Distributed Data Fusion and Resource Management for Cyberspace and Electromagnetic Activities

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

Todd Kingsbury
Silver Bullet Solutions, Inc.
Arlington,VA, U.S.A
todd.kingsbury@silverbulletinc.com

Ken Hintz
Perquire Research
Savanah, 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

ABSTRACT

Cyberspace and Electromagnetic Activities (CEMA) consist of cyberspace operations, electronic warfare, and electromagnetic spectrum management operations. Distributed Data Fusion and Resource Management for CEMA (DDFRM-CEMA) is an integrated estimation and sensor/source management process that has matured over a series of programs addressing the various functions that have ultimately been integrated into a complete analysis process. The CEMA Data Fusion (DF) Level 0-3 functions make inferences from CEMA sensor and source data to objects and events, develops linkages between them, and asserts predictions about them. The Resource Manager (RM) Level 4 DF function exploits an information-theoretic approach that optimizes data/information collection to satisfy layered Commander's Critical Information Requirements (CCIR) and disambiguate DF hypotheses. This process, called Information Based Sensor/Source Management (IBSM), measures information by the expected decrease in uncertainty in the value. It uses a "goal lattice" and sensor/source Applicable Function Table (AFT) to maximize the expected information value rate (EIVR) through sensor cues and source requests. This data-pull scheme is essential for CEMA DF where data-push is infeasible, e.g., pushing Packet Captures (PCAPs) would create multiply more. DDFRM-CEMA operations are made semantically consistent by a formal and extensible ontology that can go from CEMA modalities to organizational behaviors, intentions, and plans, and whose formal structure reinforces mathematically correct relationships. The ontology represents relationships (temporal, whole part, causality, etc.) with which to fuse attack patterns from sensed observations and extracted features. DDFRM-CEMA is considered a unique analytical toolkit/integrated estimation and action-taking process that offers distinctive features and benefits to complex problems in the CEMA problem spaces.

Keywords: cyberspace, CEMA, fusion, ontology, resource management, optimization, directed graphs, artificial intelligence, IBSM

1 OPERATOINAL CONCEPT AND RELEVANCE

In the early days of cyberspace, DoD, like all organizations, was on its own in detecting, assessing, and responding to threats. Today, the Cybersecurity and Infrastructure Security Agency (CISA), within the Department of Homeland Security, operates a warning system that relies on information sharing and partnerships with the private sector, other government agencies, and the intelligence community. For down-range units, United States Cyber Command (USCYBERCOM) provides deploying units a Cyber Mission Team (CMT) and a Cyber Protection Team (CPT), complete with cyber toolkits and mobile clouds that monitor CISA and other alerts and take action to fortify and/or remediate the unit if it may be vulnerable to the reported activities. However, in an all-out attack against a down-range unit, the national response may be too late or not at all under Denied, Disrupted, Intermittent, and Limited (DDIL) or Anti-Access Area Denial (A2/AD) conditions, localized network attack, coordinated enemy Cyber and Electromagnetic Activities (CEMA) [1], or attack against specialized military Internet of Things (IoT) / Supervisory Control and Data Acquisition (SCADA) equipment for which there is no civilian counterpart. Further, if the enemy is executing a coordinated multi-warfare attack, the CEMA component may be only a small part of the overall kill chain whose role and impact may not be immediately apparent, i.e., a clever adversary will execute various of the types of CEMA shown in Figure 1 such that each activity remains below an alert threshold but in a manner that, aggregated, is a significant threat. Hence the military has a requirement for organic enemy CEMA detection, awareness, and understanding in a multi-domain context.

The mission requirements call for a Data Fusion (DF) and Resource Management (RM) architecture and algorithms that can produce contextual hypotheses that can be integrated with other domains in realtime. This implies CEMA hypotheses in the all-domain ontology, with mathematically-principled hypotheses scores suitable for multi-modal (sensor) and multi-node association. Due to the relatively limited manning in tactical units, it must be highly automated and trustable. Because the enemy will be covert, the fusion must exhaust all sources that could reveal and disambiguate hypotheses but, due to the realities of network and communications limitations for forward units, must pull data selectively and optimally.

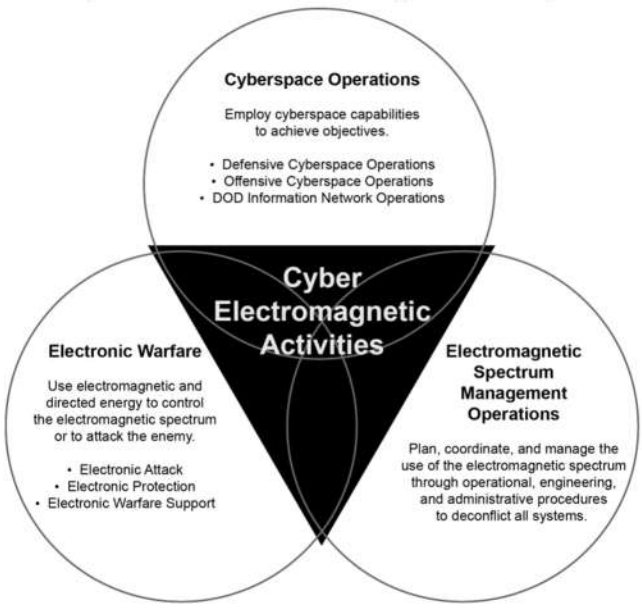

Figure 1. CEMA (from ref [1])

2 HIGH LEVEL DATA FUSION (DF) AND RESOURCE MANAGEMENT (RM) FRAMEWORKS

Core functions of command and control systems are DF and resource management and many tools conducting these functions have been developed that could be adapted for CEMA. At their core, DF processes are information-based *estimation* processes, directed at providing the best-possible mission-critical information to support various mission tasks and functions. (Expansion of the DF process model and its levels are described in [2].) Importantly, effective design of these processes ideally includes various runtime adaptation capabilities that adjust the DF processes to real-time contingencies needed to maintain various optimality criteria that are embedded in the overarching DF operations. These adaptive processes may include runtime control of certain resources that either support DF operations (such as adaptive sensor and source management tuned to optimizing DF estimation algorithms) or, if DF is the core information

subsystem, DF estimates may trigger actions on certain mission resources such as countermeasures. The system-boundary assessment for DF, a systems-engineering issue, will determine the extent of adaptive control-type processes and functions that the *DF framework* will have in any given application.

