R. and Sambhoos, K. "Continuous Preservation of Situational Awareness through Incremental/Stochastic Graphical Methods," 14th International Conference on Information Fusion, Chicago, IL, 26-29 July 2011.
  - Wang, Dong; Abdelzaher, Tarek; Kaplan, Lance.; Social Sensing Building Reliable Systems on Unreliable Data; Elsevier Science; 2015

- Resource Management
  - Hintz, K. J., Sensor Management and ISR, 2020, Artech House:Boston, 2020

Cyber Electromagnetic Activity (CEMA) 2022

ASSOCIATION OF OLD CROWS

MAY 3-4

Belcamp, MD

Questions?