18th International Conference on Information Fusion
Washington, DC - July 6-9, 2015

Situation/Threat Context Assessment

Erik P. Blasch
Air Force Research Laboratory
Rome, NY, 13441
erik.blasch@gmail.com

Steven A. Israel
Raytheon
Chantilly, VA, 20151
steve.israel@hotmail.com

***Abstract*— *There is a debate within the information fusion community whether situation and threat assessment (SA/TA) are separate as called out in the Joint Directors of the Lab (JDL) or interlinked in the Data Fusion Information Group (DFIG) Model. Situation assessment seeks a geospatial and temporal acknowledgement of the environment while threat assessment determines the impacts from the situation. Three types of impacts exist: entities (e.g., objects), environments (e.g. natural disasters), and relationships (interactions among entities). While object assessment can be determined from Bayes and/or evidential reasoning, it is also extended to threat assessment through a prior effects and world modeling. In this paper, we bring together the discussions of context as related to the discussion on SA/TA contextual analysis. While it is inherent that context plays a role in TA; we seek to highlight some of the assumptions, difficulties, and needs for TA – most notably stemming from requirements for sensor, user, and mission (SUM) management. SA and TA can be separate, linked, or serial, depending on the circumstance. An example is presented that highlights the need for context assessment in threat analysis as related to the changing situation.*

Keywords: *Information Fusion, Level 5 User Refinement, High-Level Information Fusion, Situation Assessment, Threat Assessment*

I. INTRODUCTION

A threat is an assessment that an individual or group has the potential to cause harm to specific entity or entities. Threat assessment, coupled with situation assessment, has three parameters: intent, capacity, and knowledge [1]. These parameters stem from context as shown in Figure 1, such as terrain gathered from imaging sensors. Contextual information refines the estimates of object, situation, and threat analysis and supports user refinement of the situation. One example of the user-threat continuum for context is the design relationship including ground sampling distance (GSD) and field of view (FOV) for the National Imagery Interpretability Rating Scale (NIIRS) [2, 3] which highlights the need for situation awareness metrics [4].

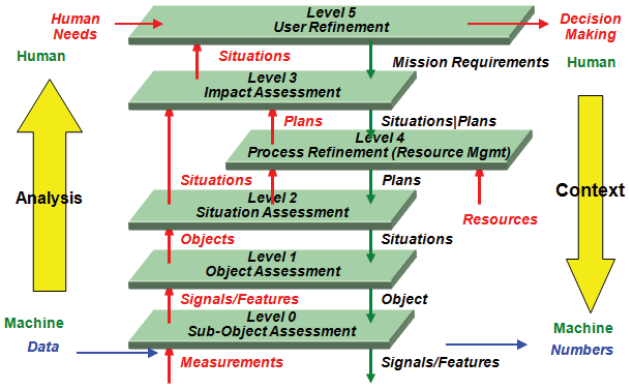

Figure 1 – Information Fusion Levels

Threat assessment (Level 3) can include actors (e.g., drug trafficking), relations (e.g., organized crime), weapons, and information warfare [5]. Non-national actors pose difficult contextual threats as 1) there is no identifiable location; 2) they maintain no persistent doctrine; and 3) they can attack different political, financial, cyber, and/or cultural domains, when their opportunity for success is greatest [6]. One example of a terrorist event is the bombing during the 2013 Boston Marathon. The bomber's intent was to destabilize the public trust. The bomber's capacity was small amount of funds and two individuals. The bomber's technical knowledge was in home-made explosives and the operational knowledge of the crowd movement during the marathon to maximize their impact. By not addressing SA/TA assumptions can lead to errors impacting decision making.

The rest of the paper is as follows. Sect. II defines the lexicon for describing threats. Sect. III describes common elements of threat, their impacts on decision supports systems, and a series of assumptions. Sect. IV provides example of how the developer assumptions can be quantified using evidence theory. Sect. V provides conclusions.

II. DEFINING THREATS

To identify the threat's intent, capacity, and knowledge, analysts seek information from four basic knowledge types: *entity knowledge* provides the static who or what, where, and when information; the *activity or event knowledge* provides dynamic components for how, *association or relational knowledge* provides with whom and link method information, and finally *context knowledge* provides why information. The information knowledge from an information fusion system combined with context supports a user (e.g., Level 5 fusion) in refining the threat assessment. Using the information types, an analyst seeks to answer the following questions:

- Is the threat credible?
- Who are the actors composing the threat?
- Where is the threat from or intended to be?
- When would the threat take place?
- What is the likelihood of threat impact against individuals, entities, and locations?
- How has the threat evolved since the previous assessment?

Information from one knowledge type can be used to cue another (Figure 2). Evidence is data or rules about the situation (e. g., entities, activities, associations) and context to characterize a threat. Evidence accumulation is conceptualized as building a legal case rather than object prosecution. Evidence can take the form of direct or circumstantial. *Direct evidence* links a signature (entity, activity, association) to known entities; i.e., labeled data. *Circumstantial evidence* requires an inference to link information to an entity. Together, these processes surround the threat assessment and

can be separate, linked, or serial processes contributing to threat assessment, but it depends on the circumstances and assumptions that contribute to SA/TA.

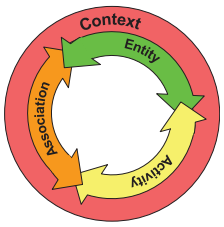

Figure 2 – Knowledge types for evidence in the SA/TA environment. Note: the colors indicate the research community's ability to measure knowledge type's confidence.

Activity and entity information can be nested to describe transactions and events. Transactions are linked activities, where information or materials are passed. Events are related activities occurring over a given domain and time [7]. These events can lead to a situation assessment that modifies the threat environment or provides information of concern (processed separately) for future threat analysis. Thus, the SA/TA could be linked immediately, in a future time, or fade from importance.

Information from the four knowledge types can be exploited by actors of organizations such as high quality predictions of future activities [8]. The majority of the data are provided willingly and unconsciously by the public such as through social networks [9].

