The 16th International Command and Control Research and Technology Symposium (ICCRTS)
21-23 June 2011, Quebec City, Canada
"Collective C2 in Multinational Civil-Military Operations"

Paper No.22

Deception Detection in Multicultural Coalitions: Foundations for a Cognitive Model

Track 3: Information and Knowledge Exploration

Authors: Joan Kaina, Marion G. Ceruti, Ph.D., Kevin Liu,
Scott C. McGirr, Ph.D., and James B. Law, Ph.D.

Organization: Space and Naval Warfare Systems Center Pacific (SSC Pacific)

Address: 53560 Hull Street, San Diego, CA 92152-5001, USA, (619) 553-4068

Email: joan.kaina@navy.mil, marion.ceruti@navy.mil, kevin.liu1@navy.mil,
scott.mcgirr@navy.mil, jim.law@navy.mil

Marion G. Ceruti, Ph.D., Point of Contact
(619) 553 4068

Filename: Kaina et al. COGDECEP.22.16thICCRTS.2011.v25

Deception Detection in Multicultural Coalitions: Foundations for a Cognitive Model

Joan Kaina, Marion G. Ceruti, Ph.D., Kevin Liu, Scott C. McGirr, Ph.D., and James B. Law, Ph.D.
Space and Naval Warfare Systems Center Pacific (SSC Pacific)
53560 Hull Street, San Diego, CA 92152-5001, USA
joan.kaina@navy.mil, marion.ceruti@navy.mil, kevin.liu1@navy.mil, scott.mcgirr@navy.mil

Abstract— Decision makers in command centers need better methods to deal with deceptive information before it influences and degrades the outcome of command decisions. Deception poses unique threats to coalitions that are less likely to occur with individual forces. Coalitions also offer diverse viewpoints and approaches to dealing with deception. Cognitive vulnerabilities and limitations and the degree to which one can be deceived depend on both context and culture. This paper considers ontology of deception, themes of deception, and describes a deception-detection model based on preparation, detection and reaction. Cognition plays a central role in deception because the deceiver attempts to manipulate the target into believing something that is not true. The domain of deception and deception detection involves identifying physical and verbal discrepancies as well as inconsistencies in information or context, as well as the use of nonverbal cues. A cognitive approach is discussed that considers personality, cultural, and organizational factors that affect the heuristics of deception and its detection. The paper shows how the model applies in a discussion about deception detection in coalitions, including deception about group membership. The paper concludes with directions for future research.

I. Introduction

In coalition operations involving multiple countries with the participation of multiple levels of government, as well as civil and private organizations, the strength of the resulting team depends on unique functions and capabilities that each group contributes to the effort. Although these diverse teams are stronger due to the unique contributions of many, this strength is offset partially by the challenges of greater complexity. One of these challenges consists of increased opportunities for adversaries to practice deception. Coalitions must be aware of this to ensure the effectiveness of Command, Control, Communications, Computers, Intelligence and Surveillance (C^4ISR) infrastructure and operations.

Deception has been defined in a variety of ways, as reported in [12]. The general consensus of opinion among researchers is that deception is a deliberate attempt to mislead another [12], without reference to the mode of deception, e.g. verbal or graphic. More specifically, it also has been defined as an intentional verbal message that does not reflect honestly an individual's actual opinion [46]. Deception has been studied throughout history. A wide variety of deception and deception-detection studies have been reported in the literature. In ancient China, strategist and philosopher Sun Tzu is credited with having expounded military strategy [34]. Later, in renaissance Italy, philosopher and author, Machiavelli, described the politics of war and maintaining dominance in society [30]. Both authors wrote separate books titled *The Art of War* [30], [34]. These innovators of military science offered much insight into military strategy. They viewed military strategy as a physical process based on ideas and developed theories based on observations [34], [38]. The importance of deception in military strategy has long been well known. (See, for example, [7], [10], [19] and [26].) Sun Tzu alluded to deception in his *Thirteenth Chapter: The 22 Spies* [34]. Although the necessity of deception for a successful military campaign was well understood, the details of deception remained ambiguous. Research in deception during the World War II timeframe stimulated great interest in the mechanics and underlying themes of deception for both the Allied and the Axis powers. Whaley considered wartime deception in detail in his deception models [38], incorporating many basic concepts, such as cognition.

Information acquisition as we know it and its importance to deception obviously were not considered in the days of Sun Tzu. More recently, the deception-detection studies, models, approaches, and frameworks have focused on various aspects of computer automation [13], [17], [43], [44], [45]. Some of these include the automated support for group deception detection [13], [17] in particular. Lambert's cognitive model has explored deception detection from the target's point of view [24]. (N.B. The "target" is the entity to whom the deception is directed.) Furner and George found that the best way to hinder deception depends not only on the receiver, but also on the medium [16]. Face-to-face communication is considered the richest communication medium [16], [17] due to the presence of multiple nonverbal [23], [46] as well as verbal [43], [44], [45] cues that are not all present in text.

However, the detection of meaningful facial-pattern changes is much more difficult to automate than textual analysis because facial expressions are more difficult to quantify than, say, word counts. For example, Zhou and coworkers [43], [44], [45] considered deception in text-based computer-mediated communication, a medium that is much more amenable to the automated analysis of large data sets than is deception in face-to-face communications, which tend to occur in one-on-one encounters. (See, for example [15].) Tilley and co-workers found that females were better than males at detecting deception in electronic media [33]. Two research groups [13] [17] studied deception detection during a group-based collaboration, which could prove useful for applications in coalition command and intelligence centers.

Building on the works mentioned above, this paper represents a step toward a cognitive deception-detection model. Part of this investigation is to explore the connection between cognitive reasoning and a deception theory. (See for example, [2], [7], [14], [18] and [24].) We believe that a reliable deception-detection model must be based on cognitive themes. Cognitive effectors have a subconscious influence on the heuristics of an individual. If these effectors can be measured and their influence on heuristics, tracked, the vital deception points in an information system can be determined and monitored [2], [16]. This paper considers a high-level deception-detection model based on preparation, deception, and reaction that can serve as a conceptual framework for cognitive effectors that influence heuristics.

The organization of this research paper is as follows. Section II outlines an ontology of deception. Section III describes deception theory and presents common deception themes. Section IV explores cognition and the use of heuristics. Section V describes an overview of a high-level deception-detection model called the Preparation, Deception and Reaction (PDR) model. Section VI describes some observations and hypotheses. Section VII suggests implications of deception detection in coalition command and intelligence centers. In this section describes some examples of practical use of the PDR model. Section VIII discusses group bias and detection challenges. Section IX considers deception detection regarding group membership. Section X describes the larger infrastructure necessary to support the use of the PDR model, as well as other deception models, in a model base, open-systems environment supported by a Service-Oriented Architecture (SOA). Finally, section XI suggests directions for future research in this area.

II. ONTOLOGY OF DECEPTION

An ontology of deception accounts for and provides relationships between various types of deception. It is based on an ontology or model of cognition, some elements of which were explored in [24]. An ontology of deception would inherit characteristics from several branches of a general, upper ontology, including the ontology of cognition. These branches are not necessarily orthogonal. A comprehensive ontology of deception will contain at least the following key concepts.

A. Upper ontology

1. Ontology of cognition
2. Ontology of behaviors

The ontology of deception belongs at this level, inheriting characteristics from both ontologies of cognition and behavior.

B. Middle ontology

1. Various domain ontologies can be used to help generate feature lists as search criteria in machine-learning tools and algorithms.

2. Application ontology is based on intents and tasks of analysts, who may be "users" of deception-detection automated tools. Analysts may be deception-detection agents or they may read reports from deception-detection agents.

C. Lower ontology

1. Data originate from multiple open sources where search methods are, or could be, automated.

2. Data from multiple open sources, not in machine-readable format.

3. Data from reports of specific human observers cannot always be automated, especially with the same speed as automatic data feeds from sensors.

Concept nodes in the ontology of deception include but are not limited to:

A. Types of Deception - What constitutes deception?

1. Verbal

a. Lies - statements that are intentionally false

b. Misleading statements - not exactly a lie but creates the wrong impression

c. Omission of important verbal details, the inclusion of which would change the target's perception about the facts of the situation.

