Context Assumptions for Threat Assessment Systems

Steven A. Israel and Erik Blasch

Abstract Decision support systems enable users to quickly assess data, but they require significant resources to develop and are often relevant to limited domains. This chapter identifies the implicit assumptions that require contextual analysis for decision support systems to be effective for providing a relevant threat assessment. The impacts of the design and user assumptions are related to intelligence errors and intelligence failures that come from a misrepresentation of context. The intent of this chapter is twofold. The first is to enable system users to characterize trust using the decision support system by establishing the context of the decision. The second is to show technology designers how their design decisions impact system integration and usability. We organize the contextual information for threat analysis by categorizing six assumptions: (1) specific problem, (2) acquirable data, (3) use of context, (4) reproducible analysis, (5) actionable intelligence, and (6) quantifiable decision making. The chapter concludes with a quantitative example of context assessment for threat analysis.

Keywords High-level information fusion · Situation assessment · Threat assessment · Context · Timeliness · Uncertainty · Unknowns

5.1 Introduction

A threat is an assessment that an individual or group has the potential to cause harm to specific entity or entities. Threat assessment has three parameters: intent, capacity, and knowledge or intent, capability, or opportunity [1]. During the Cold War, sovereign nations engaged other sovereign nations using military-specific vehicles operating in collaborative groups. The battle groups were centrally

S.A. Israel
Raytheon, Chantilly, VA, USA
e-mail: Steven.a.Israel@Raytheon.com

E. Blasch (✉)
Air Force Research Lab, Rome, NY, USA
e-mail: erik.blasch@gmail.com

L. Snidaro et al. (eds.), *Context-Enhanced Information Fusion*,
Advances in Computer Vision and Pattern Recognition,
DOI 10.1007/978-3-319-28971-7_5

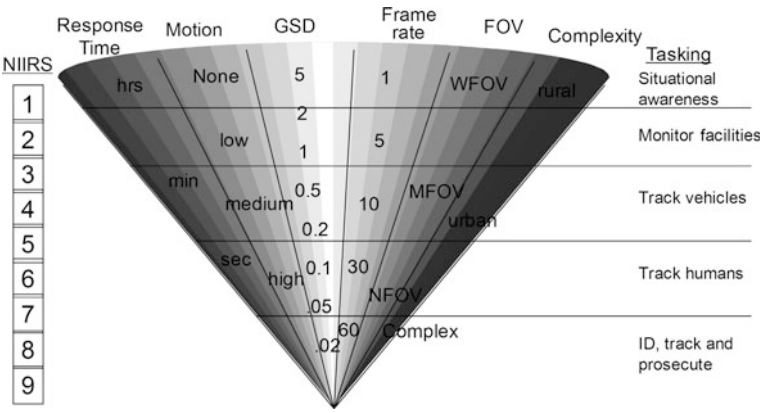

Fig. 5.1 Image quality parameters versus tasks: courtesy of David Cannon [5]

coordinated and positioned away from civilian activities to maximize their maneuverability [2].

The Cold War military performed directed data collection, which means that they maintained custody of the information throughout the stovepiped exploitation chain. Enemy intent and capacity were based upon knowledge of the leaders, military strength and readiness, and doctrine. For example, the Cold War threats were so well understood that the required information and analyst tasks determined the design for imaging sensors [3, 4]. Figure 5.1 identifies that design relationship including ground sampling distance (GSD) and field of view (FOV) for the National Imagery Interpretability Rating Scale (NIIRS).

In addition to the traditional Cold War threats, threats to sovereign nations also include: organized crime, narcotics trafficking, terrorism, information warfare, and weapons of mass destructions (WMD) [6]. Non-national actors pose different threats in the following manner: (1) there is no identifiable battlefront; (2) non-national actors keep and garrison few if any pieces of heavy military hardware, rocket launchers, tanks, etc., which both reduces their physical signature and minimizes their liabilities; (3) they maintain no persistent doctrine; (4) their numbers and actions form only a small fraction of a percentage of the resident population; and (5) they dictate attacks in the political, financial, cyber, and cultural domains in addition to the geospatial, when their opportunity for success is greatest [7–9].

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 a 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.

The remainder of this chapter is laid in the following manner. Threats to sovereign nations are defined. The common elements of those threats and their impacts on decision supports systems are identified. The assumption used by

decision support system developers are made explicit. Finally, an example of how the developer assumptions can be quantified using evidence theory is performed.

5.2 Defining Threats

5.2.1 Threat Assessment

To identify the threat's intent, capacity, and knowledge, analysts seek information from four basic knowledge types (Table 5.1): entity knowledge provides the static *who* or *what, where,* and *when* information; the activity or transaction knowledge provides dynamic components for *how*; association knowledge provides *with whom* and *link method* information; and finally context knowledge provides *why* information. Using these information types, the analyst seeks to answer the following:

- Is the threat credible?
- Who are the individuals or groups composing the threat?
- What is the impact and likelihood of threat against individuals, entities, and locations?
- How has the threat evolved since the previous assessment?

Table 5.1 Diversity of knowledge types

Information level	Description	Example questions	Metadata
Entity	Static target, noun: person, car, building, website, idea	Determine type of target, location, and time: where, what, and when?	Name, work, ownership, membership, address, area extent, topic, and content
Activity/Event	Entity performing action	Tracking entity, routes, estimating traffic patterns, transactions, volume, changes: where's it going, is it moving with the rest of traffic, how many file downloads?	Traffic volume, direction, diversity, mode, domain type (financial, physical, social media), coordinated activities, criminal acts, and daily commute
Association	Functional relationship among entities	Network, membership, purpose: who are the friends of the entity, what is the purpose for their association?	Interpersonal (family, friends, employer), social interactions (people, places), topic, purpose, accessibility, cost, and transaction type
Context	Conditions under which entity interacts within its environment	Determine activity/event/transaction purpose along with tactics, techniques, and procedures: why?	Culture, geography, cost, politics, subject, history, religion, social interaction, availability, and access

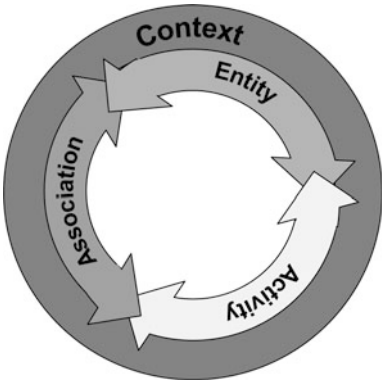

Fig. 5.2 Knowledge types for evidence in the human environment

Information from one knowledge type can be used to cue another (Fig. 5.2). Evidence is data or rules about individuals or other entities, activities/transactions, associations, and context used to characterize a threat. Evidence accumulation is conceptualized as building a legal case rather than the Cold War target prosecution [10]. Evidence can take the form of direct or circumstantial. Direct evidence links a signature (entity, activity, association) to known actor(s) or entities; i.e., labeled data. Circumstantial evidence requires an inference to link information to an entity.