Threat assessments should have unique requirements. Intelligence questions can be broken into three basic categories: assessment, discovery, and prediction [10]. Though the focus of this paper is threat assessment, many of the concepts are applicable to discovery and prediction. To perform threat assessment, evidence accumulation must be structured to track activities of actors independent of collection mechanism [11]. People may be *cooperative*, such as member of on-line social networks that provide a wide range of personal information; *non-cooperative* individuals limit their public footprint; or *uncooperative* individuals actively seeking to defeat attempts of their information being collected. To support people against threat assessment, cyber awareness can be gained through decision support tools.

Jonas [12] suggested the following traits that a decision support system should possess.

- *Sequence neutral processing*: knowledge is extracted as it becomes available and assessed as evidence immediately. Note: the system must be cognizant that data may arrive out of order from when it was collected and confidence can change
- *Raw data must be processed only once* [13], because access, collection-evaluation, and transmission of data generate a tremendous computational, storage and network burden due to the 5V (volume, velocity, veracity, variety, and value) big data issues.
- *Relationship aware*: links among individuals to either known or discovered individuals become part of the entity meta-data.
- *Extensible*: system must be able to accept new data sources and attributes
- *Knowledge based thesaurus*: support functions exist to handle noise when comparing queries to databases.
    - Cultural issues such as transliteration of names or moving from the formal to the informal.
    - Imprecision such as a georeference being a relative position rather than an absolute location; i.e., *over there* versus a specific latitude and longitude [14].
    - Text, rhetoric, and grammar change often and the change rate is even faster in social media than more formal communications such as broadcast news.
- *Real-time*: changes must be processed on the fly with decisions happening in an actionable timeline; i.e., on-line learning.
    - Perpetual analytics: no latency in alert generation.
- *Scalable*: able to expand based upon number of records, users, or sources.

Next, we organize a taxonomy of assumptions of context-based threat assessment systems using evidence analysis.

III. Decision Support Assumptions

Decision support threat assessment systems require pragmatic understanding of the complexity of the task due the variety of entities, associations, and activities for different contexts. Figure 3 is an engineering functional block diagram for a generic information exploitation system. At each functional block, the common assumptions made by users or technology developers is made explicit [15]. Within each section, the assumption is further resolved. We have organized the assumptions for a context-based threat assessment decision support system into: objectives, data collection, evidence analysis, decisions, actions, and uncertainty quantification which is similar to the: observe, orient, decide, act (OODA) paradigm.

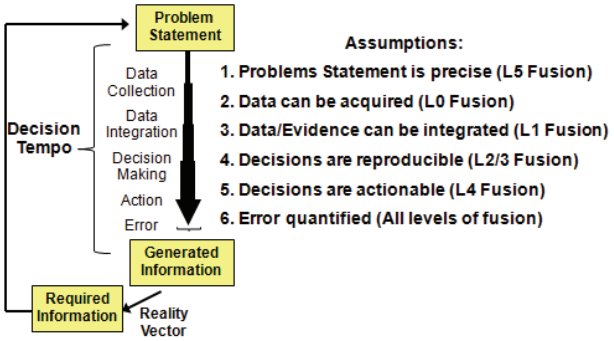

Figure 3 – Assumptions within the SA/TA Environment

Each assumption in Figure 3 contributes to intelligence errors and intelligence failures [16]. Intelligence failure is the systemic organizational surprise resulting from incorrect, missing, discarded, or inadequate hypotheses. Intelligence errors are factual inaccuracies in analysis resulting from poor or missing data. Though this paper focuses on threats to cyber systems [17], the concepts are applicable for understanding threats within social networks [18], by criminals [19], and to financial systems [20].

Assumption 1: The Problem Statement is Specific
The problem statement is specific assumes that the decision support system's output relates to the problem statement [21], which is noted in Figure 3 as the reality vector. The problem statement assumption asks fundamental questions: Can the threat be described as a question or hypothesis? Is the decision relevant the question?

Assumption 1.1 *Can the Threat be described as a Question?*

The first assumption is to understand the type of question being asked. Asking the right question relates directly to context such as the intent, capacity, and knowledge as shown in Figure 4. This uncertainty probably led Donald Rumsfeld [22] to state the following:

> "There are known knowns; there are things we know that we know.
> There are known unknowns; that is to say there are things that, we now know we don't know.
> But there are also unknown unknowns – there are things we do not know we don't know."

Treverton [23] described this taxonomy as puzzles, mysteries, and complexities. Figure 5 highlights the ability to translate unknowns into knows. The first case, and obvious to information fusion is a *data-driven* approach in which the perceived unknowns are mapped to perceived knowns (whether reality has been satisfied). For example, collections can verify that the perceived unknown is still unknown. The second case is a *knowledge-driven* in which the unknown reality is moved to a known reality. To make things known, *context-based* approaches match the unknown perceived unknowns into reality through evidence analysis.

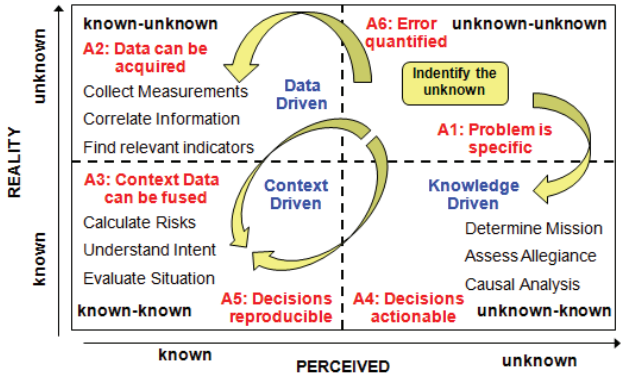

Figure 4 - Context-driven threat assessment

The next part of the question is to understand blindspots. Analysts typically assume that threat networks consist of a central hierarchical authority and then look for evidence of a center of gravity of harm, which is similar to the Federal Bureau of Investigation (FBI) combating organized crime in the 1950s and 1960s [24]. Although this paradigm might have been prevalent prior to the 9/11 attacks [25] Current threat networks are transient based upon opportunity and mutual interests [26].