2. Non Verbal

a. Self deception

i. Denial of facts and conclusions - ignoring what you don't want to believe

ii. Incorrect assumptions - making it easier to believe what is not true

iii. Belief of the unlikely - using uncertainty to justify a belief in something with a very low probability of truth (One cannot call it fact due to uncertainty.)

b. Camouflage

i. Image or object is embedded in like surroundings. This includes the addition of unexpected and non-obvious image or data.

ii. Hidden messages are embedded in text
- e.g. terrorist using the plan for a social event to disguise the plan for an IED placement. Here, the level of complexity of the text, the emotional tone of the speech or text, and the coherence of text are not likely to match what one would expect in social-event planning.

iii. Covert channel - using properties of words to communicate data, sometimes numerical, unrelated semantically to the words themselves. This low-bandwidth channel can be used to communicate key data. Three examples are as follows:

- "go south I fly land soon" = safe combination "25-13-44"
- "Worry and strife" = "wife"
- Modulating real-time file access (e.g. open and close) to represent 1s and 0s for the low-level transmission of ASCII

code. File open for a few seconds = 0; file open for 1 min. or longer = 1

c. Alteration of existing image - e.g. removal of blood stain from crime-scene digital image. This omission of what originally was present creates an incorrect impression.

d. False imagery creation - e.g. counterfeit bills

e. Partial imagery obscuration or masking to omit relevant details. Here, no alteration of image is needed. All that is necessary here is to hide or exclude the incriminating part.

3. Multi-agent deception

a. This type of deception involves two or more deceivers both aware of each other but one of whom also is deceived. For example, a high-ranking deceiver also may deceive a lower-ranking deceiver, in addition to deceiving the target. (N.B. The "deceiver" is the entity, usually a person or group of people who initiate a deception plan.)

B. Deception-detection methods and approaches

1. Behavior

a. Direct personal observation

The types of deception detection closely parallels the deception types described above. For example, one verbal cue that is said to signal lying is the presence (or absence [1]) of speech errors and the use of disfluent utterances (e.g. "um," "ah," and other filler words such as "you know" and "like"). More disfluencies can indicate a lie in the making, revealing the cognitive overload as the deceiver's attention is on the lie fabrication. No disfluencies could indicate a rehearsed lie [1]. On the other hand, people who do not speak well can use multiple disfluencies even in truthful speech. In this case, two opposite behaviors have been linked to deception. As a result, disfluent words probably are not reliable discriminators between deceivers and truthful people.

Direct personal observation of a potential deceiver involves at least two classes of cues - verbal and nonverbal cues. (See, for example, [46].) These are not orthogonal as nonverbal cues can be triggered from the vocal medium. In spite of the relative efficiency associated with the automated analysis of language using textual transcriptions, a growing body of research literature strongly suggests that nonverbal cues are significantly more important than strictly verbal information in deception detection. (See, for example, [11] and [15].) The following is a list of nonverbal cues [11], [15], [23] that have been used in deception detection with various degrees of success.

i. body language – cohesion with verbal content, overall body posture (e.g. leaning forward or backward), head movements, genuine and spontaneous vs. deliberate and contrived facial expression of emotions, symmetry, leakage through microexpressions, hand postures, dynamic gestures, finger tapping, fidgeting, covering one's mouth or face, eye-contact shifting, gaze duration, expression duration, speed of onset, blinking, and pupil-size variation.

ii. physiology – galvanic skin response, breathing, etc.

iii. acoustic vocal quality and variation – pitch, timbre, rate of articulation, latency of response, rhythmic or broken delivery pattern.

iv. chemical – odor, pheromones, etc.

v. emotional expressiveness and heightened arousal

Whereas all these are variables are independent of the verbal content of a message or statement, instantiations of these variables may correlate well with the content of a particular message or speech for a given scenario.

The deception-detection literature contains conflicting information regarding effective detection of deception using behavioral observations [11]. Some researchers report that specific cues have been useful whereas others did not attribute their detection rates to the same cues. No universal cue set has been discovered to date [11].

b. Indirect observation of deceiver in a recorded file

i. Voice analysis by linguists, acousticians, and psychologists can help detect cues in speech delivery associated with false content. This type of acoustic analysis is directed toward a class of nonverbal cues associated with variations in the sound of a person's voice.

ii. Similarly, cues regarding deception can be transmitted through body language. An analysis of these cues using video files could reveal obscure cues that otherwise might go undetected because of video's capability of multiple replay.

c. Observation of deceiver's artifacts

i. Text written by deceiver who intentionally created these artifacts can be studied using computational-linguistic analysis techniques, e.g. part-of-speech analysis, Linguistic Inquiry and Word Count (LIWC) such as searches on bigrams, trigrams. Style, mood, and register changes can be detected as anomalies above baseline using feature-extraction techniques. Moreover, the following linguistic cues have been studied [31] with respect to deception detection: the number of syllables, words, sentences, short sentences, and simple sentences; the vocabulary complexity; the sentence-level complexity; rates of adjectives and adverbs; level of informality as determined by the error rate. These and other cues can be linguistic cues to deception in some contexts.

ii. Personal items left behind in a location vacated by deceiver - unintentional exposure

iii. Covert audio tape or video tape. Here the deceiver is unaware of recording, therefore, does not attempt to conceal anything

iv. Deceiver does not "lie" per se, but de-emphasizes the salient features of the truth by separating them and hiding them in various places throughout voluminous text, thus making detection of the truth difficult. This fragmentation causes the truth to be hidden for all intents and purposes. Detecting this form of deception is very difficult because the task now becomes an exercise in truth detection in clutter for the deception-detection agent, sometimes called an "auditor," who must find the pieces, "connect the dots," and ascertain the truth. This form of deception could prevent the target from finding the truth in time to make crucial decisions. It also could delay truth discovery long enough for the adversary to escape or get the upper hand. (N.B. The "adversary" is the opponent of own forces, same as the "enemy." Usually, it is or includes the deceiver or some other hostile entity that would benefit from deception. It usually does not include an ingroup deceiver as any such individual is expected to be a member of the coalition, deception not withstanding.)

2. Non-behavioral discrepancy

a. Using observations for independent corroboration unrelated to what or how the deceiver communicates, e.g. report of observation of x at location y that is inconsistent with deceiver's report.

b. The deception-detection agent uses viewpoint verification to determine whether or not the deceiver possibly could be in a position to know the truth. For example, the deception-detection agent might reason that the deceiver could not have known certain information or observed certain events due to known the vantage point of the deceiver when the event occurred. This kind of deception detection is useful against a deceiver who attempts to cover up his or her lack of information, thus purporting to know facts that the deceiver could not have known.

3. Hypothesis generation occurs when the deception-detection agent forms multiple hypotheses to explain observations, one hypothesis of which is that the deceiver is lying or practicing some other form of deception described above. The deception-detection agent then tries to select the correct hypothesis by an analysis aimed at determining which hypothesis has the most corroborating evidence. This exercise can become another kind of detection-in-clutter task, depending on how many hypotheses were generated.

C. Deception deterrence

1. Validation and verification

2. Announced or predictable searches

D. Deception scenarios

1. Who? - Actors and agents

a. Deceiver - the dishonest person

b. Target - the person, group or organization that the deceiver attempts to deceive

c. Deception-detection agent - The person or software agent that tries to discover deception or attempted deception

d. Unaware deceiver – A person who passes on false information without knowing it is false. An unaware deceiver would not transmit false information intentionally. (N.B. According to an accepted definition of deception [13], an unaware deceiver does not qualify as a true deceiver because of the lack of awareness about the deception.)

e. Group deception - Two deceivers, unequal in rank, work as a team to deceive the target. The lower-ranking deceiver is unaware of certain facts known to the higher-ranking deceiver. The lower-ranking deceiver takes all the risks and if caught, will not know all the facts and can't possibly implicate the higher-ranking deceiver. Unlike the unaware deceiver, both deceivers in this case are aware of their participation in group deception.

2. How? - Modes of deception

a. Speech

i. In person - Body language and non-textual (e.g. pronunciation) cues are available, subject to interactive probes

ii. Recorded video - Body language and non-textual cues are available. This is not an interactive mode.

iii. Audio tape – Auditory, non-textual cues are available; body language is absent; not interactive

b. Chat - Informal text meant to be read at the time of writing; relies heavily on the context of the current situation.

c. Text - Formal text written to be read later verbatim relies less on context of the current situation.

d. Textual transcriptions of speech - Formal or informal speech written down, e.g. transcribed from a recording. A textual transcription reads differently from formal text.
{e.g. "...as I described earlier" (speech) vs. "...as indicated above" (written)}

3. Why? - deception objectives [3] [23],

a. Avoid capture and associated adverse consequences, such as physical harm

b. Avoid being punished

c. Protect another person from being punished

d. Infiltrate a group to gain access to proprietary information or other valuable assets

e. Influence behavior of others

f. Financial gain or some other reward

g. Win the admiration of others

h. Get out of an awkward social situation or avoid embarrassment

i. Avoid having to deal with a difficult situation

j. Maintain privacy

k. Gain competitive advantage over a target.

l. Exercise power over another

m. Because some deceivers cannot stop. Deception comes naturally and compulsively to pathological liars, who lie because of habit.