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 [11].

Information from the four knowledge types is now being exploited by corporations and private citizens. Intelligence can be sold to advertisers; used for bootstrapping on other types of attacks, business espionage, and generation of high-quality predictions of future activities [12]. The majority of these data are provided willingly and unconsciously by the public [13].

5.2.2 Threat Assessments Should Have Unique System Requirements

Intelligence questions can be broken into three basic categories: assessment, discovery, and prediction [14]. Though the focus of this chapter 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 individuals independent of collection mechanism [15]. Individuals may be cooperative, such as member of online social networks that provide a wide range of personal information; noncooperative individuals limit their public footprint; and uncooperative individuals actively seek to defeat attempts of their signature being collected.

Jonas [16] 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.
  - The decision and confidence may change with time as additional confirming and rejecting evidence are reported.
- *Raw data must be processed only once* [17], 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) 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 [18].
  - 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., online learning.
  - Perpetual analytics: no latency in alert generation.
- *Scalable*: able to expand based upon number of records, users, or sources.

5.3 Assumptions for Decision Support Systems

The remainder of this chapter describes the assumptions for threat assessment decision support system. Figure 5.3 is an engineering functional block diagram for a generic information exploitation system. For a given *problem statement*, there are assumptions included in the threat assessment. These assumptions are organized into the Data Fusion Information Group (DFIG) model levels (L1 … L5) of information fusion. Together, the assumptions along the processing chain are included in the *generated information* that accompanies a threat decision. However,

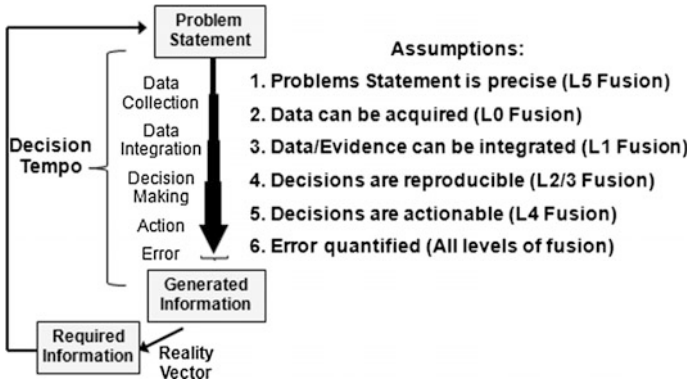

Fig. 5.3 Assumptions within the human environment

there must be a *reality vector* that translates the decision into the required information. The ops tempo determines the amount of context that can be accurately relayed in the assumptions that accompany a decision. At each functional block, the common assumptions made by users or technology developers are made explicit [19]. Within each section, the assumption is further resolved.

Each assumption in Fig. 5.3 contributes to intelligence errors and intelligence failures [20]. 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 chapter focuses on threats to governments [21], the concepts are applicable for understanding threats within social networks [22], by criminals [23], and to financial systems [24].

Assumption 1 The Problem is Specific

Assumption 1: The Problem Statement is Specific
The problem statement in specific assumes that the decision support system's output relates to the problem statement [25], which is noted in Fig. 5.3 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 or a Hypothesis?
The first part is to understand the type of question being asked. Asking the right question relates directly to context. For current insurgent warfare [2], nations face

threats from a number of groups each with different outcome intent, capacity, and knowledge as shown in Fig. 5.4. This uncertainty in the enemy probably led Donald Rumsfeld [26] 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 [27] described this taxonomy as puzzles, mysteries, and complexities. Figure 5.4 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-driven* approaches match the unknown perceived unknowns into reality through evidence analysis.

The next part of the question is to understand blindspots. Originally, analysts assumed that threat networks consisted of a central hierarchical authority. Analysts would then look for evidence of a kingpin and assess their capacity to do harm, which is similar to the Federal Bureau of Investigation (FBI) combating organized crime in the 1950s and 1960s [23, 28]. Although this paradigm might have been prevalent prior to the 9/11 attacks [29], Al Qaeda and its confederates moved away from that model shortly afterward [2]. Current threat networks are transient based upon opportunity and mutual interests [30].

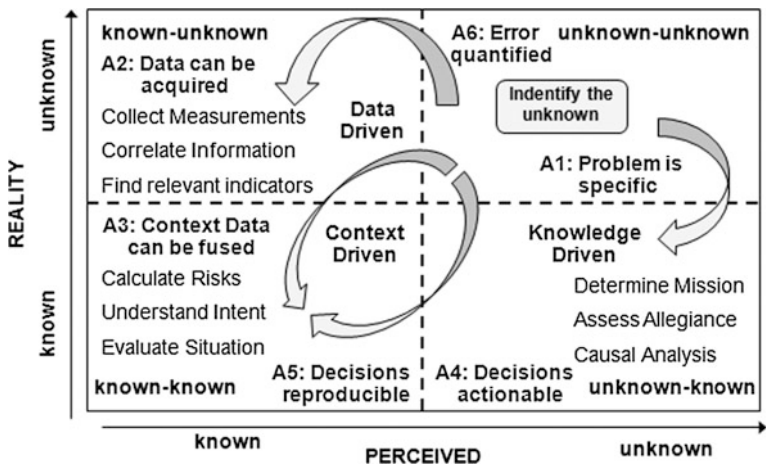

Fig. 5.4 Context-driven threat assessment

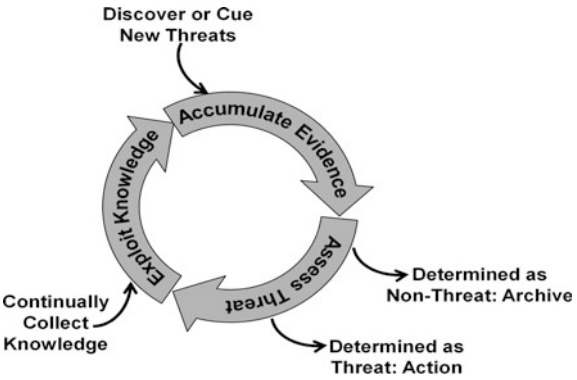

Fig. 5.5 Strategy for attacking loose confederation networks

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 (Fig. 5.5) [31].