There is no clear solution for how to ask the right question or even that having the right information guarantees success. For example, given a chess board arranged in the normal starting position, no single opening move exists for the white player that guarantees a win even though (s)he has perfect situational awareness. The strategy to chess is to play the game until a small number of alternatives exist before taking finishing action. The same strategy is essential for assessing and countering threats (Figure 5) [27], as with collecting, discovering, and determining the threat.

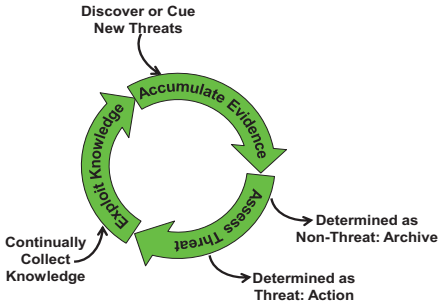

Figure 5 - Strategy for attacking loose confederation networks.

Assumption 1.2 *Is the Decision a Relevant Question?*

Analytical workflows commonly focus on specific data modalities, exploitation techniques. The reliance on existing processing chains has a number of causes. The first cause is *mechanical*; sensor data have known workflows. Their output products have known and quantifiable performance metrics. The second cause is *organizational inertia*; adopting new business processes takes strong leadership for change and involves risk. The third cause is the *lack of resources* [28]: the number and skill set for analysts are very focused among a relatively small cadre [29]. The fourth cause is changing any element in the exploitation chain requires training and a *learning timeline* which is a large investment of time, money, and most likely a near term reduction in performance. The fifth cause is that though a new or different knowledge source may contain *sufficient information content*, its technological readiness could be insufficient for operational usage.

To test the problem statement, all evidence must be structured to either confirm it or reject it. Therefore, analysts who generate problem statements must also understand the structure of the output. The downstream cost is the burden of transforming the data, prior to analysis.

Currently, evidence accumulation is a manual, cognitive process. However, analysts spend much of their time locating data sources than assessing information. Government and industry have problems federating disparate data repositories and resolving entities across those systems. Other issues facing the analysts are that their customer bases and product diversity are increasing. Another unfortunate circumstance for the current generation of analysts is that the timelines have shortened to assess system performance and usability.

Johnston [16] produced a series of tools and techniques to address the issues stated by Rumsfeld, which include questioning the foundation assumptions, black-hatting friendly capabilities, looking for precursor actions, alternative analysis, etc. Other researchers are re-discovering that the critical actors that enhance threat capacity are those individuals and entities with unique skills and capabilities that arrive *just-in-time*, i.e., the strength of weak ties [30].

Assumption 2: Data can be Acquired to Fill Knowledge Gaps
Streaming data constantly updates the data store for exploitation as knowledge. Operators are assumed to know the attributes of these disparate data and their effect on the individual hypotheses. Additionally, data acquisition assumes a number of issues: data collection is unbiased, target signatures are constant, data quality can be determined, and the all information is collected [31].

Assumption 2.1 *Data Collection is Unbiased*

Non-directed data sources have diverse origins, incomplete chain of custody, and biased analysis. The provenance links may also contain a level of uncertainty and degrees of correlation which reduces the trustworthiness of the source [32, 33]. Although the total amount of data is large, the amount of data available as evidence may be sparse for a specific problem set, location, or entity.

Assumption 2.2 *Target Signatures are Constant*

Target signatures are the information types (entity, activity, association, or context) that describe an individual within a domain (geospatial, financial, cyber, etc). The assumption has two basic components. First, an individual's or entity's interactions with their environment are invariant over time and space. Second, observed activity has a known and constant meaning. Interpreting activities is difficult because they vary with:

- Not all threat activities are anomalies; and not all anomalies are threats.
- **External stressors**: such as the arrest of a threat network member, will cause a change in the Tactics, Techniques, and Procedures (TTPs) of the group, ala Maslow's hierarchy. Yet the network itself may remain intact [34].
- **Cultural difference within a population**: Eagle [35] showed that individual's use of communication is a function of their anthropological attributes as well as network strength and stability.
- **Type and size of network**: Members of a threat network are also members of the general population [36]. The majority of the threat individual's actions are benign. Therefore even knowing that an individual is part of a threat network, determining which of their actions contributes to a threat is difficult.
- **Anonymity**: Threat actors in the cyber domain may usurp authorized user's identity [37]. Identity theft is commonplace in financial transactions even with tokens and passwords, i.e., credit cards and on-line banking [38].

To mitigate the effect of changing target signatures, analysts attempt identify individuals across all domains in which they operate. The tracking process is called certainty of presence. Certainty of presence has the added benefit to discover when a signature for a particular entity is no longer valid in a given domain. Though membership within modern threat networks are based on mutual gains, individuals generally interact among those who they trust and have deep ties [39, 40].

Assumption 2.3 *Data Quality is Knowable*

Data quality deals with the accuracy and precision of each data source [41]. For many directed sensors, the inherent data quality can be computed by convolving target, sensor, and environmental parameters [1, 42] (Figure 6). However, non-directed and non-sensor data have aspects of human interactions that include missing attributes, incorrect or vague inputs, and even ill defined attribute classes. Incorrect or incomplete data could be due to human input errors, such as day/ month/ year variations or even leading zeros. Depending upon the context, incorrect information could be an indicator of hostile activity; i.e., deliberate malfeasance.

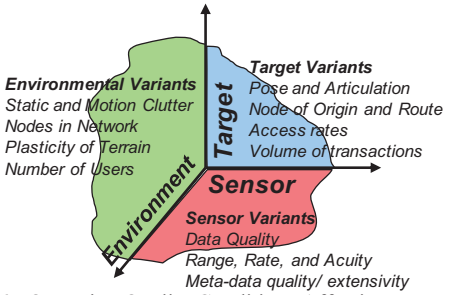

Figure. 6 - Operating Quality Conditions Affecting Data quality.