There has been a necessary progression of detection of adversary enemy CEMA from isolated, independent, and single-sensors evolving to federated, networked, integrated pattern matching to CEMA Tactics, Techniques, and Procedures (TTP). Associated with this sensor fusion problem is the inexorable increase in the quantity, quality, and diversity of sensors and sources about CEMA devices and software. A new application of explainable optimal information theory provides situational awareness having minimal uncertainty of predicted CEMA vulnerabilities given the implemented hardware, software, mitigations, and maneuvers. As an optimized process recording its own decisions, "why" means to improve the situational awareness as an explainable goal, and "how" means which architecture is proposed. The proposed architecture, evolving from a kill-chain system-of-systems approach, enables an optimization scheme that can arbitrate among the known evidence and information needs for detecting interdependent network and application CEMA-attack patterns and can arbitrate among the vulnerabilities and mitigations that are known to be applicable for a given mission use case or vignette.

We see CEMA requirements as very tactically-oriented and involved with balancing ISR, EW, and CEMA within missions. This would imply that DF processes should be associable to the various functions of the Kill Chain. DF functional support to full Kill Chain processes are as nominated in Figure 2 below, inspired by correlating DF functions (shown in orange boxes) to the six steps of the Joint Targeting Cycle [3]. The yellow boxes indicate functions having interdependencies with DF functions and in certain designs can be co-developed in a synergistic approach.

In broad terms, such DF capabilities need to support assessment of hostile *mission and intent*, develop *targeting knowledge* adequate to enable optimal *weapon assignment*, support *weapon operations* e.g., to possibly provide Electromagnetic (EM) maneuver or EW actions to weaponry, and as well to support Battle

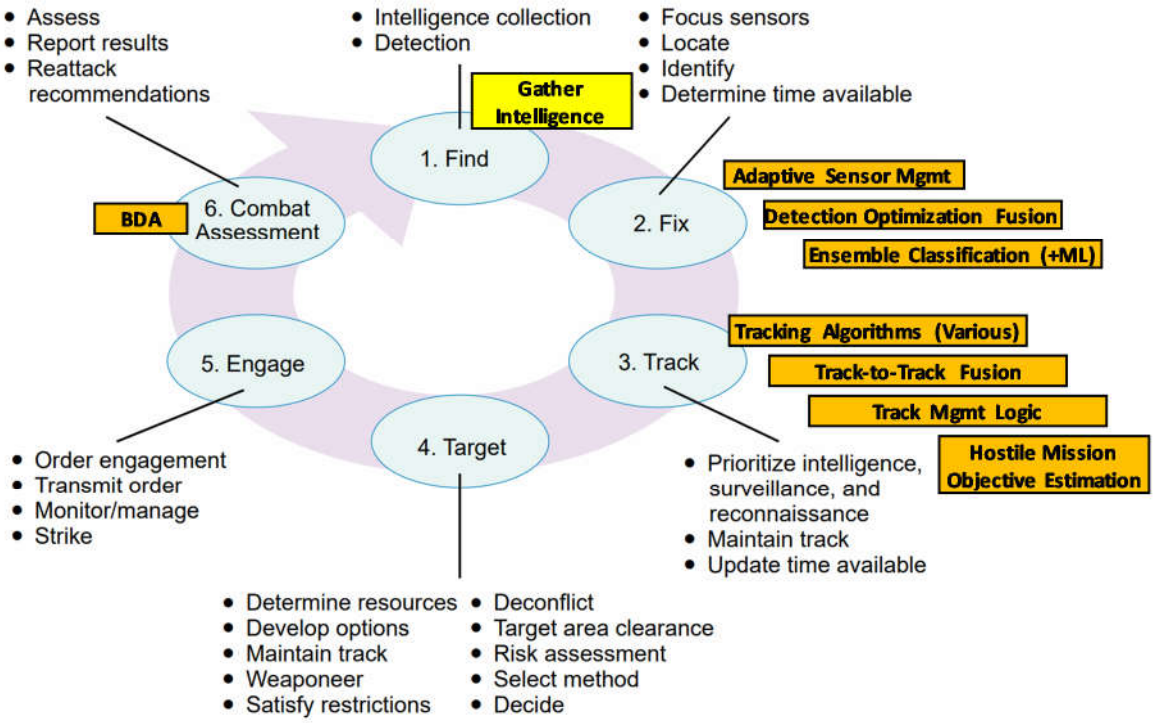

Figure 2. Functional Correlation of DF Functions to the Joint Targeting and Engagement Cycle (background from ref [3])

Damage Assessment (BDA) and possible re-targeting. Extended capabilities of these types will require not only a layered DF framework but one that is adaptive in various ways, and managed in a hierarchical scheme, focused primarily on achieving mission effectiveness. Thus, we are proposing a DF framework that has *three fusion layers* that enable layered estimation for: operational mission situation assessment, target knowledge elaboration, and weapon employment and BDA support.

Our DF framework for *precision targeting* mission applications is shown in Figure 3. Meta-control of these layered fusion processes is managed by a layered scheme of adaptive control functions as shown in Figure 3. At the top or mission level, a *mission process controller* (purple box [1]), that manages the interplay of the layered *fusion processes* -- boxes [A], [B], and [C] shown in Figure 3. Exploitation of fusion process interdependencies is a topic that our team has studied previously (e.g., [4]) and has developed frameworks for (e.g., [5]); this is an important factor affecting adaptive designs. *Layered process control* also involves *adaptive sensor management* that exploits any agilities in ISR sensors and sources for not only space-time ("pointing") management but also any other sensor controls that improves organic collection of tactical situational data. As sensor / source data is collected, it needs to be intelligently fed to the correct fusion layer; this is enabled by an input manager controller. Thus, our framework has two other control loops -- purple boxes [2] and [3] that manage sensor operations and data feed operations for ingestion, storage, and processing of sensor data. Notice too that the layered framework should be integrated with any/all mission planning functions as shown in the green boxes of Figure 3. Thus, the framework is very hospitable to such future enhancement.

Throughout this framework, we see a wide variety of possible insertion points for artificial intelligence (AI), machine learning (ML), and/or deep learning (DL) technologies. Among these could be AI/ML/DL for Data Association (DA) functions (e.g., see [6]), AI/ML/DL techniques for *ensemble classification* (e.g., see [7], [8], and [9]), and even for target tracking operations (e.g., see [10] and [11]). Our view here however recommends caution in insertion or exploitation of AI/ML/DL technologies, as CEMA missions have properties that can constrain the use of these technologies such as:

- High OPTEMPO that constrains real-time explanation of opaque outputs to CEMA operators, as "explanation" capabilities are proving crucial to effective use of AI/ML/DL [12]
- Specialized testing and evaluation (T&E) during development that assures no or very limited occurrences of unintended consequences