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* [32]: the number and skill set for analysts are very focused among a relatively small cadre [33]. 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, individuals 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 and they rarely have the time to perform their after action reviews (AARs) to assess system performance and usability.

Johnston [20] produced a series of tools and techniques to address the issues stated by Rumsfeld, which include questioning the foundation assumptions, looking for precursor actions, alternative analysis, etc. For example, black-hatting friendly capabilities which includes a hacker who violates computer security for little reason beyond mischievous or satisfaction behavior. Other researchers are rediscovering that the critical actors that enhance threat capacity are those individuals and entities with unique skills and capabilities that arrives *just-in-time*, i.e., the strength of weak ties [34].

Assumption 2 Context Data can be Acquired

Assumption 2: Context Data can be Acquired to Fill Knowledge Gaps
The assumption that data can be acquired to fill knowledge gaps is a holdover from the directed collections of the Cold War. The purpose for data collection is to improve decision confidence above some threshold. Many data streams are continually generating information, so the context is dynamic. So, data collection is less important than continually trolling known databases for new content or determining the location of relevant data sources. Data acquisition assumes a number of issues: data collection is unbiased, target signatures are constant, data quality can be determined, and all the information is collected [35].

Assumption 2.1 Data Collection is Unbiased
Nondirected data sources have diverse origins and their chain of custody is incomplete. The provenance links may also contain a level of uncertainty, which reduces the trustworthiness of the source [36, 37]. 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:

- **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 [38].
- Not all threat activities are anomalies; and not all anomalies are threats.

- **Cultural difference within a population**: Eagle [39] showed that the 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 [40]. 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 [41]. Identity theft is commonplace in financial transactions even with tokens and passwords, i.e., credit cards and online banking [42].

Sakharova [24] documented the change in Al Qaeda's financial transactions since 9/11. Originally, the group was highly centralized using commercial banking institutions, money laundering techniques, and countries with lax laws and poor banking oversight. As western countries cracked down on their legitimate banking operations, the group changed tactics to holding and transferring money in fixed commodities such as gold. Alternatively, these groups used the more traditional Islamic money transfer method of Hawala, which is comparable to Western Union transfers using trusted, usually unaffiliated, individuals without formal record-keeping.

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 [43, 44].

Assumption 2.3 Data Quality is Measureable

Data quality deals with the accuracy and precision of each data source [45]. For many directed sensors, the inherent data quality can be computed by convolving target, sensor, and environmental parameters [46] (Fig. 5.6). However, nondirected and nonsensor 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.

Human interactions make digital data, cyber in particular, suspect as evidence because: (1) Altering digital records is easy and the chain of custody is difficult to confirm; (2) Forensic data review may not yield information about file manipulation; (3) Lack of standards for the collection, verification, exploitation, and preserving digital evidence; (4) The 5Vs make the organization, scanning, and sifting functions by investigators difficult for determining the responsible party for the digital attack; and (5) Assigning the information to a unique individual is difficult to prove [21].

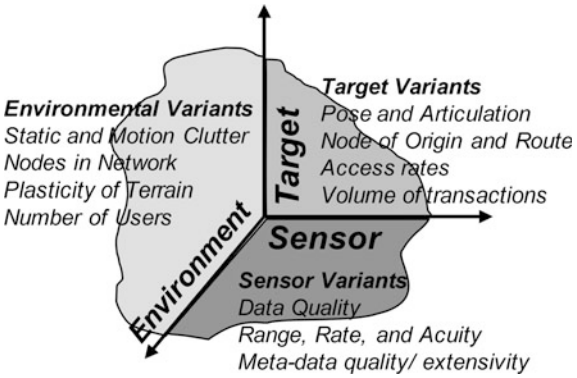

Fig. 5.6 Operating quality conditions affecting data quality

Assumption 2.4 All Knowledge is Collected

This assumption assumes that analysts have access to all the directed and nondirectional data collection and that those data contain 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

Assumption 3: Data can be Fused

The fundamental goal for data fusion is to develop discrete decision on a threat assessment. Fusing disparate data can add error as to whether the observations relate to a common entity, activity, or association [47]. As the amount of evidence increases, these uncertainties are expected to resolve. Two fundamental assumptions associated with data fusion are: the data fusion strategy is fixed and knowledge can be abstracted to different resolutions, which require context (or for that matter the right context) to change fusion strategies to produce the correct fidelity.

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 [48–50]. Information Fusion is the interaction of sensor, user, and mission [51] for situation and threat assessment [52]. Challenges for information fusion [53] include the design of systems to identify and semantically classify threats as information

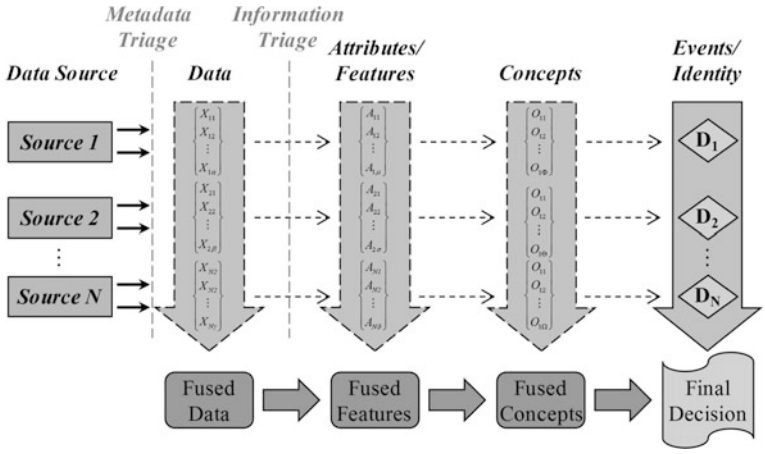

Fig. 5.7 Data structures for knowledge types

exploitation as information management [54]. The integration should be based upon the constraints of the data streams (Fig. 5.7). Many constraints exist for data level integration that require 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. However, for threat information there must be relevant features that come from threat concepts for a given threat event identification.