4. When? - e.g. Timelines can be used to refute false claims of causality when the cause follows the effect.

A substantial collection of examples of deceptions and deceptive techniques has been translated into a cognitive model for modeling deception in military situations [24]. These examples are arranged in the model into categories of cognitive levels [24]. The model includes the following actions: sense, perceive feature, perceive form, associate, define the problem, observe the situation, define the problem-solving status (i.e. form an hypothesis), determine solution options, begin to respond, direct, implement form, implement feature, and drive affectors. Reflexes, conditioned behavior, intuition, perception at higher and lower levels, and memory also are included in the model [24].

III. Deception theory

To select or develop a model for deception detection, one must understand the concepts of deception described above and how an enemy may use deception to influence a target. Modern deception theory and experiments have increased our knowledge and awareness of deceptive material and cues, such as those in speech delivery associated with false content as described above. For example, Waltz and Bennett [37] considered significant innovations of modern deception theory and extracted the common themes. Figure 1 shows an overview of these common deception themes.

Deception begins with an objective. What would the deceiver like to gain from their interaction with the target? The main goal of deception is to gain a competitive advantage over a target. Therefore, the deception objective was to either hide critical information from the target or make the target believe false information.

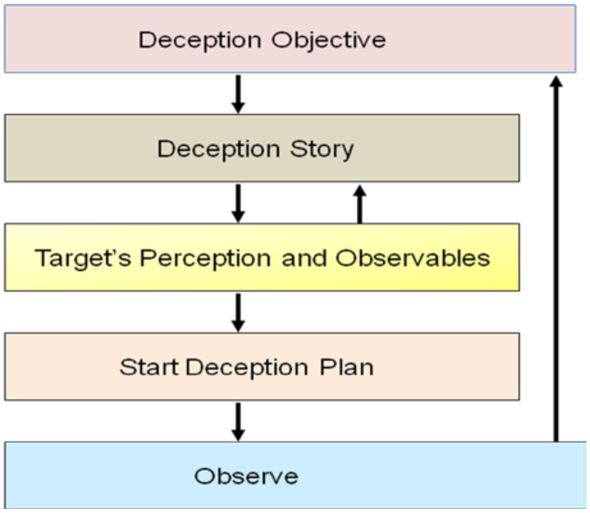

Figure 1. Common deception themes

The next step in most deception models is to create a 'deception story' that consists of the scripted events that the deceiver would like to implement in their deception scheme [9] [37]. The deceiver creates a scenario specifying the type of actions that the deceiver, the target, and any outside forces will perform. This could include, for example, the creation of deceptive information that will be presented to the target. The deceiver may plan on using deceptive tactics such as a lure or an 'accidental' mistake [10], [25], [28], [37]. These tactics and others are the methods of exposing the falsified information to the target. Then, the deceiver will try to anticipate and account for what the target or any outside force might do.

After fabricating a deception story, the deceiver must try to understand the target's perceptions and what the target might observe. In some cases, the deception "story" might consist of an image with alterations. After the deception plan has started, it is up to the target to interpret what, if any, information the deceiver has falsified or omitted. If the target does not find the information credible, or is incapable of receiving the data, the deception will fail [37]. Here the deceiver must interpret the cognition of the target to predict how the target will perceive, interpret, and react to the information. If the deception story does not induce or coerce the desired actions from the target, the deceiver must rework the deception story [37]. All of this is done before the start of the deception plan because after the plan has been initiated, it cannot be altered.

After refining the deception story, the deception plan is executed. This entails enacting the tactics outlined by the deception story, or simply making the false image available to the target. The final step of the deception model for the deceiver is to observe [37] the situation to verify the results of the deception. Here, the data gathered will be used to determine whether the deceiver's perception of the target's reasoning is correct. If the target reacts in the predicted manner, the deceiver assumes that the deception was successful. If the target displays an unexpected reaction, most likely the deception story has failed. This is because either the deception story needed more refinement, or the circumstances of the target have changed, i.e. the target has obtained information that was not available to the deceiver at the time when the plan was formulated.

The next step is to determine the actions after deception. If the initial deception were successful, another deception may be required, or the target may be in a position to be exploited.

IV. COGNITION AND THE USE OF HEURISTICS

Cognition is defined as the act or process of knowing, which includes both awareness and judgment [35]. Cognition also involves perception, learning, recall, and reasoning. Cognitive concepts constitute the underpinnings of the common deception themes in Figure 1.

Table 1: List of common heuristics used in various contexts

Heuristics [2] [6] [10] [16] [18] [47]	**Definition**
Overconfidence	Overestimation of the probability of being right
Availability	Using easily available examples as references
Restriction of search domains	When solving a complex problem and resources (e.g., time, materials, money, personnel, etc.) are limited, the search space for the solution must be restricted to that most likely to yield the desired result using the least amount of resources.
Anchoring and adjustment	Establishing or declaring an arbitrary basis and adjusting around that point
Framing (i.e. setting a frame of reference or point of view)	Emphasizing aspects that are consistent with one's beliefs, values, attitudes, & models, while minimizing or ignoring aspects that are inconsistent with that viewpoint.
Oversensitivity to consistency	Seeing a pattern in noise
Frequency	Approaches with a higher frequency of success (or failure) come to mind before approaches with lower frequencies success (or failure).
"Law" of small numbers	Extrapolation of results from a small population to a larger population
Perceptual resistance to change	After a conclusion has been reached, it is difficult to change.

To a great extent, the success or failure of a deception operation, or, conversely, deception-detection task will depend on the operation or task complexity, the extent to which cognitive factors have been taken into account, and the cognitive overload that results from the deception or detection process. Both the deceiver and the deception-detection agent can experience cognitive overload.

Heuristics often involve mental shortcuts to enable problem solvers to simplify cognitively complex tasks that involve assessment of probability and prediction. This is a form of task reduction [5]. By definition, heuristic methods are used either because they have been found to work or because they are expected to work apart from any other justification for their use beyond simplification [36]. For example, heuristics for solving or simplifying some classes of problems in mathematics and physical sciences, and social sciences are used when more analytical methods are deemed intractable.

Table 1 lists common heuristics, some of which are based on questionable "logic" and lead to errors. Experts and novices use different heuristics [5]. Experts use more sophisticated heuristics and they tend to avoid heuristics that lead to errors whenever this is possible. All problem solvers run the risk of being overwhelmed with complexity, but novices reach this point much sooner than experts will. When the number and nature of the variables and their interactions are unknown, the use of heuristics is often the only recourse.

Table 2: Examples of factors that can affect heuristics, as well as when and if to use heuristics

Cognitive Factors [13]	**Definition**
Arousal	Degree to which the individual is active or passive
Power	Dominant or submissive. This factor relates to the expert-novice difference.
Pleasantness	Pleasant or unpleasant
Intensity	Tense or relaxed
Personality Traits [22], [27]	
Extroversion vs. introversion	Sociable, assertive, playful vs. aloof, reserved, shy
Emotional stability vs. neuroticism	Calm, unemotional vs. insecure, anxious (Similar to intensity)
Agreeable vs. disagreeable	Friendly, cooperative vs. antagonistic, faultfinding (Similar to pleasantness)
Conscientiousness	Self disciplined, organized vs. inefficient, careless
Openness to experience (ability to analyze situations & recognize potential)	Intellectual, insightful, vs. shallow, unimaginative This factor also relates to the expert-novice difference.
Organization Factors [2] [14] [16] [18] [21] [32]	
Collectivism and trust	Value and trust of relationship of people in the network
Power distance	Degree of separation (e.g. equality or inequality) between individuals at adjacent or other levels of rank in the society (Relates to cognitive power)
Social network strength	How strong social network connections are (culturally, group strength)
Shared codes and languages	Specialized languages that the network uses
Communication context (high or low)	Implicit meaning in phrases & messages vs. literal meaning of the separate words
Cultural Factors [2] [14] [16] [18] [21] [32]	
Individualism	Degree to which the society reinforces individual vs. collective achievement and interpersonal relationships
Masculinity	Degree to which the society reinforces or does not reinforce male achievement, control and power. Extent to which an individual views the world as competitive rather than nurturing (Relates to power)
Uncertainty Avoidance	Level of tolerance for uncertainty and ambiguity within the society. Risk propensity of individuals and the tendency to avoid action where the outcome is unclear. Conformist societies value predictability, e.g. Japan
Perceptual Style	"Filters" or patterns that affect how people identify, recognize, & react to events
Self concept	Effect of culture on how people perceive, define, portray, value, and view themselves, including but not limited to self esteem.
Time orientation and perception	Time as monochromic, linear primary frame of reference that drives schedules and behavior (Western view) vs. time as a tool to meet the needs of the group, enhance relationships, enhance trust, and share information (Middle-Eastern view)
Ethics and constraints	Moral distinction between good & evil. Extent to which moral behavior is governed by guilt, shame, saving vs. losing "face" & probability of being caught.
Cause and effect	Degree to which a person's destiny is a result of past actions vs. the idea that an individual has no control over destiny