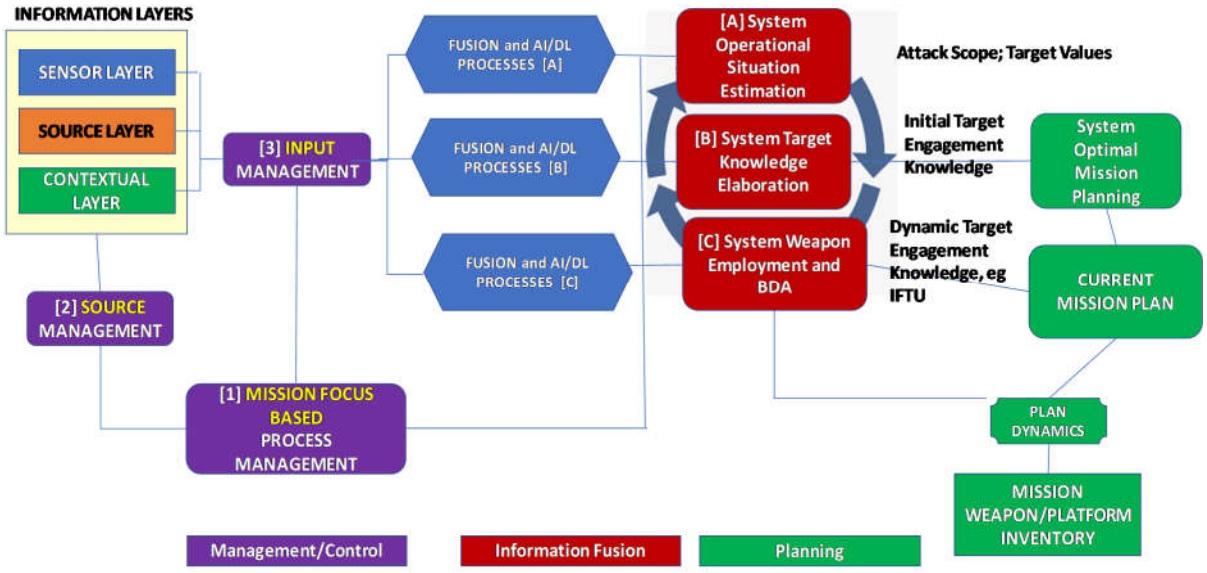

Figure 3. Conceptual/Functional Layered Fusion Framework

- Assured Rule of Engagement (ROE) - compliant behaviors that are always quantifiable, recordable, and hence repeatable processes

We point these out in the context of good systems engineering and careful tradeoffs that we see as important for use of these methods.

3 DDFRM-CEMA ARCHITECTURE

With these general DF architecture principles in mind, the DDFRM-CEMA architecture shown in Figure 4 was engineered as a partition of the various functions into components which are required to manage the sensor and data source resources and to log the explanation of why each management decision was made. It also enables machine learning applied to assist the internal operation in a Human-on-the-Loop (HOL) system or applied to training an attack pattern recognizing convolutional neural network.

Its major components are:

- CEMA Ontology. DF and RM operate on a formal and extensible ontology that can go from CEMA modalities to real-world organizational behaviors, intents, and plans. It was developed under international defense cooperation with a formal structure that enforces mathematically correct relationships. The ontology represents relationships (temporal, whole part, causality, etc.) with which to fuse attack patterns from sensed attack steps or phases. It employs a super-subtype (SST) tree of a-priori common types of CEMA techniques that is used in generating DF hypotheses and another SST tree of CEMA techniques indicating vulnerabilities and mitigations and maneuvers.
- Distributed Data Fusion. CEMA DF uses Directed Acyclic Relationship Graphs (DARG) to make inferences (hypotheses and likelihood ratios) from sensor and data sources to objects and events and linkages-between and predictions-about them. An actor template tool based on the CEMA ontology is used to predict attack behavior candidates. Instantiated A-Box graphs represent actors in CEMA

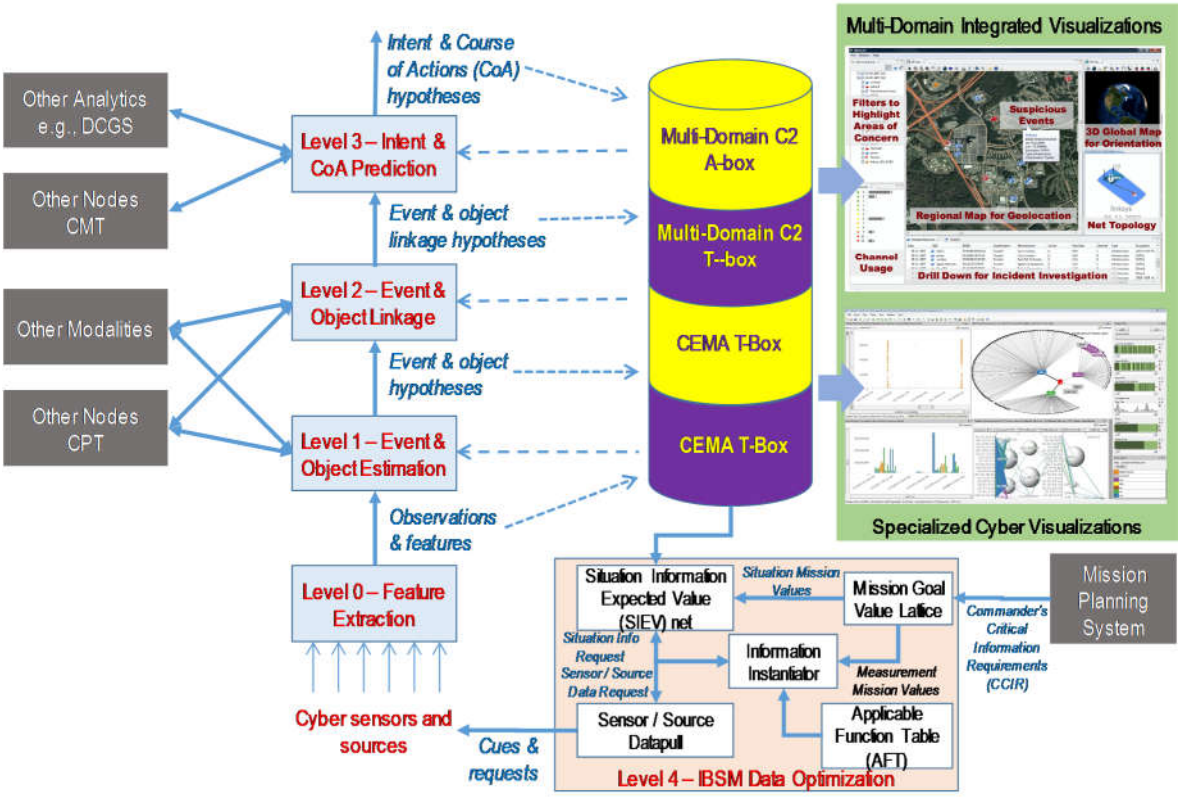

Figure 4. DDFRM-CEMA Architecture Overview

hypotheses as a Bayesian situational network containing candidate threats and behaviors and their associated likelihood ratios.