Data fusion errors include the duplication of information across fields, fields incorrectly populated, and extensive use of unstructured data. Time stamps contribute to misregistration 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.

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 [55]. 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 Context Decisions are Reproducible

Assumption 4: Context Decisions are Reproducible
Decisions are reproducible assumes that the decision making process is robust and auditable [56]. 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 Threat Assessment is Pattern Recognition
The conventional pattern recognition paradigm contains assumptions that are violated by evidence accumulation [57].

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

The reality is that evidence accumulation for threat assessment does not adhere to any of the above assumptions, because no two 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 threat 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 [58]. 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 [59] used Wald [60] sequential evidence to provide evidence bases using this strategy.

Assumption 4.2 Operational Context is Understood
Context is fundamental to decision making [61]. Context is the environment for interpreting activities [62]. 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 4.3 Human Decision Making is a model for Computational Decision Engine

Humans perform evidence accumulation similar to the model in Fig. 5.5 [63] and have specific thresholds for recognition and understanding from which decisions are rendered, i.e., the *Eureka moment* [9, 32, 64–66]. Other uniquely human issues also contribute to failure are:

- Stereotyping based upon consistency, experience, training, or cultural and organizational norms
- Not rejecting hypotheses that do no longer fit the situation; not questioning data completeness
- Evidence evaluation
  - Greater faith placed in evidence that the analyst collected or experienced
  - Absence of evidence = Evidence of absence
  - Inability to incorporate levels of confidence into decision making

Several research studies have refuted this assumption by relating decision performance to include reduced timelines, criticality of decision, visibility of decision maker, experience, etc. [20, 67–69]. This class of problems are often called time-critical decision making. Time-critical decisions in humans are often characterized by the following:

- Decreased emphasis on identifying and tracking alternatives
- Exaggerated influence on negative data
- Pieces of available evidence are often missed or not accounted for during the decision process
- Tendency toward automated decisions; faster than actually required
- Mistakes tend to grow dramatically even for low-complexity situations
- Increased time allocated to the wrong step in the decision process

Analysts operating in a time-critical decision making environment will be affected by their personality towards risk; i.e., being risk-averse, risk-neutral, or risk prone. Also, the decision maker's presence in the environment is a factor along with their ability to evaluate the situation. However, the research shows that decision making within a stressed environment can be improved through training. The training should contain four elements: increasing the individual's knowledge base, develop policies and procedure so the individual has a cognitive look up table, perform tasks in simulated stressful environments, and provide cognitive tools for handling stress. The goal is to change the decision maker's process from cognitive to automatic [70].

Assumption 5 Context Decisions are Actionable

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 [71]. 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 [72, 73]. Graph representations require simplifications to demonstrate relationships [74], which may mask other interactions [75, 76]. 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 [77]. The concept is called time-sensitive computing (Fig. 5.8). 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 [78]. So, the algorithms operate until either the performance threshold or the available time has been met.

Assumption 6 Context Errors can be fully Quantified

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

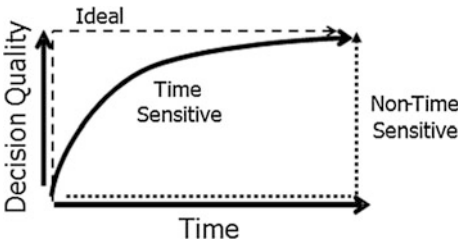

Fig. 5.8 Data structures for knowledge types time versus decision quality for computational strategies (adapted from [78])

metrics can be combined to match the system level performance measures (Fig. 5.4—Error arrow). Error analysis does not provide any information for decision relevance [79].

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.

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 [80] 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) [81] is investigating these issues for both context analysis and future interoperable standards [82].

5.4 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 is used for evidence accumulation. We seek to address the assumptions: (6) quantifiable, (5) actionable, (4) reproducible, (3) use of context data, (2) acquirable, and (1) specific for which we use evidence theory through Proportional Conflict Redistribution (PCR).

Recently, [83] 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. Yen

[84] developed methods to account for nonuniform priors. Others have also tried to compare Bayes and evidential reasoning (ER) methods [85]. Assuming that we have multiple measurements $Z = \{Z_1, Z_2, \ldots, Z_N\}$ for cyber detection D being monitored, Bayesian and ER methods are developed next.

5.4.1 Relating Bayes to Evidential Reasoning

Using the derivation by Dezert [83], assuming conditional independence, one has the Bayes method:

$$P(X|Z_1 \cap Z_2) = \frac{P(X|Z_1)P(X|Z_2)/P(X)}{\sum_{i=1}^{N} P(X_i|Z_1)P(X_i|Z_2)/P(X_i)} \tag{5.1}$$

With no information from Z_1 or Z_2, then $P(X \mid Z_1, Z_2) = P(X)$. Without Z_2, then $P(X \mid Z_1, Z_2) = P(X \mid Z_1)$ and without Z_1, then $P(X \mid Z_1, Z_2) = P(X \mid Z_2)$. Using Dezert's formulation, then the denominator can be expressed as a normalization coefficient:

$$m_{12}(\varnothing) = 1 - \sum_{X_i; X_j | X_i \cap X_j} P(X_i|Z_1)\mathrm{P}(X_i|Z_2) \tag{5.2}$$

Using this relation, then the total probability mass of the conflicting information is

$$P(X|Z_1 \cap Z_2) = \frac{1}{1 - m_{12}(\varnothing)} \cdot P(X|Z_1)P(X|Z_2) \tag{5.3}$$

which corresponds to Dempster's rule of combination using Bayesian belief masses with uniform priors. When the prior's are not uniform, then Dempster's rule is not consistent with Bayes' Rule. For example, let $m_0(X) = P(X)$, $m_1(X) = P(X \mid Z_1)$, and $m_2(X) = P(X \mid Z_2)$, then

$$m(X) = \frac{m_0(X)\, m_1(X)\, m_2(X)}{1 - m_{012}(\varnothing)} = \frac{P(X)\, P(X|Z_1)\, P(X|Z_2)}{\sum_{i=1}^{N} P(X_i)P(X_i|Z_1)\, P(X_i|Z_2)} \tag{5.4}$$

Thus, methods are needed to deal with nonuniform priors and appropriately redistribute the conflicting masses.