Heuristics are relevant to deception because deceivers can use heuristics based on cognitive or group biases [7] to influence a target into accepting an act of deception as truth. Heuristics are influenced by background, history, culture, and surrounding environment. Heuristics are also important in deception detection. To assess heuristics, one must consider the cognitive, personality, cultural and/or organizational factors of the individual or group either deceiving or being deceived. Some factors that can affect heuristics are described in Table 2, which describes four factor groups arranged in order increasing sphere of influence. Table 3 defines the characteristics of each level from the most personal to the most impersonal level. For example, "cognitive factors," which are the most personal with the smallest sphere of influence (i.e. one individual) are listed first. Personality influences other people in the vicinity of, and under the direction of an individual, but this influence might not be as great as the influence of an organization. Cultural factors are listed last because cultures are the most impersonal entities. Cultures generally have a larger sphere of influence than individuals, small groups, and organizations.

Table 3: Characteristics of the types of factors that can affect heuristics, arranged in order of level of influence

Factor Type	Characteristics of the level
Cognitive (Most personal)	Most personal and private level, known only to an individual. This is the smallest sphere of influence.
Personality	Affects small-scale groups and people in the immediate vicinity or under the authority of an individual.
Organizational	Pertains to larger sphere of influence than any single individual. Includes multiple individuals, personalities, and subgroups.
Cultural (Most impersonal)	Most general and impersonal level. Includes many individuals and organizations. Pertains to the largest sphere of influence, such as coalitions.

Power distance, network strength, shared codes, and languages can influence heuristics directly. Many of the concepts described in Table 2 are interrelated through the connection between cognition and personality, cognition and culture [7], as well as organizations and culture. Research shows that some of these factors play a role in the media that individuals use to communicate with each other. Correlations between various cultural and organizational factors and certain heuristics are indicated in some various places in Table 2. Further research is needed to characterize how the factors listed in Table 2 interact and correlate in the deception process and in deception detection.

V. HIGH-LEVEL DECEPTION-DETECTION MODEL

To deceive, cognitive knowledge of the target is required, or at least, assumed. If potential targets can anticipate the cognitive biases deceivers want to exploit, the targets can monitor themselves more closely to avoid the deception. This idea is the basis of the high-level Preparation, Detection, and Reaction (PDR) deception-detection model described below.

The PDR model, which is illustrated in Figure 2, is consistent with other more detailed and specialized models [13], [17], [24] of cognition and deception. In this model, the flow of data and events can be iterative, that is, counter deception can trigger another round of detection efforts. The focus of the discussion below is on preparation and detection because reaction can be a form of deception rather than deception detection.

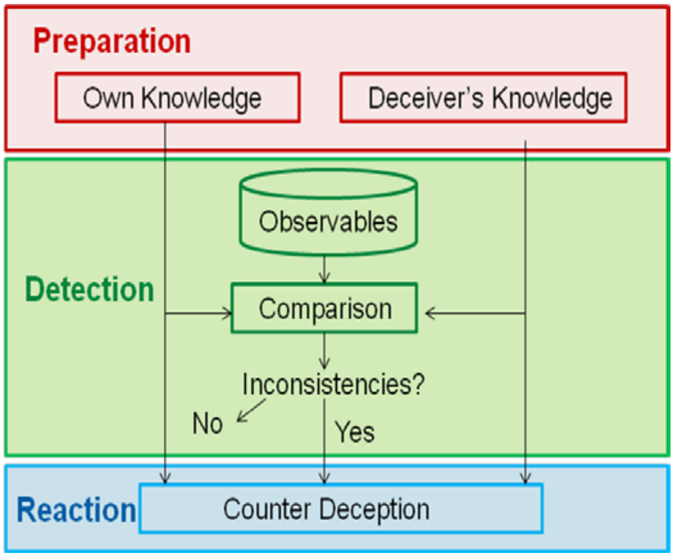

Figure 2. Block diagram of the Preparation Detection Reaction (PDR) deception-detection model

The preparation phase deals with gathering information about the environment in which a possible deception may occur. According to the common themes of deception in Figure 1, a deceiver will customize a deceptive act for the target. This means, for example, that deceiver will form the deceptive information in such a way that the target's heuristics will be exploited. Therefore, for effective deception detection, a potential target must be aware of his or her own heuristic weak points to know how the deceiver will attack. From a cognitive viewpoint, most of the analysis of a deception-detection tool will be focused towards the user of these tools, who is most likely to be an intelligence analyst.

An understanding of the deceiver's point of view also is important. Knowledge of possible communication channels and their potential vulnerabilities is necessary to detect deception. For use in the reaction phase, the cognitive state of the deceiver should be ascertained as well. To determine the cognitive states, the factors that influence heuristics, some which are mentioned above, should be monitored and the most vulnerable heuristics should be noted. These are the heuristics that the enemy will most likely try to exploit.

The detection phase will involve the use of the information from the preparation phase to detect inconsistencies. If the target's cognitive state is known, anything that triggers the vulnerable heuristic that was found in the preparation phase can be flagged as a possible deception. The cognitive aspects of deception detection can vary. When detecting deception, one also must look for verbal and physical discrepancies as well as format discrepancies.

The reaction phase of the PDR model consists of a counter-deception plan. When a deception is detected, the target can exploit the fact that the deceiver believes the deception plan has succeeded.

Examples of the PDR model are discussed below in section VII on deception detection in coalition command and intelligence centers.

VI. Observations and hypotheses

The key to understanding deception detection on in face-to-face interactions may be the observation of cue sets that indicate deception in individuals. The PDR deception-detection model involves a comparison between or among the observables. This comparison can take many forms. For example, the expert detecting deception will compare all the observable to the cues that indicate deception and rapidly discard any observables that do not constitute deception cues. This comparison, which can proceed rapidly and sometimes intuitively, can result in a correlation hypothesis between two or more cues, and a confirmation or modification of that hypothesis as more cues are observed to support or refute the hypothesis.

For example, Paul Ekman, a recognized expert at deception detection, has demonstrated the importance of sequences of visually detectable cues, such as facial muscle-group coordination and correlations expressed as changes in facial expressions and face-muscle postures used in concert to detect deception [15]. Some of these changes are called microexpressions [11], which are involuntary and last only a short time. In [20], [18], and [28], deception detection was achieved based on correlations of multiple cues. This is evidence that cue sets contain a mixture of verbal and nonverbal cues, especially microexpressions [11].

For example, in a non-deceptive situation, many facial cues rise in concert, whereas facial expressions of deceivers emphasize a few cues that arise more randomly and chaotically [15]. A smile without the use of multiple natural facial muscles (particularly around the eyes) indicates a deception at being friendly and not a genuine expression of happiness [15].

Expert deception-detection agents can detect and correlate cues that they observe among the variety of behaviors present that do not constitute cues. A complex combination of visually observable, acoustic, linguistic, non-linguistic, and sequential cues is likely to be responsible for high scores that have been observed in the testing and professional practice of deception detection during interpersonal contact.

A cognitive burden is imposed on the deceiver who tries to manage many cues simultaneously with various success rates. Managing this cognitive burden itself produces microexpression and other cues that can lead an astute deception-detection agent to suspect deception. This is because deception can be detected when behaviors are not self consistent, or when a few features are very strong and other features are very weak. Behavioral inconsistencies constitute a class of cues that depend on one or more behaviors. The deceiver, not being able to control all cues simultaneously due to the cognitive burden, presents an artificial distribution of features that is unnatural and, therefore, detectable. The deceiver's cognitive burden increases particularly in face-to-face, real-time deception scenarios where both verbal and nonverbal cues are available for detection with follow-up questions. (See, for example [15].)

The apparent discrepancies in the effectiveness of detecting deception via behavioral cues could be explained by considering individual differences, such as various levels of deception-detection expertise, the variability in human behavior, and variations in personality. For example, research has demonstrated that the variety of nonverbal cues, i.e. a specific cue set, is a particular characteristic of a specific deceptive individual [11]. The evaluation and successful use of many cues and their interactions impose a cognitive burden on the deception-detection agent as well as the deceiver. The deception-detection agent may use heuristics described in Table 1 as well as other heuristics that facilitate the mental data fusion of detected cues.