- Resource Management. Information Based Sensor/Source Management (IBSM), a resource optimization technology, adapts the DF system to CEMA sensors and data sources using a situation dependent lattice of mission goals valuing optimal information-gathering observations and indicators. It effectively combines competing, independent, orthogonal vulnerabilities, mitigations, and maneuvers into a situational awareness value for tasking competing sensors and data sources. IBSM enables a data-pull data scheme, very effective for large volume CEMA sensor datasets that can be impractical to push, e.g., PCAPs – pushing PCAPs creates more PCAPs.

3.1 CEMA Ontology

Involved in this synthesis challenge in the case of CEMA analytics are the many data layers typically considered in CEMA contexts, for example, as described in Joint Pub 2-03 [13] and shown in Fig. 1. As can be seen, geospatial data is prevalent in the lower layers while the upper layers tend to be textual. Other diagrams Joint Pub 2-03 Figures IV-4 and in Joint Pub 3-0 [14Figure IV-1 illustrate the layers from a real-world or ontological perspective. Entities in these upper layers often are from categories drawn from the PMESII-T [15], DIME [16], and/or ASCOPE [17] taxonomies. These layers and taxonomies are interrelated in complex ways (see, e.g., [18, 19]).

It is important to note that these data layers are "disparate", meaning that they are essentially different in kind and thus they do not easily allow comparison or synthesis. Cyberspace introduces additional layers, whether ISO 7-layer or logical / personal / supervisory layers. There are three major challenges to be overcome in achieving efficient and effective synthesis of these data. First, operating on the raw, disparate data, is an ***alignment*** process that normalizes all data to a common reference. This process can involve several steps from coordinate conversions to data translations, uncertainty characterization, and normalization, as well as developing an ontology concordance that ultimately prepares the data for subsequent operations. The output of these operations is normalized data grounded in a common reference frame.

The next process of ***association*** addresses the challenge of associating the still-disparate but normalized data so that inter-layer associative relevance and relations can be computed. The output here results in inter-layer associations among the data. At this point, all of the data has been operated on to create a complete evidential picture of the operational domain. The next algorithm set are ***exploitation*** algorithms that allow

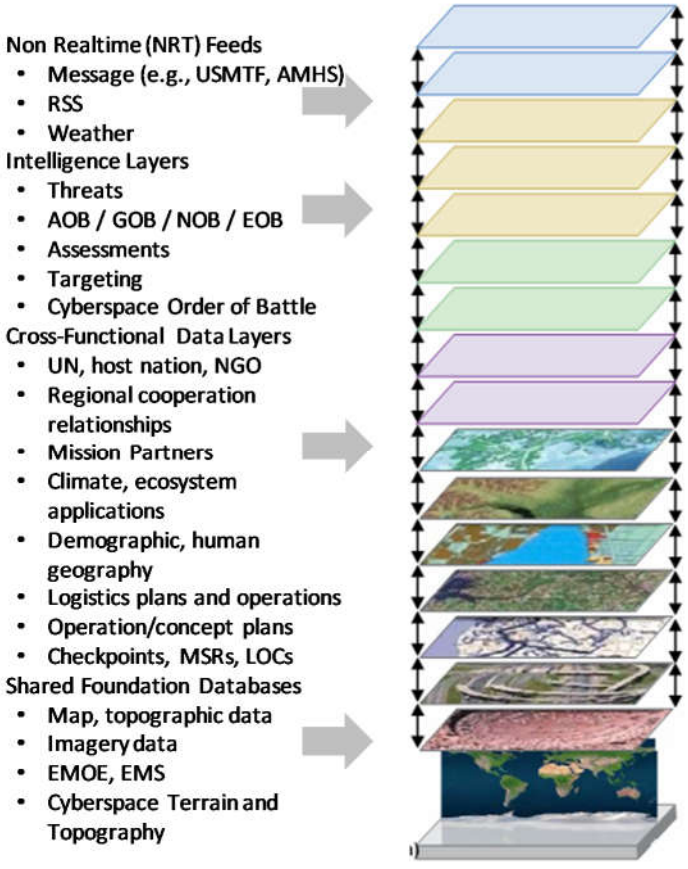

Figure 5. Geospatial Intelligence in Joint Operations (adapted from ref [13])

C2 and tactically-significant queries to be posed to this integrated evidence in order to extract/assess the existence of critical situational or CCIR inferable from the composite evidence.

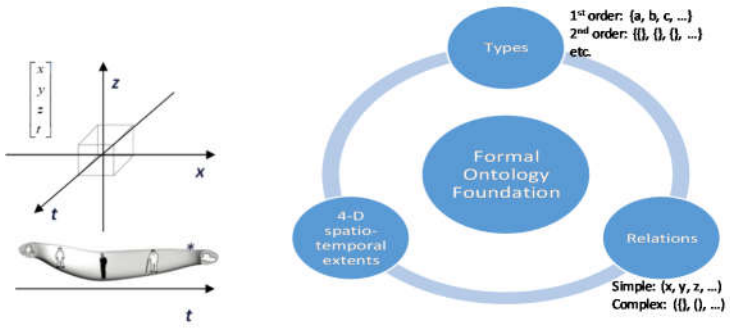

Figure 6. Foundation Ontology's Three Principal Things

An ontology or data model represents the concepts in these layers and inter-relates them. What ontology can add over an everyday data model is formal foundational and common pattern layers. Formal means the CEMA ontology has a mathematical foundation as illustrated in Figure 6. Our CEMA ontology implements high order type theory, is four-dimensional [20], and mereotopologic [21]. It is extensional, using physical existence as its criterion for identity. Extensional ontology is well suited to managing change over time and identifying elements with a degree of precision that is not possible using names alone. For DF, this supports re-discovery of lost tracks and representation of their evolution over time including prediction of possible future states.

The CEMA ontology links cyberspace data standards shown in Figure 7 at the lower layers to behavioral patterns at the PMESSI-T, DIME, or ASCOPE ontology layers.