Assumption 2.4 *All Knowledge is Collected*

This assumption assumes that analysts have access to all the directed and non-direction data collection and that the data contains all threat information. In reality however, users only know the volume of data they can access and are most likely unable to estimate the amount of missing information. The assumption is that the available information can fully describe the threat. The cost of false alarms can be computed and related to intelligence errors. However, the cost of missing evidence cannot be computed and most likely to lead to surprise - intelligence failures.

Assumption 3: Context Data can be Fused

The fundamental goal for data fusion is to develop discrete signatures. Fusing disparate data adds the error of whether the observations relate to a common entity, activity, or association [43]. As the amount of evidence increases, these uncertainties are expected to resolve. The two fundamental assumptions associated with data fusion are: the data fusion strategy is fixed and knowledge can be abstracted to different resolutions.

Assumption 3.1 *The Data Fusion Strategy is Fixed*

This discussion parallels the relevance of the decision process from Assumption 1. Since the combination of intent, capacity, and knowledge is unique for each threat, there is no expectation that that a specific data type can be collected [44, 45]. Information Fusion is the interaction of sensor, user and mission [46] for situation and threat assessment. Challenges for information fusion [47] include the design of systems to identify and semantically classify threats as information exploitation as information management [48]. The integration should be based upon the constraints of the data streams (Figure 7). The most constraints exist for data level integration that requires the individual sources to be aligned in space and time, classically called data fusion. Usually, only image data are layered in this fashion. More commonly, attribute/ feature integration is performed where the data are only constrained by time or space.

Data fusion errors include the duplication of information across fields, fields incorrectly populated, and extensive use of unstructured data. Time stamps contribute to miss-registration by either poor definition of the clock or incorrect values. To mitigate these issues, background processes are required to test for duplication and trustworthiness, which is often described as metadata triage. Information triage assesses the individual data streams for information content.

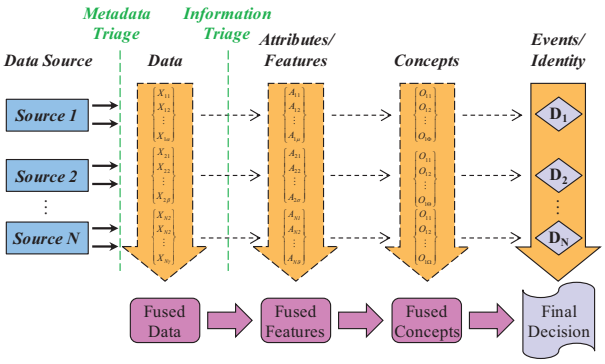

Figure 7 - Data Structures for Knowledge Types

Assumption 3.2 *Knowledge can be abstracted from Other Resolutions*

This assumption states that data of differing resolutions can be combined without a loss of information content. Anomaly detection is often performed by observing deviations from the norm [49]. If data are generalized to coarser resolution, then the observed differences between an anomaly and the normal will be smoothed: possibly below a detection threshold. If the data are assigned to higher than collected rates, uncertainty creeps into the relationship among entities, activities, or events.

Assumption 4: Decisions are Reproducible
Decisions are reproducible assumes that the decision making process is robust and auditable [50]. The assumptions built into the earlier functional blocks are expressed during decision making. Each piece of evidence's impact on the decision is assessed as it arrives. At decision time, the decision confidence is quantified. The assumptions made about the decision process are: threat assessment is pattern recognition, the operational context is understood, and human decision making is a good model for a computational engine.

Assumption 4.1 *Assessment is Pattern Recognition*

The conventional pattern recognition paradigm contains assumptions that are violated by evidence accumulation [51].

- Threats fall within specific classes, are known *a priori*, exclusive, and exhaustive
- Data are not perishable
- Knowledge classes are generated off-line
- Target signature variation is fully understood
- Performance degrades predictably with signal aberrations

The reality is that evidence accumulation for assessment does not adhere to any of the above assumptions, because no two situations/threats are the same. Human activities are not independent, but interactive. Therefore, supervised classifiers that map input attributes to output classes are not relevant.

The current assessment philosophy is to use anomaly detection. Anomaly detection requires a mechanism to continually sample the environment and measure normal conditions. Currently researchers use graph theory to map individuals within threat networks, and then infer the impact and likelihood [52]. The cost is that graph analysis is not computationally scalable.

Machine decisions require the system to determine both an upper and lower evidence threshold, which can be conceptualized as a hypothesis test. The upper threshold is to accept the threat hypothesis and alert the user to take action. The lower threshold is to reject the hypothesis and alert telling the user that no threat exists. Irvine and Israel [53] used Wald [54] sequential evidence to provide evidence bases using this strategy.

Assumption 4.2 *Operational Context is Understood*

Context is fundamental to decision making [55]. Context is the environment for interpreting activities [56]. Prior to the Boston Marathon Bombing, the bomber's activities were consistent with those of the crowd. Even if the authorities were able to review the imagery and social media available of the bombers, they had no basis to interpret the bomber's activities as anomalies or threats. After the explosions, the context changed as the suspects began to flee Boston when their identities were discovered.

Assumption 5: Decisions are Actionable
Actionable decisions require trust in the decision process, unambiguous interpretation of the decision, and time to act. Actionable decision is no guarantee of a correct or optimal decision.

Assumption 5.1 *Decision Engines are Trusted*

Trust is a uniquely human concept. Cyber and financial systems have been using trust to describe authentication. Measures exist for data quality [57]. However trust for computational decision engines, trust relates to human confidence in the results. Trust can be developed by providing decision lineage, where lineage is the audit trail for the decision's entire processing chain. Threat assessment also looks for agreement across disparate points of view (political, business, civil, secular, etc). No automated measure has been discovered for this Chapter.

User Trust issues then are confidence (correct detection), security (impacts), integrity (what you know), dependability (timely), reliable (accurate), controllability, familiar (practice and training), and consistent (reliable).