Equation (1) describes how an expert deception-detection agent might organize cues sets. Let S be a weighted set of deception cues that contribute to the deception "signal." These cues can be of any type, such as those described above in Section II in the paragraph on behavior. X, Y, and Z are examples of single observable cues to deception. The coefficients, a_i, b_i, c_i, and k_i are weighting factors that represent the importance of each cue or combination of cues in the detection task. Different contexts will suggest different distributions of weighting factors. Moreover, if a cue is not present or the behavior associated with it does not constitute a cue in the context of the observation, the corresponding weighting factor would be zero.

$$(1) \quad S = \sum a_iX_i + \sum b_iX_iY_i + \sum c_iX_iY_iZ_i \; . \; . \; . \sum k_iW_iX_iY_iZ_{i\ldots}$$

Each successive term in (1) represents either a simple cue or the fusion of deception cues at a higher level of aggregation. For example, the first group, a_iX_i, represents single, individual, simple, and uncorrelated cues. The other sums in (1) represent complex cues. For example, the second group, $b_iX_iY_i$, represents correlations of cues taken pairwise. Similarly, the third group, $c_iX_iY_iZ_i$, represents interactions and correlations among a group of three different cues, etc. In (1), a cue is never combined or correlated with itself. Thus, terms like $c_iX_iX_iX_i$ or $c_iX_iX_iX_j$ would not be allowed. Equation (1) is not new. It is based on the Virial expansion [4], which describes interactions of molecules in the gas phase and their contribution to an equation of state [4].

Section II lists many possible cues. Wood reports 10,000 nonverbal body-language and paralanguage cues (e.g., voice, tone, rate, volume etc.) [40], [41], [42]. The combinatorial explosion results in an unmanageable set of total cues to track unless one uses of heuristics. The number of possible cues is too much for anyone, even an expert, to monitor and track in an analytical, conscious, or rational way. Rather, these cues are processed on a nonverbal, subconscious, and emotional level [42], where considerable filtering, integrating, and summarizing take place as necessary heuristics to process the input at a higher level of aggregation. For example, a deception-detection agent might summarize nonverbal cues at the subconscious level so the members of a cue set will be grouped and integrated into a complex cue and handled cognitively as a single entity or feature rather than a set.

Another heuristic is to ignore cues with low coefficients in equation (1), that is, with low probability of being relevant. The threshold can be set higher and higher until a manageable set of salient cues emerges. This approach is related to the “Availability” heuristic described in Table 1, where the strongest cues are viewed as the most “available” ones. Cues that are insignificant or absent are considered “unavailable” for observation. An example of a three-way cue interaction that may be sufficient to trigger a deception-detection is the combination of a gaze diversion, with a pupil size enlargement and a change in the number of complex sentences.

Fortunately, not all cues may be needed for deception detection. For example, six cues may be present but only two of them might be sufficient to trigger suspicion. Further inquiry may produce enough evidence to conclude deception without the necessity to use all six cues. The task becomes simpler than a rigorous analysis of all cues and their interactions, but is relies on past experience regarding which cues to are the most important and revealing.

The rapid identification of behavioral cues in each individual’s cue set and the efficient discovery of how these cues interact constitutes an important difference between expert and novice deception-detection agent. Whereas different experts could rely on different cue sets under different circumstances and in different contexts, another mark of expertise is the knowledge of when to change strategies or modify approaches to deception detection.

VII. DECEPTION DETECTION IN COALITION COMMAND AND INTELLIGENCE CENTERS

This section considers some of the features of deception detection that pertain in particular to the dynamics of coalition C^4ISR vis-à-vis the PDR deception-detection model. Each deceptive act, regardless of the medium, poses different threats to a coalition. The coalition needs to detect the deception in time to correct the problem before it affects coalition operations. Information in coalition command centers is received in multiple media. Each medium has its own set of challenges regarding deception.

Similarly, command centers receive data in multiple formats, including but not limited to network-based computer messages, verbal messages via radio or in person, chat, transcriptions of speech, formal text (i.e. not textual transcriptions), and imagery. Data sets arrive from multiple sources that are even more diverse in coalition operations than they are in unilateral operations. Coalitions may be especially vulnerable to deception if the coalition partners are unfamiliar with the details of each others’ internal information formats and reporting styles. This underscores the importance of preparation in coalition operations, as depicted in Figure 2. In the preparations prior to operations, coalition members should become aware of message types used by other coalition members and the common errors that are observed. Departure from these errors may constitute a cue to deception.

For example, an operator may notice an error in a message written in a familiar format that might go undetected in a foreign format. This error may be evidence of tampering and an attempt at deception. The PDR model predicts that the operator will attempt to use his or her knowledge of the correct format and compare the expected format to the format where the error is detected. If the error looks like an error that is commonly detected in this message type, the operator may accept it as an honest mistake. However, if the error reflects a discrepancy in the sender’s knowledge about something that should have been known in a truthful setting, the operator can identify the error as a cue to deception, flag the message as deceptive, suspect the sender as a deceiver, and initiate counter deception procedures.

Communications automation itself can interfere with the detection of deception. Face-to-face communication offers the richest source of deception cues whereas text-based media offer much fewer cues to deception [15], [16], due to the filtration mechanism that removes direct visual contact. Therefore, deceivers have an advantage in dispersed coalitions that must communicate using chat or email.

The combination of task complexity and deception has been linked to poor performance in groups [17]. Both the task and the ability to detect deception suffer in complex environments. Deception detection is a subset of decision making because the deception-detection agent must decide whether the aggregate of cues indicates deception. Moreover, many groups can have either no effect or a negative effect on the decision process [17]. As task complexity increases, so does the need to communicate among group members. This overhead introduces an inefficiency that degrades performance. The knowledge and expertise each member brings to a group may be insufficient to compensate for the complexity. The presence of this communications-based inefficiency, together with a more complex environment in general, produces a cognitive overload that can interfere with attending to cues that signal deception.

Coalitions, in which members do not all speak the same language, must employ translators for communications precision and efficiency. If a coalition translator does not have enough information to suspect deception in a message or personal interaction, this will result in a translation that does not flag deception, regardless of whether deception is present. Moreover, translators are trained in languages but not necessarily in how to detect verbal and nonverbal cues described in Section II that might reveal the sender's emotional state, political opinion, deceptive intentions, or group bias. One of the challenges of coalition operations is the increased risk that translators may find themselves in the role of unaware deceivers, as described in Section II.

For example, to illustrate an application of the PDR model with a hypothetical situation, a translator uses his or her own knowledge to translate a body of text. The language in which the text is written is not the native language of the translator. Some of the material in the text is not true but this is not obvious to the translator. In this case, of where the deceiver's knowledge overcame the knowledge of the translator in the preparation phase. Deception detection did not occur for that reason. When the translator compared the observables, the cues that could reveal deception were not detected, so the translator found no inconsistencies and passed the translation along to coalition members as ground truth.

Another factor that can affect deception detection in multicultural coalitions is the difference in ability of individuals from different cultures to discern or infer meaning in a textual communication in addition to the literal meaning of the words that are used in the message. The ability to "read between the lines" depends on the culture. For example, a Middle Easterner accustomed to more indirect forms of communication may be better at understanding the intent of a high-context message than a Westerner would [32]. For this reason, the ease of deception detection also is likely to depend on culture. For example, what at first seems like an irrelevant detail may be the key to identifying and understanding [32] the meaning in a message in general. More particularly, a seemingly small detail could signal an attempted deception. Different cultures will impart different knowledge in the preparation phase of the PDR model and people from different cultures pay different amounts of attention to various observables in the detection phase. This is like having a different set of weighting factors (a_i, b_i, etc.) in equation (1).

On the other hand, a deceptive message (or conversation) may express two logical points of view that alone appear self consistent. However, upon closer examination, these view points are actually contradictory and inconsistent with each other, thus alerting the target or the observer to possible deception. For example, a ship's position may be reported as being 8 miles due South of an island by one source and 9 miles due west of the same island by a different source. Either the first is true and the second, false, or vice versa. Both can't be true simultaneously but both could be false. In any case, such inconsistencies in messages call into question the reliability and truthfulness of the messages and their senders. A Westerner using linear, logical thinking is more likely to detect deception in a message like this than a Middle Easterner who is looking for other cues and "reading between the lines."