5.4.2 *Proportional Conflict Redistribution*

Recent advances in DS methods include *Dezert-Smarandache Theory* (DSmT). DSmT is an extension to the Dempster–Shafer method of ER which has been detailed in numerous papers and texts [86]. In [87] are introduced the methods for reasoning and presented the hyper power-set notation for DSmT [88]. Recent applications include the DSmT Proportional Conflict Redistribution rule 5 (PCR5) applied to target tracking [89].

The key contributions of DSmT are the redistributions of masses such that no refinement of the frame Θ is possible unless a series of constraints are known. For example, Shafer's model [90] is the most constrained DSm hybrid model in DSmT. Since Shafer's model, authors have continued to refine the method to more precisely address the combination of conflicting beliefs [91] and generalization of the combination rules [92, 93]. An adaptive combination rule [94] and rules for quantitative and qualitative combinations [95] have been proposed. Recent examples for sensor applications include electronic support measures, [96], physiological monitoring sensors [97], and seismic-acoustic sensing [98].

Here we use the *Proportional Conflict Redistribution* rule no. 5 (PCR5). We replace Smets' rule [99] by the more effective PCR5 to cyber detection probabilities. All details, justifications with examples on PCR*n* fusion rules and DSm transformations can be found in the DSmT compiled texts [86]. A comparison of the methods is shown in Fig. 5.9.

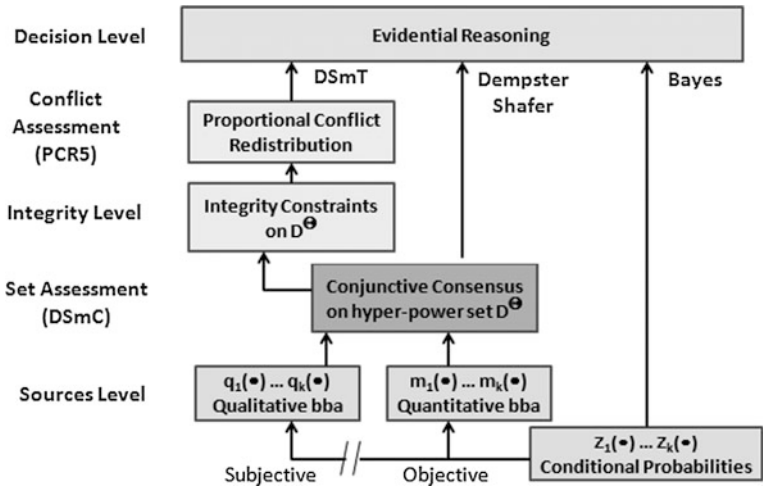

Fig. 5.9 Comparison of Bayesian, Dempster–Shafer, and PCR5 fusion theories

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 [86] for full justification and examples): $m_{\mathrm{PCR5}}(\varnothing) = 0$ and $\forall X \in 2^{\Theta} \backslash \{\varnothing\}$, where $\varnothing$ is the null set and 2^{Θ} is the power set:

$$m_{\mathrm{PCR5}}(X) = \sum_{\substack{X_1; X_2 \in 2^{\Theta} \\ X_1 \cap X_2 = X}} m_1(X_1) + m_2(X_2) + \sum_{\substack{X_2 \in 2^{\Theta} \\ X_2 \cap X = \varnothing}} \left[\frac{m_1(X_1)^2 m_2(X_2)}{m_1(X_1) + m_2(X_2)} + \frac{m_1(X_1) m_2(X_2)^2}{m_1(X_1) + m_2(X_2)} \right] \tag{5.5}$$

where $\cap$ is the interesting and all denominators in the equation above are different from zero. If a denominator is zero, that fraction is discarded. Additional properties and extensions of PCR5 for combining qualitative BBAs can be found in [86] with examples and results. All propositions/sets are in a canonical form.

5.4.3 Threat Assessment from Context

In this 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 application system collects raw measurements on the data situation, such as Boston Bomber activities as an attack, (Assumption 2—acquirable). 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 5.10 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 20–27 s) while the situation is being assessed (threat or no threat);

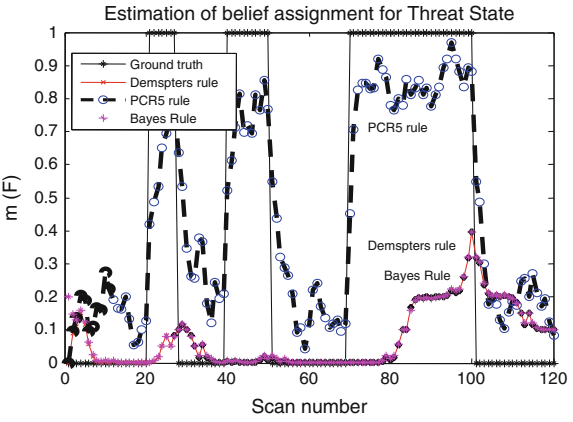

Fig. 5.10 Results of Bayesian, Dempster–Shafer, and PCR5 fusion theories for trust as a measure of a threat attack

followed by another repeated event (time 40–50 s). 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 70–100 s) from which a Bayesian method starts to indicate a change in the threat state.

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 intelligence agencies 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.

Trust is then determined with percent improvement in analysis for the state change. Since the classification of attack versus no attack is not consistent, there is some conflict in the processing of the measurement data going from an measurements of attack and vice versa. The constant changing of measurements requires acknowledgment of the change. The initial conflict in the reported evidence requires the data conflict as measured from which the PCR5 method better characterizes the information—leading to improved trust in the fusion result.