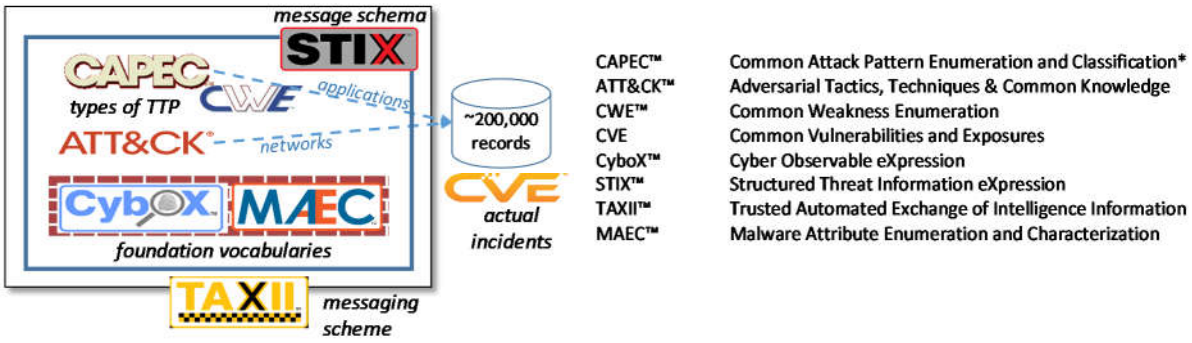

Figure 7. Examples of Cyberspace Data Schema, Reference Standards, and Message Formats

3.2 CEMA Distributed Data Fusion

DF's role in DDFRM-CEMA is as a hypothesis generator and rigorous mathematical function service within a larger CEMA data management and C4ISR system. The DF portion of DDFRM-CEMA produces indications and warnings of CEMA attack behavior hypotheses to support CEMA situational understanding (SU), Offensive Cyberspace Operations (OCO) planning, and Defensive Cyberspace Operations (DCO) responses. It is architected following the Joint Directors of Laboratories (JDL) fusion levels, and uses formal ontology for the T-Box (types) and A-Box (actuals). It computes likelihood ratios of attack behavior hypotheses. Inference links can be visualized in a graph database tool that allows customized viewing tailored to operator requirements. The likelihood ratios can be thresholded to give operators control over display clutter. It would fit in a hybrid Deep Learning (DL) architecture as a bootstrap trainer, results validator against adversarial AI, as an explainer, or for rapid data triage.

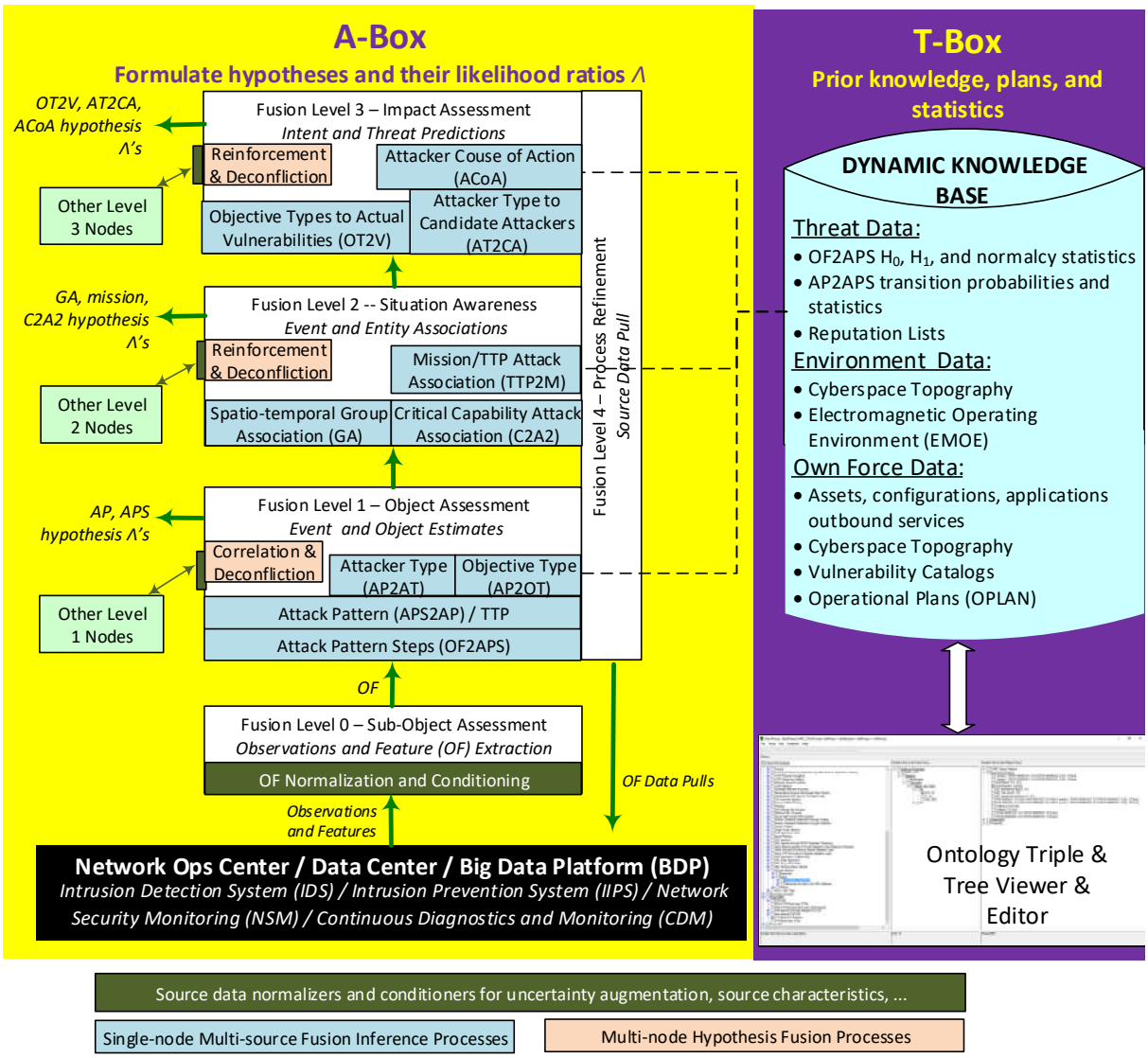

Figure 8. JDL Fusion Levels Focusing on CEMA

The JDL fusion levels focusing-on CEMA are shown in Figure 8. The principal type of inference in CEMA DF is Directed Attributed Relational Graphs (DARG) and associated graph association methods (see, e.g., [22, 23, 24]) operating off the CEMA T-Box ontology. Graphical-based analysis views the various layers in the CEMA data as graphs with nodal and edge-wise relationships. Figure 9 illustrates the application to the multiple geospatial data layers. In the upper part of the figure is a PMESII-T diagram from Joint Pub 3-0 showing that the disparate kinds of data, or layers, can have linkages. The lower part of the figure is an illustration of how this is done in a DARG. It shows the associable observed activity of two human nodes to a truck, fertilizer, and factory data, matches a template pattern (query) for a bomb attack. One way to think of DARGs is as enhanced 1st order type ontologies for which there is considerable formal foundation, e.g., [25]. The DARG template is equivalent to a 1st order type pattern, expressible in Descriptive Logic as