Assumption 5.2 *Decisions are Rendered Unambiguously*

This assumption is the relationship between the rendered evidence and decision confidence. Cognitive interpretation of graphical information is a function of contrast among elements, graphical complexity, and human experience [58, 59, 60]. Graph representations require simplifications to demonstrate relationships [61], which may mask other interactions [62, 63]. Ideally rendered decisions will also characterize the decision to the closest alternative, relationship to the evidence threshold, and that the context is correctly classified.

Assumption 5.3 *Decisions are Timely*

Under ideal conditions, computational decisions are rendered instantly. However, computational decisions have the same issues as humans with respect to finite timelines [64]. The concept is called time sensitive computing (Figure 8). Many computational applications fall into this realm of *conditional performance profiles* that allow meta-data to control processing time based upon time allocation or input quality [65]. So, the algorithms operate until either the performance threshold or the available time has been met.

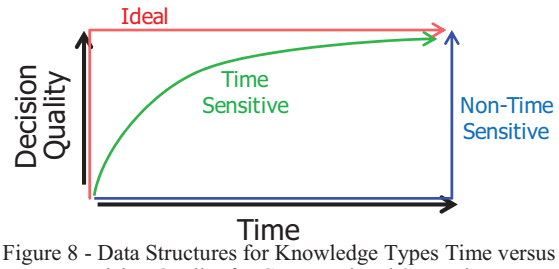

Figure 8 - Data Structures for Knowledge Types Time versus Decision Quality for Computational Strategies

The problems with this assumption are that: 1. Components are often tested using their local or domain specific metrics and translation to a global measures are either impractical or have no cognitive basis; 2. Metrics often relate to the performance of an algorithm, called producer's performance rather than the amount of evidence a user must review to make a decision, called users performance; and 3. Component level errors are incorrectly assumed to be uncorrelated.

Assumption 6: Error can be fully quantified
Identifying error sources assumes that the system can be decomposed into its functions and their components. Then, the combination of the component metrics can be combined to match the system level performance measures (Figure 3). Error analysis does not provide any information for decision relevance [66].

While the error analysis leads to incorrect threat analysis, we can assume that the threat analysis is pessimistic (e.g., lower bound). It is not that threat should not be determined, but rather that the results (with the many assumptions) should error on the side of caution. Measures of effectiveness [67] require that the many sources of uncertainty be account for in the process. Currently, the International Society of Information Evaluation and Testing of Uncertainty Reasoning Working Group (ETURWG) [68] is investigating these issues for both context analysis and interoperable standards [69].

IV. Context-Based Threat Example

The following example shows how the earlier assumptions are accounted for quantitatively. In the example, Bayes Rule is used for data fusion and Dempster's Rule for evidence accumulation. We seek to address the assumptions: (6) quantifiable, (5) actionable, (4) reproducible, (3) use of context data, (2) acquireable, and (1) specific for which we use evidence theory with *Proportional Conflict Redistribution* (PCR).

Recently, [70] has shown that Dempster's rule is consistent with probability calculus and Bayesian reasoning if and only if the prior $P(X)$ is uniform. However, when the $P(X)$ is not uniform, then Dempster's rule gives a different result. Others have also tried to compare Bayes and evidential reasoning (ER) methods [71]. Assuming that we have multiple measurements $Z = \{Z_1, Z_2, \ldots, Z_N\}$ for threat detection D being monitored, evidence can be assessed.

Recent advances in DS methods include *Dezert-Smarandache Theory* (DSmT). DSmT is an extension to the Dempster-Shafer method of evidential reasoning which has been detailed in numerous papers [72] and texts [73], such as the PCR rule 5 (PCR5). All details, justifications with examples on PCR*n* fusion rules and DSm transformations can be found in the DSmT compiled texts (Dezert, *et al.*, Vols. 1-4). A comparison of the methods is shown in Figure 9.

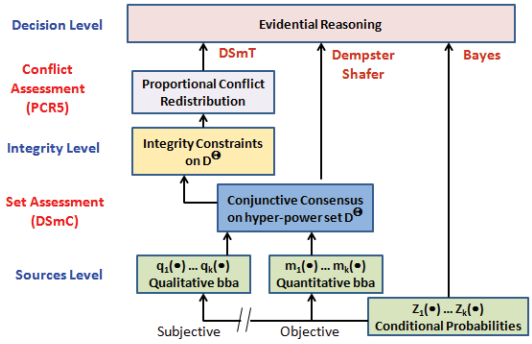

Figure 9 - Comparison of Bayesian, Dempster-Shafer, and PCR5.

In the DSmT framework, the PCR5 is used generally to combine the basic belief assignment (BBAs). PCR5 transfers the conflicting mass only to the elements involved in the conflict and proportionally to their individual masses, so that the specificity of the information is entirely preserved in this fusion process. Let $m_1(.)$ and $m_2(.)$ be two independent BBAs, then the PCR5 rule is defined as follows (see Dezert, *et al.*, 2009, Vol. 2 for full justification and examples): $m_{PCR5}(\varnothing) = 0$ and $\forall X \in 2^\Theta \setminus \{\varnothing\}$, where $\varnothing$ is the null set and 2^Θ is the power set:

$$m_{PCR5}(X) = \sum_{\substack{X_1;\, X_2 \in 2^\Theta \\ X_1 \cap X_2 = X}} m_1(X_1)\, m_2(X_2) \quad + \quad \sum_{\substack{X_2 \in X \\ c(X_1 \cap X_2) = \varnothing}} \left[\frac{m_1(X_1)^2\, m_2(X_2)}{m_1(X_1) + m_2(X_2)} + \frac{m_1(X_1)\, m_2(X_2)^2}{m_1(X_1) + m_2(X_2)} \right] \quad (1)$$

where $\bigcap$ is the interesting and all denominators in the equation above are different from zero. If a denominator is zero, that fraction is discarded.