Commanders rely on imagery for situation awareness, threat awareness, and planning. The rise in the use of digital photography vs. analog-film photography poses particular problems in terms of the credibility of the image. Alterations of negatives are easy to detect. Sometimes these anomalies can be observed on photographic prints. In contrast, a digital image can be altered in such a way that no one will know that anyone changed it. This increases the challenge of deception detection in digital photography and will require different and more sophisticated methods and approaches compared to those used to analyze film-based images.

The following example depicts a coalition issue associated with imagery. Coalitions can have wide distributions of technological sophistication for collecting, disseminating, and analyzing images over the coalition members. This means that some coalition members will have better tools, techniques, and resources than others for detecting deception using imagery and in dealing with the results. In some cases, the imagery resolution of the equipment, or the interpretation of color codes of one coalition partner may not be sufficient to tell that what looks like a tank is actually a decoy, whereas another coalition partner may have the equipment and techniques to distinguish between the true and the false.

VIII. GROUP BIAS AND DECEPTION CHALLENGES

Detection of group bias whether deceptive or not, can depend on non-traditional keywords, such as articles, pronouns, and other parts of speech [7]. The use of these keywords and the context in which they are used may signal group bias. For example, the detection of group bias may hinge on the choice and placement of articles, demonstrative pronouns, and choices of noun categories in a message. (See, for example, [7].)

If group bias can be determined or reasonably estimated, heuristics like framing can be of use in deception detection in coalition operations. (Table 1) For example, if a suspect appears to be a member of a group and a deception-detection agent wants to be able to ascertain if the suspect is truthful or a deceiver, the deception-detection agent can use his or her knowledge from the preparation phase of the PDR model to frame questions based on assumptions that reflect the beliefs, values, attitudes, bias, experiences, politics and preferences of a group to which the suspected deceiver belongs. Framing in this context is a heuristic that is used to gain the suspect's confidence with the goal of obtaining more information regarding deception or other topics of interest to coalition operations. The suspect may believe that the deception-detection agent shares the same group bias.

The main observable in this case would be something told to the deception-detection agent in confidence that indicates deception. The deception-detection agent now is in a good position to move on to the reaction phase and counter the deception, perhaps without the deceiver knowing about the detection. In this case, the deception-detection agent's knowledge determined the outcome of the deception-detection, thus overcoming the deceiver's knowledge.

Coalitions are groups, so the research that pertains to groups also applies to a great extent to coalitions. Some international coalitions evaluate ideas and make major decisions through group consensus, such that all members have a more or less equal voice. In contrast, other coalitions are based on a more hierarchical structure where all coalition members do not share the same level of authority and power, particularly if one coalition partner supplies the majority of the personnel, equipment, intelligence, and financial resources whereas the other partners offer a much smaller commitment.

Each approach toward coalition operations has its advantages and disadvantages. The group-consensus approach is more likely to consider a wide range of inputs from multiple experts. The disadvantage is that decision making, whether aimed at deception detection or some other goal, takes longer to achieve in a group setting and has been shown to be more inefficient [17]. The advantage of hierarchical coalitions is that they can be more agile and responsive, but the disadvantage is that they may fail to account for some crucial factor known to only one of the lower-ranking coalition partners.

Deception itself can interfere with decision making regardless of whether it come from individuals outside the group (outgroup) or from within the group (ingroup). Group members may practice deception if they have personal agendas that differ from that of the group [17]. Ingroup deception is more difficult to detect due to truth bias among members who are assumed to be cooperating.

If the goal of an ingroup deceiver is detrimental to the group, the deception is likely to have a negative effect, whether this effect is to interfere with decision making or degrade group performance. If the goal of the deceiver is neutral to that of the group, the effect will be less negative but not zero. Energy expended in the pursuit of deception themes (Figure 1) is energy that cannot be used to further group goals.

IX. DECEPTION ABOUT GROUP MEMBERSHIP

In coalition, where many groups must interact and cooperate to achieve victory, coalition members need to know who is a member of the coalition and who represents an imposter trying to gain unauthorized access. Therefore, the present study includes consideration and exploration of a cognitive basis for deception detection regarding group membership or identity.

The use of these keywords and the context in which they are used may signal group bias deception. For example, the detection of deception regarding group bias may hinge on the choice and placement of articles, demonstrative pronouns, and choices of noun categories in a message [7]. The Grammatical-Categories Model (GCM) [7] features a progression of grammatical categories that may be used to reveal group bias. These categories are rank ordered based on durability from the most dynamic (clusivity) to the most static (gender) category of grammar that characterized the languages that were studied. A social parallel between grammar and normal, expected behavior based on group identification is well known [7]. This pattern has been the topic of various studies [7], [21]. The strength of the interaction also follows the same parallel in the GCM.

The GCM could be used as a tool in the future to help predict where to look for the most salient group-identity characteristics, which could help determine group identity. For example, one of the most socially ingrained part of a person's identity and personality is a set of behaviors associated with his or her sex. This is reflected in the most static grammatical category, gender. Sex is the biological counterpart of grammatical gender. A person’s sex is a very strong, if not the strongest, group identifier. Grammar parallels societal norms. Therefore, it is not surprising that sexual stereotypes would include the richest set of behaviors that characterize and contrast the two groups.

Hills [20] studied “gender” deception in informal internet-text messages. Some of the male authors pretended to write as they would if they were females, whereas some females wrote their messages impersonating males. Others wrote naturally without any attempt to alter their writing style with any sex-biased deception. Subjects’ task was to identify the true sex of the individuals from an examination of their text messages and distinguish the true from the deceptive cases [20].

Analysis of 12 linguistic variables showed significant and noticeable differences in the speech patterns of males and females [20]. The aggregate of these linguistic cues contributed to subjects’ assessment and overall success rate, no single cue alone being enough to pinpoint a person's sex, i.e. to detect deception regarding group membership [20].

The text-message subjects reported that they detected deception because the people who wrote the deceptive messages overused the assumed stereotypical group traits to an extreme [20]. The subjects comments were, “Sounds too 'male' to be a real male” or “No real female would say that” [20]. The deceivers concentrated on a few easy-to-implement traits and neglected the more subtle ones. Because so many behaviors constitute the sex-group profiles, the deceivers overlooked many of them, which the subjects astutely notice.

The text-message study [20] replicated the findings of a study on transcripts of speech [29] in sex-based identity deception where 17 linguistic variables were identified [29]. These studies suggest that the identification of group-membership deception in text depends heavily on having a detailed, accurate, well-known list of group-specific linguistic characteristics or tendencies. Humans learn sex-specific behavioral traits by observing people in their own group (and other groups) on a regular basis. Without this template or profile information, deception detection regarding group identity would be very difficult, if not impossible because it depends on so many correlated features.

The results of Hills’ text-message study [20] parallel Ekman's [15] findings on body language and facial expressions. The results on textual sex-group deception discussed above suggest that coalition members could be trained to detect deception regarding membership in terrorist groups well above chance level provided a profile of group characteristics could be developed from sufficient observation. Observers could rely on some of the same cues that are used to detect authorship style and content. However, coalition members might have to study the subtle nuances of the group's collective behaviors over a long period of time to be able to achieve acceptable levels of accuracy and false-alarm rate. Thus, a profile at the group level could be developed, stored, maintained, and enhanced by multiple observers and analysts, so that this profile would be available to all coalition members but would not depend on the knowledge, bias, or errors of a single coalition member.

Regarding deception in terrorist groups, a terrorist may not control his or her behavior to exhibit all characteristics from his or her group, overemphasizing some and neglecting others. It would at least "paint a confusing picture" to an observer and cause an astute person to take notice and ask more questions or probe the situation indirectly for more data. It may be sufficient to alert a screener at a checkpoint when the probability of deception is higher than normal. It is not likely to be necessary to prove (as in a court of law) that an individual is deceptive about a group membership for the present study to be meaningful and provide value added.

X. MODEL BASES IN OPEN-SYSTEM SOA

In light of the many challenges described above that coalitions face as a result of multiple kinds of deception, some automated tools arranged in a SOA and a systematic approach could prove valuable to support coalition C^4ISR. One such architecture is depicted in Figure 3.

For example, the high-level model described in this paper, as well as other models that are designed to apply to lower levels of the ontology of deception should be integrated into the C^4ISR environment using a variety of deception-detection tools designed to support the goals of coalitions. In this section, the term “user” refers to the analyst who uses automated tools to detect deception. Except for counter deception, the “user” is not engaged in deception, but in detecting deception, or in reading texts of deception-detection agents who report on deception.

Due to increased use of models and the trend toward modeling and simulation of diverse processes, model bases are needed to support coalition analysts’ work in deception detection and deterrence. Moreover, an ontology, such as the one outlined in section II, is needed to ensure that each model and tool will be available to the analyst in a SOA, the chief advantage of which is service discovery [39].