a "terminological component" (T-Box) in a knowledge base [26]. The DARG evidential data (lower and right part of Figure 9) is the assertion component" (A-Box). A DARG could be represented in web ontology language (OWL) with properties expressing the DARG's attributes. Existing DARG software was developed under Multidisciplinary University Research Initiative (MURI). DARG takes the next step in this AI state-of-practice, not just enabling representation of multi-layered data, but also implementing algorithms for multi-layer graph association and query-matching to associated evidential data [27]. The analytical processes involve representation of layered data, cross-layer (graph) association, and associated evidence-to-CCIR queries by graph-matching. In recent work, an inexact subgraph matching algorithm was developed as a variation of the subgraph isomorphism approach for situation assessment [28, 29, 30, 31]. This procedure can be enhanced to represent inaccurate observations or data estimates, and inaccurate structural representations of a state of interest, thus accounting for the various uncertainties in multilayer data. Various probabilistic and possibilistic uncertainty representations, transformations between representations and methods for establishing similarities between representations have been assessed.

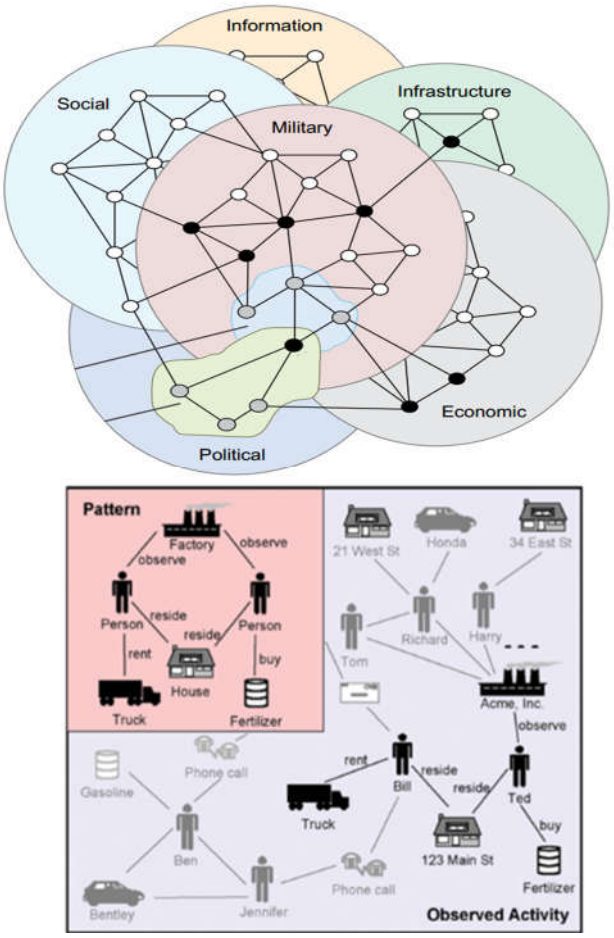

Figure 9. Template Graph Association across Disparate Data (top from ref [14])

In Figure 10 we discuss a simple graph association example where two DARGs G_1 and G_2, share some similarities (common nodes and relationships (arcs)); Figure 10 (B) shows the common subgraphs between the two graphs. The last one G_{sg4} is defined as the "maximum common subgraph (MCG)". Once we identify the MCG, we can synthesize the information in the two graphs as in Figure 10 (C). Identifying the MCG is a challenging problem, especially when the elemental nodes don't match perfectly (as shown by unique colors in Figure 10.) We are working on new methods for the fast association of graphs and build on our considerable past work in these complex technical areas.

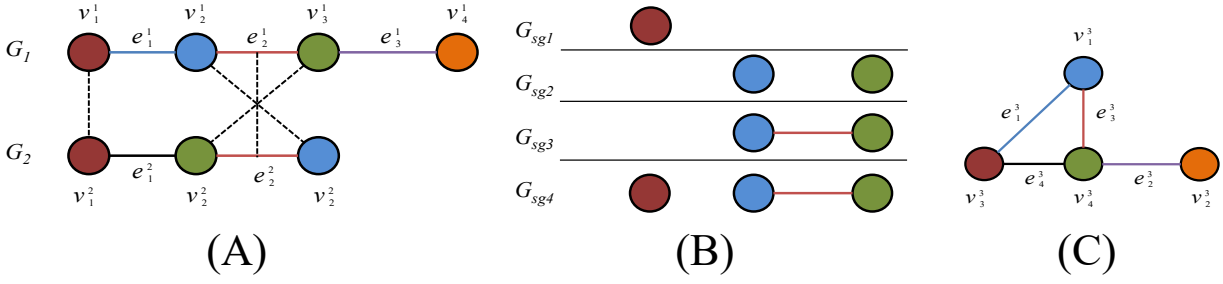

Figure 10. Graph Association: (A) Two graphs G1 and G2; (B) Common Graphs; (C) Merged Graph (from ref [27])

3.3 DDFRM-CEMA Resource Management

The scheme for RM is called Information Based Sensor/Source Management (IBSM). IBSM is an innovative one-of-a-kind holistic information satisficing solution to multi-platform, heterogeneous, and real-time data and source management. As a Level 4 DF process, IBSM measures information by the expected decrease in uncertainty in the CCIR value and the time to acquire the information. As shown in Figure 11, IBSM adapts the DDFRM-CEMA system to the situation and sensor network using a situation dependent lattice of information goals -- such as to disambiguate fusion hypotheses -- against optimal information-gathering actions. A key element of the IBSM adaptation process design is a "goal lattice" which is initialized with multiple relative mission goals. It is closed loop, indirect, and achieves context sensitive control through the use of interacting, mission-oriented multi-goal lattice with human-on-the-loop (HOL) that can algorithmically arbitrate across competing goals for optimal control of data and information sources. IBSM translates changing information needs and goals into sensor and source requests to maximize the Expected Information Value Rate (EIVR). IBSM cues sensors to collect additional data (e.g., detailed logs) and pulls information from data sources (e.g., Big Data Platform) that could be impractical to push to the node (e.g., PCAPs).