The improvement of PCR5 over Bayes is shown in Fig. 5.11 and compared with the modest improvement from DS. The average performance improvement of PCR5 is 50 % and DS is 1 %, which is data, context, and application dependent. When comparing the results, it can be seen that when a system goes from a normal to an attack state, PCR5 responds quicker in analyzing the attack, resulting in maintaining trust in the decision. Such issues of data reliability, statistical credibility, and application survivability all contribute to the presentation of information to an application-based user. While the analysis is based on behavioral situation

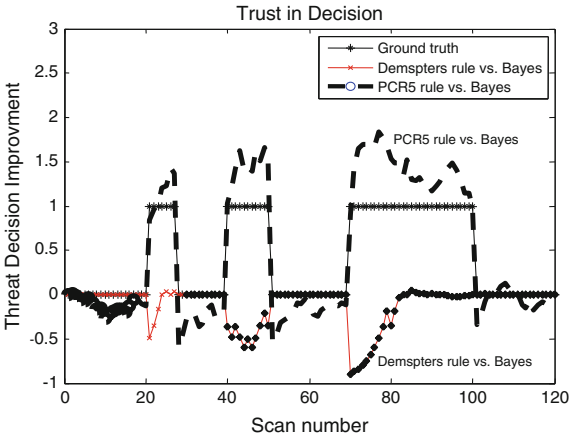

Fig. 5.11 Results of Bayesian, Dempster–Shafer, and PCR5 fusion theories for threat detection improvement

awareness, it is important to leverage context, but also be aware when the contextual factors are not complete, hence conflict.

5.5 Discussion

The chapter explicitly identified the common assumptions incorporated into computational decision engines. The assumptions at each functional block propagate through the system and dramatically affect the utility of their output. In the case of threat assessment, these assumptions could lead to intelligence failures. Context is important, but not completely measureable in a timely method. By understanding these assumptions, system users can mitigate these pitfalls by employing skepticism and confirmation in the results. The notional example provided a method of a change in the threat state that would aid in emergency response.

5.6 Conclusions

We outlined the analysis of threat assessment given the context of the situation. Threat analysis needs were juxtaposed against the assumptions developers use to make the computational decision support system tractable. We showed that the long-term system goals have some very real near-term realities. We organized the contextual information for threat analysis by categorizing six assumptions: (1) specific problem, (2) acquirable data, (3) use of context, (4) reproducible analysis, (5) actionable intelligence, and (6) quantifiable decision making. 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.

We hope that we enlighten users of tools to question the accuracy and relevance of the computer generated analysis. Likewise, we hope that developers better understand the user's needs of these tools in an operational environment. Context for threat assessment must be discernible by both the machine and the user.

Acknowledgments 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. A.N. Steinberg, Foundations of situation and threat assessment, Chap. 18, in *Handbook of Multisensor Data Fusion*, ed. by M.E. Liggins et al. (CRC Press, London, 2009)
2. T.X. Hammes, *The Sling and the Stone: On War in the 21st Century* (Zenith Press, 2006)
3. J. Leachtenauer, National Imagery Interpretability Ratings Scales: Overview and Product Description. *American Society of Photogrammetry and Remote Sensing Annual Meetings*, pp. 262–271, 1996
4. J.M. Irvine, National imagery interpretability rating scales (NIIRS): overview and methodology, in *Proceedings of SPIE,* vol. 3128 (1997)
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, in *Proceedings of SPIE*, vol. 6209 (2006)
6. J.T. Picarelli, Transnational threat indications and warning: the utility of network analysis, in *AAAI Fall Symposium on Artificial Intelligence and Link Analysis Technical Report* (1998)
7. D. Galula, *Counterinsurgency Warfare: Theory and Practice* (Praeger Security International, Westport, 1964)
8. R. Trinquier, *Modern Warfare: A Frenchy View of Counterinsurgency* (Praeger Security International, Westport, 1964)
9. R.K. Betts, Analysis, war, and decision: why intelligence failures are inevitable. World Polit. **31**, 61–89 (1978)
10. D.L. Thomas, Proving constructive possession in Virginia: a change in the tradewinds. Colonial Lawyer **18**, 137–166 (1989)
11. S.A. Israel, Toward a common lexicon for exploiting activity data, in *IEEE Applied Imagery and Pattern Recognition Workshop: Computer Vision: Time for Change*, pp. 6 pages (2012)
12. Y. Altshuler, N. Aharony, A. Pentland, Y. Elovici, M. Cebrian, Stealing reality: when criminals become data scientists (or vice versa). IEEE Intell. Syst. 2–10 (2011)
13. C.R. Vincente, D. Freni, C. Bettini, C.S. Jensen, Location-related privacy in geo-social networks. IEEE Internet Comput. 20–27 (2011)
14. R. Colbaugh, K. Glass, J. Gosler, Some intelligence analysis problems and their graph formulations. Intell. Community Res. Dev. **315**, 27 (2010)
15. A. Vinciarelli, Capturing order in social interactions. IEEE Signal Process. Mag. 133–152 (2009)
16. J. Jonas, Threat and fraud intelligence, Las Vegas style. IEEE Secur. Priv. 28–34 (2006)
17. A.E. Gattiker, F.H. Gebara, A. Gheith, H.P. Hofstee, D.A. Jamsek, J. Li, E. Speight, J.W. Shi, G.C. Chen, P.W. Wong, Understanding system and architecture for big data. IBM, pp. 4 pages (2012)
18. C.Y. Lin, L. Wu, Z. Wen, H. Tong, V. Griffiths-Fisher, L. Shi, Social network analysis in enterprise. Proc. IEEE **100**(9), 2759–2776 (2012)
19. M.J. Duggin, C.J. Robinove, Assumptions implicit in remote sensing data acquisition and analysis. Int. J. Remote Sens. **11**, 1669–1694 (1990)