In the example, we assume that policies of threat analysis are accepted and that the trust assessment of must determine whether the dynamic data is trustworthy, threatening, or under attack (Assumption 6 – quantifiable). The notional application system collects raw measurements on the data situation, such as Boston Bomber activities as an attack, (Assumption 2 - acquireable). Situation awareness is needed to determine the importance of the information for societal safety (Assumption 1 – specific). With a prior knowledge, data exploitation can be used to determine the situation (Assumption 3 - use of context data). The collection and processing should be consistent for decision making (Assumption 4 – reproducible) over the data acquisition timeline. Finally, the focus of the example is to increase the timeliness of the machine fusion result for human decision making (Assumption 5 – actionable).

Conventional information fusion processing would include Bayesian analysis to determine the state of the attack. However, here we use the PCR5 rule which distributes the conflicting information over the partial states. Figure 10 shows the results for a societal status undergoing changes in the

social order such as events indicating an attack and the different methods (Bayes, DS, and PCR5) to access the threat. An important result is the timeliness of the change in situation state as depicted. In the example, there is an initial shock of information that lasts for a brief time (time 20 to 27 seconds) while the situation is being assessed (threat or no threat); followed by another repeated event (time 40 to 50 seconds). As shown the change in state is not recorded by Bayes, but the PCR5 denotes the change. After the initial attacks, the threat state is revealed (time 70 to 100 seconds) from which a Bayesian method starts to indicate a change in the threat state.

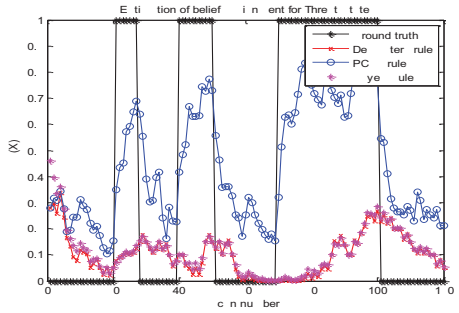

Figure 10 - Results of Bayesian, Dempster-Shafer (similar to Bayes), and PCR5 Fusion Theories for trust as a measure of a threat attack.

The threat analysis is presented in Figure 11 of which the average threat condition, based on context, is determined using PCR5. As the changing context persists, Bayesian methods do not adapt to the changing environment.

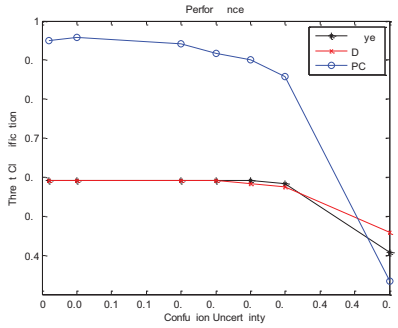

Figure 11 - Results of Bayesian, Dempster-Shafer, and PCR5 Fusion Theories for threat detection improvement.

Here it is important to note that context is used in the PCR5 as the knowledge of the first event leads to a contextual change (that is not detected by using Bayes Rule). Likewise, the possibility for a state change (unknown unknown) is determined from the conflicting data. The conflict used in the example is 20% which is an example where some users are reporting the facts (threat event), while others are reporting differently since they cannot confirm the evidence. The notional example is only shown to highlight the importance of context. Two cases arise: (1) whether the data is directly accessible, hence conflict in reporting, and (2) exhaustively modeling all contextual data to be precise is limited – leading to some failures.

V. CONCLUSIONS

We outlined the analysis of situation/threat assessment given the context of the environment. Threat analysis needs were juxtaposed against the assumptions developers use to make the computational decision support systems tractable, which inherently is based on situation assessment. We showed that the long term system goals have some very real near-term realities. We organized the contextual information for situation/threat analysis by categorizing six assumptions: (1) specific problem, (2) acquireable data, (3) use of context, (4) reproducible analysis, (5) actionable intelligence, and (6) quantifiable decision making. By understanding these assumptions, system users can mitigate these pitfalls by employing skepticism and confirmation for context assessment [74]. Together, a notional example was presented to highlight the need for evidence theory (e.g., PCR) to deal with conflicting information in building a context assessment.

Future work will focus on Level 5 user refinement against the assumptions presented above. The user inputs context through mental, explicit, and analytical models [75]. Computational modeling (causal, descriptive, and/or action-based) must answer user information needs in a timely and effective manner against threats and the situation.

ACKNOWLEDGEMENTS

This work is partly supported by the Air Force Office of Scientific Research (AFOSR) under the Dynamic Data Driven Application Systems program and the Air Force Research Lab.

REFERENCES

[1] S. A. Israel, "Toward a Common Lexicon for Exploiting Activity Data," In *IEEE Applied Imagery and Pattern Recognition Workshop: Computer Vision: Time for Change* (6 pages). 2012.

[2] J. Leachtenauer, "National Imagery Interpretability Ratings Scales: Overview and Product Description.." *American Society of Photogrammetry and Remote Sensing Ann. Meetings*, pp. 262-71, 1996.

[3] J, M. Irvine, "National Imagery Interpretability Rating Scales (NIIRS): Overview and Methodology. Proc. *SPIE,*Vol. 3128, 1997.

[4] E. Blasch, E. Bosse, and D. Lambert, *High-Level Information Fusion Management and Systems Design*, Artech House, Norwood, MA, 2012.

[5] J, M. Irvine, D. Cannon, J. Miller, J. Bartolucci, G. O'Brien, L. Gibson, C. Fenimore, J. Roberts, I. Aviles, M. Brennan, A. Bozell, L. Simon, S. A. Israel, "Methodology study for development of a motion imagery quality metric," *Proc. SPIE,* vol.. 6209, 2006.

[6] J. T. Picarelli, "Transnational Threat Indications and Warning: The Utility of Network Analysis," *AAAI Fall Symposium on Artificial Intelligence and Link Analysis Technical Report*, 1998.

[7] R. K. Betts, "Analysis, War, and Decision: Why Intelligence Failures Are Inevitable," *World Politics, 31*, 61-89, 1978.

[8] Y. Altshuler, N. Aharony, A. Pentland, Y. Elovici, M. Cebrian, "Stealing Reality: When Criminals Become Data Scientists (or Vice Versa)," *IEEE Intelligent Systems*, 2-10, 2011.