The resulting system is predicated on viewing sensors (including data/information sources) as an input channel to a probabilistic model of the world. While Shannon showed how to encode channel data, he was notably indifferent about what was sent through the channel. IBSM assumes that the individual sensors are operating locally as part of a large data enterprise and that the information (data with value) through the

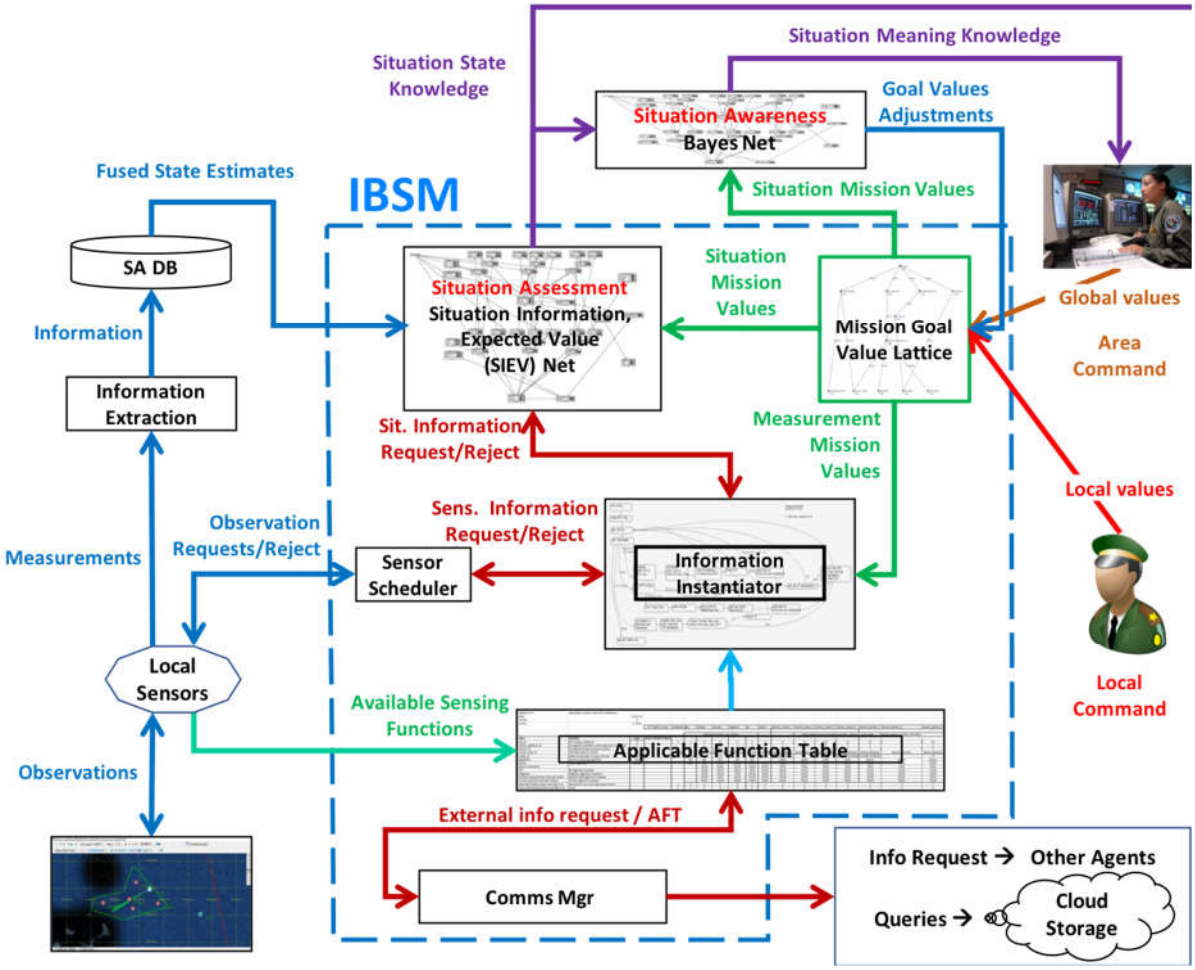

Figure 11 Information Based Sensor/source Management (IBSM) block diagram.

channel can be maximized by deciding what data should be acquired. In this context, information is measured by the expected decrease in uncertainty in our situational assessment weighted by its mission value and the time to acquire the information of potential adversary CEMA.

The IBSM scheme has been extensively studied and has been selectively applied in research programs [32].

4 SUMMARY AND NEXT STEPS

Parts of the DDFRM-CEMA have been developed under various projects so the software is research grade and not integrated as a system described herein. The team is looking for opportunities to productionize and integrate the DDFRM-CEMA components. As well, there are several enhancements we have thought about, illustrated in Figure 12.

a. Automated Knowledge Base Statistical Learning. In the first picture, the DF's knowledge base priors (e.g., p(H0), p(H1), normalcy statistics, attack pattern step transition probabilities and statistics) are learned and adapted 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 social process models akin to process models of maneuvering aircraft..

b. Automated Attack Pattern Learning and Correlation. 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).

c. Cueing from and Explaining Anomaly Detec. 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.

d. 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.