20. R. Johnston, *Analytic Culture in the US Intelligence Community: An Ethnographic Study* (Center for Study of Intelligence, Central Intelligence Agency, Washington, 2005), pp. 173 pages
21. D. Chaikin, Network investigations of cyber attacks: the limits of digital evidence. Crime Law Social Change **46**, 239–256 (2006)
22. S.A. Macskassy, F. Provost. A brief survey of machine learning methods for classification in networked data and an application to suspicion scoring, in *Workshop on Statistical Network Analysis at the 23rd International Conference on Machine Learning* (2006)
23. J.H. Ratcliffe, *Intelligence-Led Policing* (Willan Publishing, Cullompton, Devon, 2008)
24. I. Sakharova, Al Qaeda terrorist financing and technologies to track the finance network, in *IEEE Intelligence and Security Informatics* (2011)
25. J. Nagl, *Learning to Eat Soup with a Knife: Counterinsurgency Lessons from Malaya and Vietnam* (Praeger Publishers, Westport, 2002)
26. 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)
27. G.F. Treverton, *Intelligence for an Age of Terror* (Cambridge University Press, New York, 2009)
28. S. Ressler, Social network analysis as an approach to combat terrorism: past, present, and future research. Homel. Secur. Affairs **2**, 10 (2006)
29. V.E. Krebs, Mapping networks in terrorist cells. Connections **24**, 43–52 (2002)
30. 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)
31. B. Bringmann, M. Berlingerio, F. Bonchi, A. Gionis, Learning and predicting the evolution of social networks. IEEE Intell. Syst. 26–24 (2010)
32. R. Travers, The coming intelligence failure. Studies in Intelligence (CIA) **40**, 35–43 (1997)
33. T.J. Burger, Inside the Nerve Center of America's counterterrorist operations, in *Time Magazine* (2004)
34. M.S. Granovetter, The strength of weak ties. Am. J. Sociol. **78**, 1360–1380 (1973)
35. M.K. Sparrow, The application of network analysis to criminal intelligence: an assessment of the prospects. Soc. Networks **13**, 251–274 (1991)
36. P. Buneman, S. Khanna, W.C. Tan, Data provenance: some basic issues. Found. Softw. Technol. Theor. Comput. Sci. 87–93 (2000) Springer
37. E. Blasch, A. Jøsang, J. Dezert, P.C.G. Costa, K.B. Laskey, A.-L. Jousselme, URREF self-confidence in information fusion trust, in *International Conference on Information Fusion* (2014)
38. E.H. Powley, Reclaiming resilience and safety: resilience activation in the critical period of crisis. Hum. Relat. **62**, 1289–1326 (2009)
39. N. Eagle, Behavioral inference across cultures: using telephones as a cultural lens. IEEE Intell. Syst. 62–64 (2008)
40. S. Milgram, The small-world problem. Psychol. Today **1**, 61–67 (1967)
41. G. Lawton, Invasive software, who's inside your computer. IEEE Comput. **35**, 15–18 (2002)
42. S. Graham, The urban battlespace. Theor. Cult. Soc. **26**, 278–288 (2009)
43. S. Saavedra, F. Reed-Tsochas, B. Uzzi, Asymmetric disassembly and robustness in declining networks. Proc. Natl. Acad. Sci. **105**, 16466–16471 (2008)
44. H. Sundaram, Y.R. Lin, M. DeChoudhruy, A. Kelliher, Understanding community dynamics in online social networks. IEEE Sign. Proc. Mag. 33–40 (2012)
45. B. Kahler, E. Blasch, L. Goodwon, Operating condition modeling for ATR fusion assessment, in *Proceedings of SPIE*, vol. 6571 (2007)
46. B. Kahler, E. Blasch, Sensor management fusion using operating conditions, in *Proceedings of IEEE National Aerospace Electronics Conference (NAECON)* (2008)
47. S. Rassler, Data fusion: identification problems, validity, and multiple imputation. Austrian J. Stat. **33**, 153–171 (2004)

48. I. Bloch, A. Hunter, Fusion: general concepts and characteristics. Int. J. Intell. Syst. **16**, 1107–1134 (2001)
49. D.L. Hall, *Mathematical Techniques in Multisensor Data Fusion* (Artech House) (1992)
50. J. Llinas, C. Bowman, G. Rogova, A. Steinberg, E. Waltz, F. White, Revisiting the JDL data fusion model II, in *International Conference on Information Fusion* (2004)
51. E. Blasch, Sensor, User, mission (SUM) resource management and their interaction with level 2/3 fusion, in *International Conference on Info Fusion* (2006)
52. E. Blasch, E. Bosse, E. Lambert, *High-Level Information Fusion Management and Systems Design* (Artech House, Norwood, MA, 2012)
53. 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 Aerosp. Electron. Syst. Mag. **27**(9) (2012)
54. E. Blasch, A. Steinberg, S. Das, J. Llinas, C.-Y. Chong, O. Kessler, E. Waltz, F. White, Revisiting the JDL model for information exploitation, in *International Conference on Info Fusion* (2013)
55. C. Drummond, Replicability is not reproducibility: nor is it good science, in *26th ICML Evaluating Methods for Machine Learning*, pp. 4 pages (2009)
56. E. Blasch, C. Banas, M. Paul, B. Bussjager, G. Seetharaman, Pattern activity clustering and evaluation (PACE), in *Proceedings of SPIE*, vol. 8402 (2012)
57. R.O. Duda, P.E. Hart, D.G. Stork, *Patten Classification*, 2nd edn. (Wiley, New York, 2001)
58. 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, in *ODD '13 Proceedings of the ACM SIGKDD Workshop on Outlier Detection and Description*, pp. 40–45 (2013)
59. J.M. Irvine, S.A. Israel, A sequential procedure for individual identity verification using ECG. EURASIP J. Adv. Signal Process. Recent Adv. Biometric Syst. A Signal Process. Perspect. **243215**, 13 (2009)
60. A. Wald, *Sequential Analysis* (Dover, New York, 1994)
61. C.E. Callwell, *Small Wars: Their Principles and Practice* (University of Nebraska Press, 1906)
62. J.R. Hipp, A. Perrin, Nested loyalties: local networks' effects on neighbourhood and community cohesion. Urban Stud. **43**, 2503–2523 (2006)
63. J.D. Lee, K.A. See, Trust in automation: designing for appropriate reliance. Hum. Factors **46**, 50–80 (2004)
64. R. Parasuraman, V. Riley, Performance consequences of automation induced complancey. Int. J. Aviat. Psychol. **3**, 1–23 (1993)
65. E.J. Ploran, S.M.M. Nelson, K. Velanova, D.I. Donaldson, S.E. Petersen, M.E. Wheeler, Evidence accumulation and the moment of recognition: dissociating decision processes using fMRI. J. Neurosci. **27**, 11912–11924 (2007)
66. D.M. Trujillo, Are intelligence failures inevitable? *e-International Relations* (2012)
67. S. Brown, M. Steyvers, E.J. Wagenmakers, Observing evidence accumulation during multi-alternative decisions. J. Math. Psychol. **53**, 453–462 (2009)
68. A. Neal, P.J. Kwantes, An evidence accumulation model for conflict detection performance in a simulated air traffic control task. Hum. Factors **51**, 164–180 (2009)
69. C.F. Chabris, D.I. Laibson, C.L. Morris, J.P. Schuldt, D. Taubinsky, The allocation of time in decision-making. J. Eur. Econ. Assoc. **7**, 628–637 (2009)
70. I. Cohen, Improving time-critical decision making in life threatening situations: observations and insights. Decis. Anal. **5**, 100–110 (2008)
71. E. Agichtein, C. Castillo, D. Donato, A. Gionis, G. Mishne, Finding high-quality content in social media, in *Web Search and Web Data Mining* (ACM, Palo Alto, 2008)
72. A.M. MacEachren, *Some Truth with Maps: A Primer on Symbolization and Design* (American Association of Geographer, 1994)
73. M. Monmonier, *How to Lie with Maps*, 2nd edn. (University of Chicago Press, 1996)