A model is an approximation of an observed object or phenomenon based on assumptions about how that object, entity, or phenomenon should behave. Models can encode this approximation in automated executable software, or as non-automated algorithms, procedures and equations. A model can be a sample of a class that contains enough class features to exemplify that class of entities. A model base consists of a collection of models with metadata that show their interrelationships [8]. These metadata also can include the origin of the model, date put into service, and a short summary of the purpose and limitation of the model. Model bases are a form of information base with a high degree of information aggregation and correlation. Model bases are the next logical step in the database-knowledge-base progression toward greater and greater data aggregation, integration, and fusion. (See, for example, [8].)

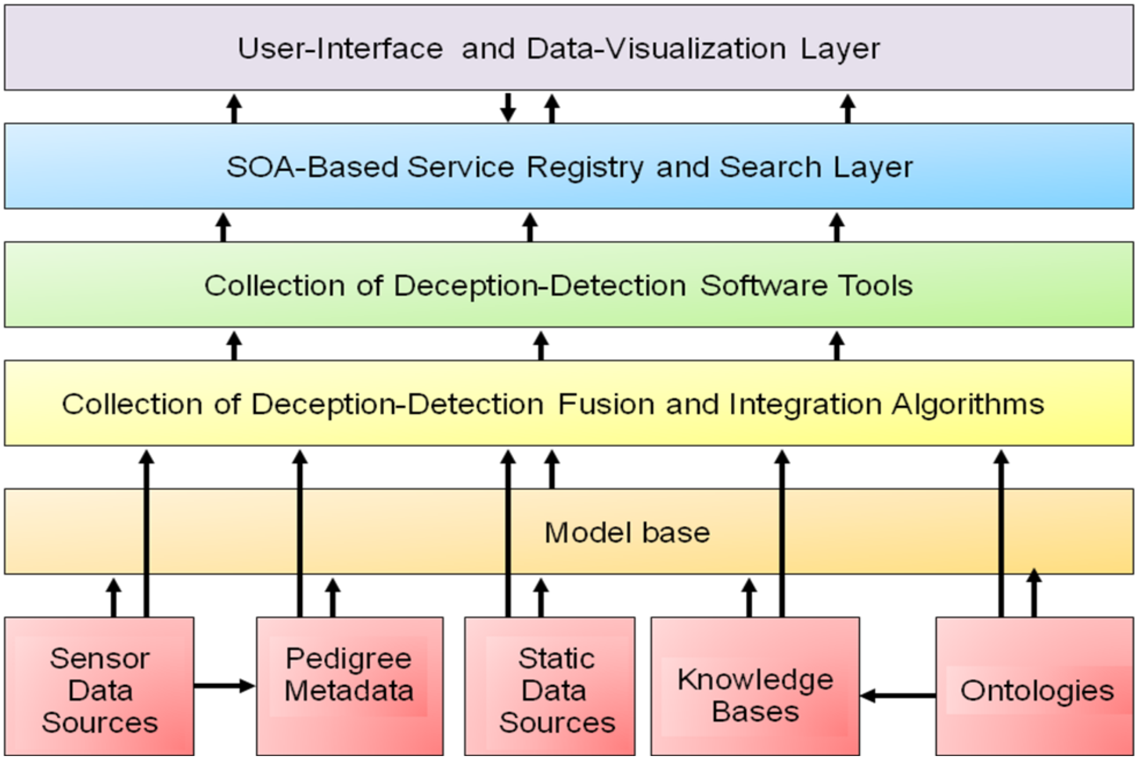
User-Interface and Data-Visualization Layer
SOA-Based Service Registry and Search Layer
Collection of Deception-Detection Software Tools
Collection of Deception-Detection Fusion and Integration Algorithms
Model base
Sensor Data Sources
Pedigree Metadata
Static Data Sources
Knowledge Bases
Ontologies

Figure 3. Functional layers in SOA for coalition deception-detection tool suite

The availability and use of open-source data constitute necessary but insufficient conditions conducive to the development of a comprehensive tool set designed to assist the analyst with understanding, detecting, and in some cases, deterring deception. To make the most of available models, an open system of modular, "plug-and-play" analyst tools must use a SOA that enables analysts who want to use the tools to learn about their existence and how the tools function.

A good SOA also has a user-friendly interface to automate the discovery, selection, and use of its models and tools, as illustrated in Figure 3. Analyst users also can understand the relationship of models and the tools that implement them so they can select the correct models to use for various applications. In SOA, a flexible, user-driven schema is needed to show the following for maximum user support.

- All the tools and how to find them,
- What the tools were designed to accomplish,
- The models that the tools use,
- Which tools could be used in parallel,
- Which tools must be used sequentially as a group,
- The input that a tool can accept from the output of other tools,
- Which tools use different means to achieve the same or similar objective,
- The track record and statistical reliability of various tools and/or models, if known,
- User comments regarding their experience with the tools, including a subjective rating scheme.

Automated translation software support to ensure equal access to all coalition members, regardless of native language.

Users need to be able to find the right deception models. To meet this need, a model base and metadata based on an ontology of deception can be used to help catalog, arrange, and organize deception models in a SOA. This approach is described below as a step-by-step procedure.

1. Import or construct an ontology of deception and an upper ontology that includes cognition. Enhance the ontology to include all the concepts discussed in section II. The deception ontology will inherit characteristics from the cognitive ontology and the domain ontologies for particular applications.
2. Select keywords that describe the models' goals and functions.
3. Identify inputs and outputs of the procedural and executable models and algorithms.
4. Locate the underlying concepts of the goals, functions, inputs, and outputs in the ontology.
5. Tag the model with locators that point to those concepts in the ontology. These tags form the basis of a reach-back capability to locate models in the future that pertain to analyst tasking.
6. Incorporate the model base, with the tags arranged by model, as part of the metadata used for service discovery in the SOA.
7. Construct a database based on the ontology's concepts to facilitate queries regarding available models, tools, and their functions.
8. Keep track of the tools that users implement together to alert users through advisory messages such as "People who used tools A and B, also used tools X and Y."

XI. Future Research and Development

Future research and testing is needed on the cultural or organizational factors that affect cognitive heuristics, as well as the classification and measurement of which factors affect which heuristics. A mathematical model, possibly to include equation (1), is needed to compute the influence of these heuristics and sort them in order of vulnerability. A prototype SOA environment with multiple deception-detection models, tools, and modules needs to be constructed and tested operationally with coalition users. More work is needed to refine automation in intelligence systems to gather relevant data for various models and to identify deceptive elements in these data sets before they can degrade coalition operations.

A primarily nonverbal aptitude test needs to be developed to predict who would be good candidates for deception-detection assignments. Training based on this test can focus on detection of microexpressions and correlating them with other cues, including but not limited to verbal cues.

Another future project would be to develop a module to detect deception in command-centers messages and install it to run in the background. Such a tool also might detect other inconsistencies, such as errors, that resemble deception but that do not arise from an attempt to mislead. Users would be able to set the threshold for notification of possible deception either to respond to increased risk of deception (lower threshold) or to minimize false alarms (higher threshold). A certain amount of automation may be possible for threshold recommendations in a mixed-initiative paradigm for users who cannot assess deception threats. The system can search for deception at multiple levels of information aggregation, e.g. data and knowledge. Like a firewall, the challenge here will be to provide significant value added to justify development cost, while not degrading the performance of network processing.

Acknowledgments

The authors thank the Office of Naval Research Code 30 program office for support of this work. This paper is the work of U.S. Government employees performed in the course of their employment and no copyright subsists therein.

References

[1] J. Arciuli, G. Villar, and D. Mallard, "Lies, lies and more lies," *Proceedings of the 31st Annual Conference of the Cognitive Science Society (CogSci 2009)*, pp. 2329 – 2334, Netherlands, 2009. http://csjarchive.cog-sci.rpi.edu/Proceedings/2009/papers/541/paper541.pdf

[2] G.E. Baoshan and Y.U. Dongming, "Social Capital and Cognitive Bias: An Empirical Study of China" *Proceedings of the IITA Internal Conference on Control, Automation and Systems Engineering*, 2009.

[3] T. Barnhart, *Verbal & Non-Verbal Deception Behavior Analysis*, July 2009. http://www.corrections.com/tracy_barnhart/?p=305

[4] G.W. Castellan, *Physical Chemistry*, Addison-Wesley Publishing Co., Reading, MA, 1964.