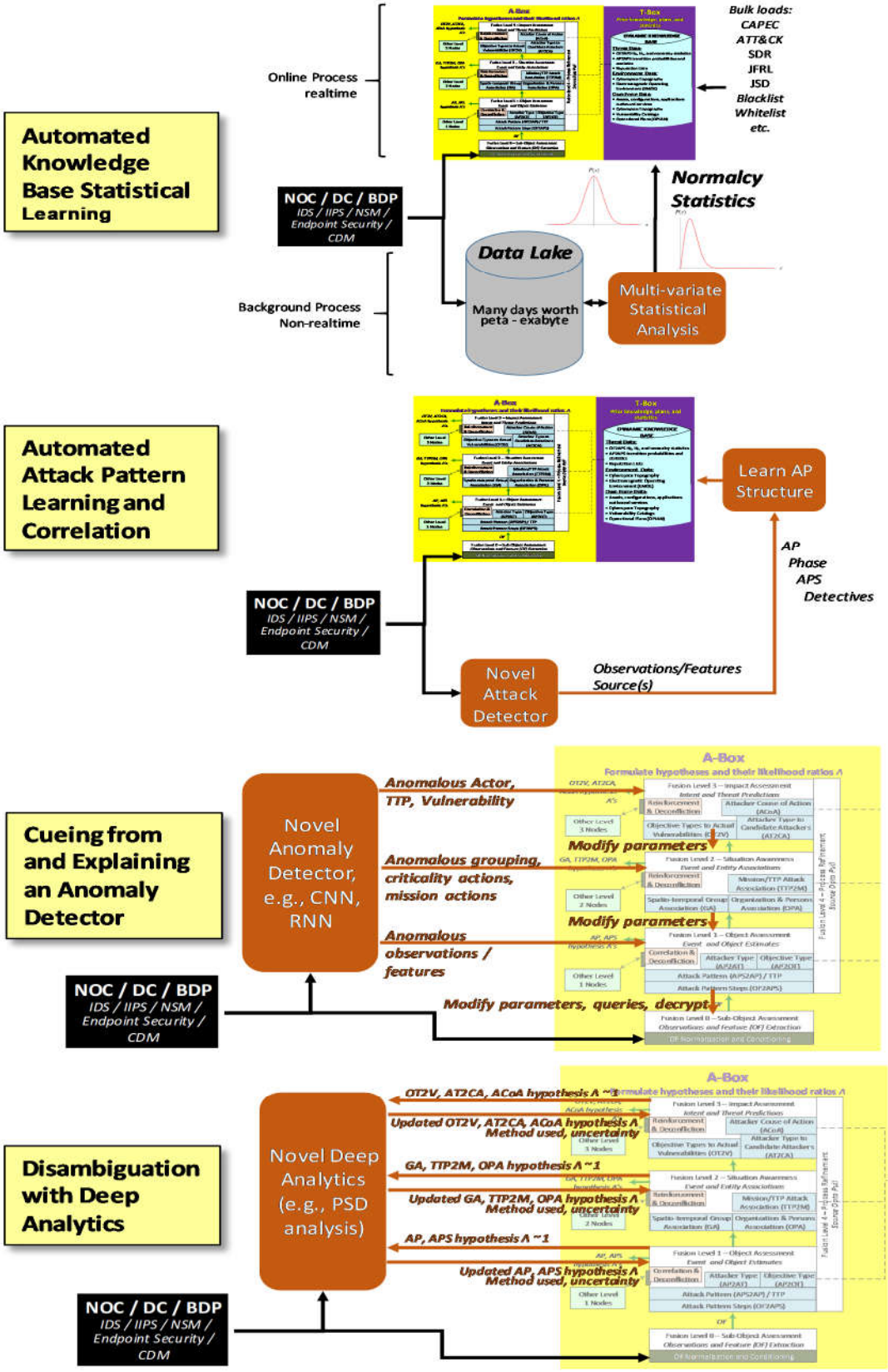

Figure 12. Ideas for further work

5 GLOSSARY

A2/AD	Anti-Access Area Denial
AMHS	Automated Message Handling System
AOB	Air Order of Battle
ATT&CK™	Adversarial Tactics, Techniques & Common Knowledge (ATT&CK)
CAPEC™	Common Attack Pattern Enumeration and Classification*
CCIR	Commander's Critical Information Requirements
CISA	Cybersecurity and Infrastructure Security Agency
CMT	Cyber Mission Team
COP	Common Operational Picture
CPT	Cyber Protection Team
CVE	Common Vulnerabilities and Exposures
CWE™	Common Weakness Enumeration
CyboX™	Cyber Observable eXpression
DCGS	Distributed Common Ground Station
DDIL	Denied, Disrupted, Intermittent, and Limited
EMOE	Electromagnetic Operating Environment
EMS	Electromagnetic Spectrum
EOB	Electronic Order of Battle
GOB	Ground Order of Battle
IFTU	In-Flight Target Update
JFRL	Joint Frequency Restrictions List
JSD	Joint Spectrum Database
LOC	Line of Communication
MAEC™	Malware Attribute Enumeration and Characterization
MSR	Main Supply Route
NGO	Non-Governmental Organization
NOB	Naval Order of Battle
PCAP	Packet Capture
SDR	Spectrum Data Registry
SST	Super-SubType
STIX™	Structured Threat Information eXpression
TAXII™	Trusted Automated Exchange of Intelligence Information
USMTF	United States Message Text Format

6 REFERENCES

[1] Department of the Army, FM 3-38, Cyber Electromagnetic Activities, February 2014.
[2] 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
[3] Joint Publication 3-60, Joint Targeting, 28 September 2018
[4] 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.
[5] 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 Se- ˜ bastian, Eds., Springer Berlin Heidelberg, 2010, vol. 6076, pp. 14–23
[6] P. Emami, P. M. Pardalos, L. Elefteriadou, and S. Ranka, "Machine Learning Methods for Solving Assignment Problems in MultiTarget Tracking," vol. 1, no. 1, pp. 1–35, 2018.
[7] Blasch, E., et al, Automatic machine learning for target recognition, Proc. SPIE 10988, Automatic Target Recognition XXIX, 109880L (14 May 2019

[8] M. Ponti, “Combining classifiers: From the creation of ensembles to the decision fusion,” in Proc. 24th SIBGRAPI Conf. Graph. Patterns Images Tuts. (SIBGRAPI-T), Alagoas, Brazil, 2011, pp. 1–10.
[9] S. Asmita and K. Shukla, "Review on the Architecture, Algorithm and Fusion Strategies in Ensemble Learning," International Journal of Computer Applications, vol. 108, 2014.
[10] A. Milan, S. H. Rezatofighi, A. Dick, I. Reid, and K. Schindler. Online multi-target tracking using recurrent neural networks. In AAAI, February 2017.
[11] Rosello, P and Kochendorfer, M., Multi-Agent Reinforcement Learning for Multi-Object Tracking, AAMAS 2018, July 10-15, 2018, Stockholm, Sweden
[12] Amina Adadi and Mohammed Berrada. 2018. Peeking inside the black-box: A survey on Explainable Artificial Intelligence (XAI). IEEE Access (2018).
[13] Joint Publication 2-03; Geospatial Intelligence in Joint Operations; 5 July, 2017
[14] Joint Publication 3-0, Joint Operations, 22 October, 2018
[15] Political, Military, Economic, Social, Information, Infrastructure, Physical Environment, and Time (PMESII-T) as defined in Operational Environment and Army Learning, TC 7-102, HQDA, 2014
[16] Diplomatic, Information, Military, and Economic (DIME)
[17] Areas, Structures, Capabilities, Organization, People and Events (ASCOPE)
[18] Hillson, R., “The DIME/PMESII Model Suite Requirements Project”, *2009 Naval Research Laboratory (NRL) Review*
[19] “Comparative Systems Analysis Framework and Thinking Tools”, *MISO Program Design and Assessments Course*, B Company, 6TH Battalion, 2ND SWTG (A), Fort Bragg
[20] Sidor, T.; Four Dimensionalism; An Ontology of Persistence and Time; Oxford University Press; 2001
[21] Smith, B.; “Mereotopology: A Theory of Parts and Boundaries”, Data and Knowledge Engineering, 20 (1996),
[22] T. Coffman, S. Greenblatt, and S. Marcus, “Graph-based technologies for intelligence analysis”, *Communications of the ACM*, 47(3 March):45–47, 2004.
[23] 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.
[24] 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.
[25] “Church’s Type Theory”, *Stanford Encyclopedia of Philosophy*, https://plato.stanford.edu/entries/type-theory-church/
[26] De Giacomo, G., Lenzerini, M., “TBox and ABox Reasoning in Expressive Description Logics”, *Proceedings of the 1996 International Workshop on Description Logics*, October 1996
[27] 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
[28] 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.
[29] 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.
[30] 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.
[31] 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.
[32] Hintz, K. J., Sensor Management and ISR, 2020, Artech House:Boston, 2020