[9] C R. Vincente, D. Freni, C. Bettini, *et al*. "Location-Related Privacy in Geo-Social Networks," *IEEE Internet Computing*, 20-27, 2011.

[10] R. Colbaugh, K. Glass, J. Gosler, "Some Intelligence Analysis Problems and Their Graph Formulations," *Intelligence Community Research and Development, 315*, 2010.

[11] A. Vinciarelli, "Capturing Order in Social Interactions," *IEEE Signal Processing Magazine*, 133-52, 2009.

[12] J. Jonas, "Threat and Fraud Intelligence, Las Vegas Style," *IEEE Security and Privacy*, 28-34, 2006.

[13] A. E. Gattiker, F. H. Gebara, A. Gheith, *et al*.., *Understanding System and Architecture for Big Data*. In (4 pages): IBM, 2012.

[14] C. Y. Lin, L. Wu, Z. Wen, H. Tong, *et al*., "Social Network Analysis in Enterprise," *Proc. of the IEEE*, 100(9): 2759-2776, 2012.

[15] M. J. Duggin, C. J. Robinove, "Assumptions Implicit in Remote Sensing Data Acquisition and Analysis," *International Journal of Remote Sensing, 11*, 1669 – 94, 1990.

[16] R. Johnston, "Analytic Culture in the US Intelligence Community. An Ethnographic Study," In (173 pages). Washington: *Center for Study of Intelligence,Central Intelligence Agency*, 2005.

[17] D. Chaikin, "Network Investigations of Cyber Attacks: The Limits of Digital Evidence," *Crime, Law and Social Change, 46*, 239-56, 2006.

[18] S. A. Macskassy, F. Provost, "A Brief Survey of Machine Learning Methods for Classification in Networked Data and an Application to Suspicion Scoring." *Int'l Conf. on Machine Learning Stat. Network Analysis Workshop*, 2006.

[19] J. H. Ratcliffe, *Intelligence-Led Policing*. Cullompton, Devon: Willan Publishing, 2008.

[20] I. Sakharova, "Al Qaeda Terrorist Financing and Technologies to Track the Finance Network," *IEEE Intell. and Security Informatics*, 2011.

[21] J. Nagl, J. *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Vol. Westport): Praeger Pub., 2002.

[22] D. Rumsfeld, *Known-knowns*. In: Defense.gov News Transcript: DoD News Briefing – Secretary Rumsfeld and Gen. Myers, United States Department of Defense (defense.gov)". 2002.

[23] G. F. Treverton, *Intelligence for an Age of Terror*. New York: Cambridge University Press, 2009.

[24] S. Ressler, "Social Network Analysis as an Approach to Combat Terrorism: Past, Present, and Future Research," *Homeland Security Affairs, 2*, 2006.

[25] V. E. Krebs, "Mapping Networks in Terrorist Cells," *Connections, 24*, 43-52, 2002.

[26] P. Klerks, "The Network Paradigm Applied to Criminal Organizations: Theoretical Nitpicking or a Relevant Doctrine for Investigators? Recent Developments in the Netherlands," *Connections, 24*, 53-65, 2001.

[27] B. Bringmann, M. Berlingerio, F.Bonchi, A. Gionis, " Learning and Predicting the Evolution of Social Networks," *IEEE Intelligent Systems*, 26-24, 2010.

[28] R. Travers, "The Coming Intelligence Failure," *Studies in Intelligence (CIA), 40*, 35-43, 1997.

[29] T. J. Burger, "Inside the Nerve Center of America's Counterterrorist Operations," In *Time Magazine*, 2004.

[30] M. S. Granovetter, "The Strength of Weak Ties," *American Journal of Sociology, 78*, 1360-80, 1973.

[31] M. K. Sparrow, "The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects," *Social Networks, 13*, 251-74., 1991.

[32] P. Buneman, S. Khanna, W. C. Tan, "Data Provenance: Some Basic Issues," In *Foundations of Software Technology and Theoretical Computer Science* (pp. 87-93): Springer, 2000.

[33] E. Blasch, A. Jøsang, J. Dezert, P. C. G. Costa, A-L. Jousselme, "URREF Self-Confidence in Information Fusion Trust," *International Conference on Information Fusion*, 2014.

[34] E. H. Powley, "Reclaiming Resilience and Safety: Resilience Activation in the Critical Period of Crisis," *Human Relations, 62*, 1289-326, 2009.

[35] N. Eagle, "Behavioral Inference Across Cultures: Using Telephones as a Cultural Lens," *IEEE Intelligent Systems*, 62-64, 2008.

[36] S. Milgram, "The Small-World Problem," *Psychology Today, 1*, 61-67, 1967..

[37] G. Lawton, "Invasive Software, Who's Inside Your Computer," *IEEE Computers, 35*, 15-18, 2002.

[38] S. Graham, "The Urban Battlespace," *Theory Culture Society, 26*, 278-88, 2009.

[39] S. Saavedra, F. Reed-Tsochas, B. Uzzi, "Asymmetric Disassembly and Robustness in Declining Networks," *Proc. of the National Academy of Sciences, 105*, 16466-71, 2008.

[40] H. Sundaram, Y. R. Lin, M. DeChoudhruy, A. Kelliher,"Understanding Community Dynamics in Online Social Networks," *IEEE Signal Processing Magazine*, 33-40, 2012.

[41] B. Kahler, E. Blasch, L. Goodwon, "Operating Condition modeling for ATR Fusion Assessment, *Proc. of SPIE*, Vol. 6571, 2007.

[42] B. Kahler, E. Blasch, "Sensor Management Fusion Using Operating Conditions, *Proc. IEEE Nat. Aerospace Electronics Conf*.. 2008.

[43] S. Rassler, "Data Fusion: Identification Problems, Validity, and Multiple Imputation," *Austrian Journal of Statistics, 33*, 153-71, 2004.

[44] I. Bloch. A. Hunter, "Fusion: General Concepts and Characteristics," *Int'l Journal of Intelligent Systems, 16*, 1107–34, 2001.