[5] M.G. Ceruti and M. Bowman "Expertise, Pattern management, and decision making: Challenges in human informatics," *Proceedings of the 5th World Multiconferencep on Systemics, Cybernetics and Informatics (SCI 2001) & the 7th International Conference on Information Systems Analysis and Synthesis (ISAS 2001)*, Vol. X, 575-580. Orlando FL. http://campus.murraystate.edu/academic/faculty/michael.bowman/ceruti-bowman-SCI2001.pdf

[6] M.G. Ceruti, B.M. Thuraisingham, and M.N. Kamel, "Restricting Search Domains to Refine Data Analysis in Semantic-Conflict Identification," *Proceedings of the 17th AFCEA Federal Database Colloquium and Exposition 2000*, pp. 211-218, Sep. 2000, San Diego CA.

[7] M.G. Ceruti, S.C. McGirr, and J.L. Kaina, "Interaction of Language, Culture and Cognition in Group Dynamics for Understanding the Adversary," *Proceedings of the National Symposium on Sensor and Data Fusion (NSSDF)*, 26-30 July, 2010 Nellis AFB, Las Vegas, NV. http://www.dtic.mil/cgi-bin/GetTRDoc?AD=ADA526247&Location=U2&doc=GetTRDoc.pdf

[8] M.G. Ceruti and S.H. Rubin, "Infodynamics: Analogical Analysis of States of Matter and Information," *Information Sciences*, Vol. 177, No. 4, pp. 969-987, 2007. http://portal.acm.org/citation.cfm?id=1222573

[9] D. Daniel and K. Herbig, "Propositions on Military Deception" *Military Deception and Strategic Surprise* Frank Cass & Co, Ltd., 1982.

[10] M. Dewar, *The Art of Deception in Warfare*. David & Charles Publishers, 1989

[11] M.W. Decaire, *The Detection of Deception via Non-Verbal Deception Cues*, 30 Nov. 2000, E. Sycamnias editor, Lakeland University, http://www.uplink.com.au/lawlibrary/Documents/Docs/Doc64.html

[12] T. Docan-Morgan, "Training law enforcement officers to detect deception: A critique of previous research and framework for the future" (Electronic Version), *Applied Psychology in Criminal Justice*, Vol. 3 No. 2, pp. 143-171, 2007.

[13] A. Deokar and T. Madhusudan, "Developing Group Decision Support Systems for Deception Detection," *Proceedings of the 38th Hawaii International Conference on System Science*, 2005.

[14] M. Douglas, *Cultural Bias*. Royal Anthropological Institute of Great Britain and Ireland, 1978.

[5] P. Ekman, "Darwin, Deception, and Facial Expression," *Ann. N.Y. Acad. Sci*. 1000: pp. 205–221, 2003.

[16] C.P. Furner and J.F. George, "Making it Hard to Lie: Cultural Determinants of Media Choice for Deception," *Proceedings of the 42nd IEEE Hawaii International Conference on System Sciences*, 2009.

[17] G.A. Giordano and J.F. George, "Task Complexity and Deception Detection in a Collaborative Group Setting," *Proceedings of the 38th IEEE Hawaii International Conference on System Sciences*, 2005.

[18] J.L. Gross and S. Rayner, *Measuring Culture: A Paradigm for the Analysis of Social Organization.* Columbia University Press, 1985.

[19] J. Haswell, *The Tangled Web: The Art of Tactical and Strategic Deception*. John Goodchild Publishers, 1985.

[20] M. Hills, You Are What You Type: *Language and Gender Deception on the Internet*. B.A. Thesis, University of Otago, 2000. http://www.netsafe.org.nz/Doc_Library/Internet_language_dissertation.pdf

[21] G. Hofstede, *Culture's Consequences, Comparing Values, Behaviors, Institutions, and Organizations Across Nations*, Thousand Oaks CA: Sage Publications, 2001. http://www.geert-hofstede.com/

[22] O.P. John and S. Srivastava, "Big-Five Trait Taxonomy: History, Measurement, and Theoretical Perspectives," in *Handbook of Personality: Theory and Research* (2nd ed.) L. Pervin and O.P. John (Eds.) New York: Guilford, 1999.

[23] J. Krivis and M. Zadeh, *Hunting for Deception in Mediation – Winning Cases by Understanding Body Language*, 2006. www.negotiatormagazine.com/kriviszadeh_june2006.doc

[24] D.R. Lambert, *A Cognitive Model for Exposition of Human Deception and Counter Deception*, Naval Ocean Systems Center Technical Report No. 1076, 1987.

[25] J. Latimer, *Deception in War: The Art of the Bluff, The Value of Deceit, and the Most Thrilling Episodes of Cunning in Military History, from the Trojan Horse to the Gulf War.* The Overlook Press, 2001.

[26] J. Lynch, *Deception and Detection in Eighteenth-Century Britain*. Ashgate, 2008.

[27] F. Mairesse, M.A. Walker, M.R. Mehl, and R.K. Moore. "Using Lingustic Cues for the Automatic Recognition of Personality in Conversation and Text," *Journal of Artificial Intelligence Research*, Vol. 30, pp. 457-500, 2007.

[28] J.D. Mitnick, and W.L. Simon, L. *The Art of Deception: Controlling the Human Element of Security*. Wiley Publishing, Inc., 2002.

[29] A. Mulac and T.L. Lundell, "Linguistic contributors to the gender-linked language effect," *Journal of Language and Social Psychology*, Vol. 5, pp. 81-101, 1986.

[30] N. Machiavelli. *The Art of War and the Prince*. Wilder Publications, 2008.

[31] T. Qin J. Burgoon and J.F. Nunamaker, Jr., "An exploratory study on promising cues in deception detection and application of decision tree," *Proceedings of the 37nd IEEE Hawaii International Conference on System Sciences*, 2004.

[32] R.S. Shumate, R. Borum, J. Turner and N.L. Fogarty, "Middle Eastern Mindset: Operational Analysis and Implicatons," *American Intelligence Journal*, Vol. 24 no. 1, pp. 45-56, Summer 2006.

[33] P. Tilley, J.F. George, and F. Marett, "Gender Differences in Deception and Its Detection Under Varying Electronic Media Conditions," *Proceedings of the 38th Hawaii International Conference on System Science*, 2005.

[34] Sun Tzu. *The Art of War*. El Paso Norte Press, 2007

[35] N. Webster, *Webster's New Collegiate Dictionary*, p. 215, C.& G. Merriam Co. Springfield, MA, 1979.

[36] N. Webster, ibid. p. 833.

[37] E. Waltz and M. Bennet, *Counterdeception: Principles and Applications for National Security*. Artech House, 2007.

[38] B. Whaley, *Stratagem: Deception and Surprise in War*. Artech House, 2007.

[39] D.R. Wilcox and M.G. Ceruti, "A Structured Service-Centric Approach for the Integration of Command and Control Components," *Proceedings of the IEEE International Conference on Service Computing (SCC 2008)*, Vol. 2, pp. 5-12, 7-11 July 2008, Honolulu, HI. http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=04578503

[40] P.Wood, "*Don't Look Like a Liar: Nonverbal Cues That Show Credibility and Deception*," http://www.pattiwood.net/uploads/Don't%20look%20like%20a%20liar.pdf

[41] P. Wood, *How to Spot a Liar*, Communication Dynamics, 2000. http://www.pattiwood.net/article.asp?PageID=2314

[42] P. Wood, *It's A Small World After All: Body Language and Global Greeting Behavior*, http://www.pattiwood.net/article.asp?PageID=2321

[43] L. Zhou, J.K. Burgoon, J.F. Nunamaker, Jr., D. Twitchell, T.Qin, "Automating Linguistics-Based Cues for Detecting Deception in Text-based Asynchronous Computer-Mediated Communication," *Group Decision and Negotiation*, Vol. 13, pp. 81-106, 2004.

[44] L. Zhou, D.P. Twitchell, T.Qin, J.K. Burgoon, J.F. Nunamaker, Jr., "An Exploratory Study into Deception Detection in Text-based Computer-Mediated Communication," *Proceedings of the 36th Hawaii International Conference on System Sciences*, 2003.

[45] L. Zhou, Y. Shi and D. Zhang, "A Statistical Language Modeling Approach to Online Deception Detection," *IEEE Transactions on Knowledge and Data Engineering*, Vol. 20, No. 8, August 2008. www.hicss.hawaii.edu/HICSS36/HICSSpapers/CLUSR16.pdf

[46] M. Zuckerman, R.S. DeFrank, J.A. Hall, D.T. Larrance, and R. Rosenthal, "Facial and Vocal Cues of Deception and Honesty," *Journal of Experimental Social Psychology*, Vol.18, pp. 378-396, 1979.

[47] *Framing*, 2002-2011 http://changingminds.org/explanations/theories/framing.htm