74. R. Amar, J. Eagan, J. Stasko, Low-level components of analytic activity in information visualization, in *IEEE Symposium on Information Visualization*, Minneapolis, pp. 111–117 (2005)
75. A. Perer, B. Shneiderman, Balancing systematic and flexible exploration of social networks. IEEE Trans. Vis. Comput. Graphics **12**, 693–700 (2006)
76. Z. Shen, K.L. Ma, T. Eliassi-Rad, Visual analysis of large heterogeneous social networks by semantic and structural abstraction. IEEE Trans. Vis. Comput. Graphics **12**, 1427–2439 (2006)
77. E. Blasch, Introduction to level 5 fusion: the role of the user, Chap. 19, in *Handbook of Multisensor Data Fusion,* 2nd edn., ed by M.E. Liggins, D. Hall, J. Llinas (CRC Press, 2008)
78. S. Zilberstein, An anytime computation approach to information gathering, in *AAAI Spring Symposium Series on Information Gathering from Distributed, Heterogeneous Environments* (1995)
79. S.A. Israel, Performance metrics: how and when. Geocarto Int. **21**, 23–32 (2006)
80. E. Blasch, P. Valin, E. Bossé, Measures of effectiveness for high-level fusion, in *International Conference on Info Fusion* (2010)
81. P.C.G. Costa, K.B. Laskey, E. Blasch, A.-L. Jousselme, Towards unbiased evaluation of uncertainty reasoning: the URREF ontology, in *International Conference on Information Fusion* (2012)
82. 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), in *International Conference on Information Fusion* (2013)
83. J. Dezert, Non-bayesian reasoning for information fusion—a Tribute to Lofti Zadeh. submitted to J. Adv. Inf. Fusion (2012)
84. J. Yen, A reasoning model based on the extended Dempster Shafer theory, in *National Conference on Artificial Intelligence* (1986)
85. E. Blasch, J. Dezert, B. Pannetier, Overview of Dempster-Shafer and belief function tracking methods, in *Proceedings of SPIE*, vol. 8745 (2013)
86. J. Dezert, F. Smarandache, Advances and applications of DSmT for information fusion (collected works), vols. 1–3 (American Research Press, 2009) http://www.gallup.unm.edu/~smarandache/DSmT.htm
87. J. Dezert, Foundations for a new theory of plausible and paradoxical reasoning. Inf. Secur. Int. J. **9** (ed. by Prof. Tzv. Semerdjiev)
88. J. Dezert, F. Smarandache, On the generation of hyper-powersets for the DSmT, in *International Conference on Info Fusion* (2003)
89. E. Blasch, J. Dezert, B. Pannetier, Overview of dempster-shafer and belief function tracking methods, in *Proceedings SPIE*, vol. 8745 (2013)
90. G. Shafer, *A Mathematical Theory of Evidence* (Princeton University Press, Princeton, NJ, 1976)
91. A. Josang, M. Daniel, Strategies for combining conflict dogmatic beliefs, in *International Conference on Information Fusion* (2006)
92. F. Smaradache, J. Dezert, Information fusion based on new proportional conflict redistribution rules, in *International Conference on Information Fusion* (2005)
93. M. Daniel, Generalization of the classic combination rules to DSm hyper-power sets. Inf. Secur. Int. J. **20**, 4–9 (2006)
94. M.C. Florea, J. Dezert, P. Valin, F. Smarandache, A.-L. Jousselme, Adaptive combination rule and proportional conflict redistribution rule for information fusion, in *COGIS '06 Conference* (2006)
95. A. Martin, C. Osswald, J. Dezert, F. Smarandache, General combination rules for qualitative and quantitative beliefs. J. Adv. Inf. Fusion **3**(2) (2008)
96. P. Djiknavorian, D. Grenier, P. Valin, Approximation in DSm theory for fusing ESM reports, in *International Workshop on Belief functions* (2010)
97. Z.H. Lee, J.S. Choir, R. Elmasri, A static evidential network for context reasoning in home-based care. IEEE Trans. Sys. Man Cyber-Part A Syst. Hum. **40**(6), 1232–1243 (2010)

98. E. Blasch, J. Dezert, P. Valin, DSMT applied to seismic and acoustic sensor fusion, in *Proceedings of IEEE National Aerospace Electronics Conference (NAECON)* (2011)
99. P. Smets, Analyzing the combination of conflicting belief functions, in *International Conference on Information Fusion* (2005)