[45] D. L. Hall, *Mathematical Techniques in Multisensor Data Fusion*: Artech House, 1992.

[46] E. Blasch, "Sensor, User, Mission (SUM) Resource Management and their interaction with Level 2/3 fusion, *Int. Conf. on Info Fusion*, 2006

[47] E. Blasch, D. A. Lambert, P. Valin, M. M., Kokar, J. Llinas, S. Das, C-Y. Chong, E. Shahbazian, "High Level Information Fusion (HLIF) Survey of Models, Issues, and Grand Challenges," *IEEE Aerospace and Electronic Systems Magazine,* Vol. 27, No. 9, Sept., 2012.

[48] E. Blasch, A. Steinberg, S. Das, J. Llinas, C. Chong, O. Kessler, E. Waltz, and F. White, "Revisiting the JDL model for information exploitation," *International Conference on Information Fusion*, 2013.

[49] C. Drummond, "Replicability is not Reproducibility: Nor is it Good Science," *ICML Evaluating Methods for Machine Learning*, 2009.

[50] E. Blasch, C. Banas, *et al*., "Pattern Activity Clustering and Evaluation (PACE)," *Proc. SPIE*, Vol. 8402, 2012.

[51] R. O. Duda, P. E. Hart, D. G. Stork, *Patten Classification* (second edition ed.). New York: John Wiley, and Sons, 2001.

[52] T. E. Senator, H. G. Goldberg, A. Memory, "Distinguishing the Unexplainable from the Merely Unusual: adding explanations to outliers to discover and detect significant complex rare events," *ACM SIGKDD Workshop on Outlier Detection and Description* (pp. 40-45), 2013.

[53] J. M. Irvine, S. A. Israel, "A Sequential Procedure for Individual Identity Verification Using ECG," *EURASIP J. on Adv. in Signal Processing: Recent Adv. in Biometric Sys.: A Sig. Proc. Perspective,* 243215, 2009.

[54] A. Wald, *Sequential Analysis*. New York: Dover, 1994.

[55] C. E. Callwell, *Small Wars: Their Principles and Practice*: University of Nebraska Press, 1906.

[56] J. R. Hipp, A. Perrin, "Nested Loyalties: Local Networks' Effects on Neighbourhood and Community Cohesion," *Urban Studies, 43*, 2503-23, 2006.

[57] R. I. Hammoud, C. S. Sahin, *et al*, "Automatic Association of Chats and Video Tracks for Activity Learning and Recognition in Aerial Video Surveillance," *Sensors*, 14, 19843-19860, 2014.

[58] E. Agichtein, C. Castillo, D. Donato, A. Gionis, G. Mishne, "Finding High-quality Content in Social Media," In *Web Search and Web Data Mining* Palo Alto: ACM, 2008.

[59] A. M. MacEachren, *Some Truth with Maps: A Primer on Symbolization and Design*: American Association of Geographer, 1994

[60] M. Monmonier, *How to Lie with Maps: Second Edition*: University of Chicago Press, 1996

[61] R. Amar, J. Eagan, J. Stasko, "Low-level Components of Analytic Activity in Information Visualization," In *IEEE Symposium on Information Visualization* (pp. 111-17). Minneapolis, 2005.

[62] A. Perer, B. Shneiderman, "Balancing Systematic and Flexible Exploration of Social Networks," *IEEE Transactions on Visualizations and Computer Graphics, 12*, 693-700, 2006.

[63] Z. Shen, K. L. Ma, T. Eliassi-Rad, "Visual Analysis of Large Heterogeneous Social Networks by Semantic and Structural Abstraction," *IEEE Tr. Vis. and Comp. Graphics, 12*, 1427-2439, 2006.

[64] E. Blasch, "Introduction to Level 5 Fusion: the Role of the User," Chapter 19 in *Handbook of Multisensor Data Fusion 2nd Ed,* Eds. M. E. Liggins, D. Hall, and J. Llinas, CRC Press, 2008.

[65] S. Zilberstein, "An Anytime Computation Approach to Information Gathering," *AAAI Spring Symposium Series on Information Gathering from Distributed, Heterogeneous Environments*, 1995.

[66] S. A. Israel, "Performance Metrics: How and When," *Geocarto International, 21*, 23-32, 2006.

[67] E. Blasch, P. Valin, E. Bossé, "Measures of Effectiveness for High-Level Fusion," *Int'l Conf. on Info Fusion*, 2010.

[68] P. C. G. Costa, K. B. Laskey, E. Blasch, A-L. Jousselme, "Towards Unbiased Evaluation of Uncertainty Reasoning: The URREF Ontology," *International Conference on Information Fusion*, 2012.

[69] E. Blasch, K. B. Laskey, A-L. Jousselme, V. Dragos, P. C. G. Costa, J. Dezert, "URREF Reliability versus Credibility in Information Fusion (STANAG 2511)," *Int'l. Conference on Information Fusion*, 2013.

[70] J. Dezert, "Non-Bayesian Reasoning for Information Fusion – A Tribute to Lofti Zadeh," *submitted to J. of Adv. of Information Fusion*, 2012.

[71] E. Blasch, J. Dezert, B. Pannetier, "Overview of Dempster-Shafer and Belief Function Tracking Methods," *Proc. SPIE*, Vol. 8745, 2013.

[72] F. Smarandache, J. Dezert, "Proportional Conflict Redistribution Rules for information fusion," 2005. http://arxiv.org/pdf/cs/0408064.pdf

[73] J. Dezert, F. Smarandache, *Advances and applications of DSmT for information fusion (Collected works)*, Vols. 1-4, American Research Press, http://www.gallup.unm.edu/~smarandache/DSmT.htm

[74] A. Steinberg, C. Bowman, *et al*., "Adaptive Context Assessment and Context Management," *Int'l Conf. on Information Fusion*, 2014..\

[75] E. Waltz, *Quantitative Intelligence Analysis: Applied Analytical models, simulations, and games*, Rowman & Littlefield, 2014.