A risk-based multi-criteria approach for threat COAs evaluation in the IPB/IPOE process

Anissa Frini, Alexandre Bergeron-Guyard
DRDC Valcartier
2459 Boul Pie XI North
Québec, QC, G3J 1X5 Canada

Anissa.Frini@drdc-rddc.gc.ca

ABSTRACT

This paper focuses on the IPB/IPOE process in a COIN context and more specifically deals with the generation and evaluation of threat COAs. The paper objectives are twofold. It presents i) a high level description of a self inference system prototype which aims at supporting threat COAs generation in the IPB/IPOE process, and ii) proposes a risk-based multi-criteria approach for the evaluation of threat COAs under uncertainty. The self inference prototype generates threat COAs using a variety of reasoning techniques: inference component (rule-based, description logics, kinematic and geo-spatial analysis), case-based reasoning, multiple hypothesis situation analysis, and threat analysis ontology. Once the set of threat COAs is generated, COAs are evaluated using a risk-based multi-criteria approach. This approach takes into account i) multiple conflicting criteria, ii) the risk attitude of the analyst, iii) the risk as a criteria of evaluation, and iv) the uncertainty (ambiguity, imprecision) of the data. More specifically, uncertainty due to subjective human judgments, preferences, values and risk attitude is modeled. In addition, the ratings of threat COAs on panoply of conflicting criteria, related to suitability, risk, complexity and loss of opportunities, are expressed in linguistic terms. Then, these terms are transformed into fuzzy numbers in order to properly deal with the uncertainty. Furthermore, the approach takes into consideration the risk attitude of the intelligence analyst. To do so, the fuzzy ratings of the COAs are modified to model the extent to which the ratings given by the analyst could be impacted by his risk attitude. Finally, the ranking of the different COAs is performed using the fuzzy TOPSIS method.

1.0 INTRODUCTION

Defence R&D Canada Valcartier (DRDC) has recently undertaken a research and development (R&D) Applied Research Projects (ARP) entitled "Self Improving Inference System (SIIS) to Support the Intelligence Preparation of the Battlefield (IPB) Process". The main objective of the SIIS project is to produce a prototype of a self improving inference system to support the analysis and sense-making aspects of the Intelligence Preparation of the Battlefield/Intelligence Preparation of the Operational Environment (IPB/IPOE). This prototype should be capable of learning and improving based on both its current performance and operator feedback.

As an initial step for this ARP, a review of literature (Tremblay *et al.*, 2011) and a workshop (Banbury *et al.*, 2011) were conducted in order to identify relevant IPB/IPOE knowledge. Specifically, the goal of this effort was to obtain an up-to-date and exhaustive portray of the IPB/IPOE process within the context of Counter-insurgency (COIN) in order to facilitate the in-depth analysis (decomposition) of the process for the capture of reasoning requirements (RR). The literature review considered over four hundred documents, both from the scientific, and the military community. The knowledge acquisition sessions involved seven military SMEs in military Intelligence. All the workshop participants had recent operational experience of IPB/IPOE in COIN contexts. A list of over 170 RR (Banbury *et al.*, 2011) was produced out of this effort. The list of RR spanned the 4 steps of the IPB/IPOE, and the need to support the development of threat courses of actions (COAs) was clearly highlighted.

In this paper, we focus on the RR associated to step 4 of the IPB/IPOE process, and more specifically on the RR in relation with threat COAs generation (the identification of the full set of adversary courses of action) and threat COAs evaluation and prioritization (the ranking of these COAs to identify the most likely ones). Accordingly, the paper objectives are twofold:

- To present a high level description of the self inference system prototype which aims at supporting the generation of threats and threat COAs using a variety of reasoning techniques.
- To provide a risk-based multi-criteria approach for threat COAs evaluation under uncertainty, which considers multiple conflicting criteria including the risk associated to the COA, the risk attitude of the analyst, and the uncertainty (ambiguity, imprecision) of the ratings.

Section 2 gives an overview of the IPB/IPOE process, and the four steps it entails. Section 3 presents a literature review of previous R&D works that aid the intelligence officers by automating or supporting the whole process or as parts of them. Section 4 illustrates how the on going research project aims at supporting the analysts conducting IPB/IPOE as a whole. Section 5 will focus on threat COAs evaluation and detail a risk-based multi-criteria approach to support evaluation and prioritization of COAs.

2.0 IPB/IPOE OVERVIEW

Intelligence Preparation of the Battlefield (IPB) is a military process designed to provide battlefield commanders with information about an enemy and the particular battle-space. IPB consists of analyzing the weather and terrain conditions within the specific geographic environment, assessing the adversary capabilities and vulnerabilities, and predicting the adversary courses of action (COAs). Similarly, Intelligence preparation of the Operational Environment (IPOE) is a systematic approach used by intelligence personnel to analyze the adversary and other relevant aspects of the operational environment (OE). IPOE is used to define the operational environment, describe the impact of the operational environment on adversary and friendly COAs, evaluate the capabilities of adversary forces operating in the operational environment, and determine and describe potential adversary COAs and civilian activities that might impact military operations.

IPB/IPOE is a continuous, cyclical process which consists of four functions (or steps) that are performed each time IPB/IPOE is conducted (see Figure 1):

1. Define the Battlefield Operational Environment (B/OE);
2. Describe the B/OE’s effects;
3. Evaluate the threat; and
4. Determine threat COAs.

Each step in the process is performed continuously to ensure that the products of IPB/IPOE remain complete and valid, providing support to the commander and direction to the intelligence system through to completion of the current mission and into preparation for the next (IPB field manual, 1994). Each step has its own specific objectives, and success or failure in achieving the desired end effects of each step can affect the outcome of the whole IPB/IPOE process.

It is worth noting that IPOE and IPB products generally differ in terms of their relative purpose, focus, and level of detail. Both processes involve the same four steps, but implement them at different levels. The objective of IPB/IPOE is to support the commander by identifying the adversary's most likely intent and COA. IPB is specifically designed to support the individual operations. IPOE uses a more macro-analytic approach that seeks to identify the adversary's strategy, vulnerabilities, and centres of gravity. IPB requires more microanalysis and more detail, in order to support operations.

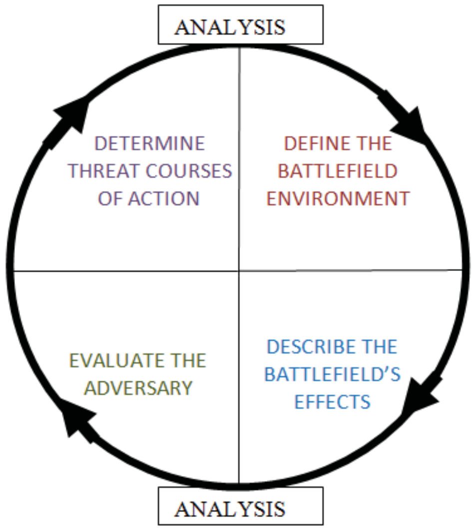

Figure 1: The IPB Process (Intelligence Field Manual, 2001)

This paper focuses on the 4th step of the IPB/IPOE process: determine the threat courses of action. The first three steps of the IPB/IPOE help provide a holistic view of the situation by defining, describing and analysing the B/OE. The fourth step of the IPOE builds on previous ones, in order to provide a detailed understanding of the adversary probable intent and future strategy. This is done in five steps (US Joint IPOE, 2009):

- Identify the adversary's likely objectives and desired end state
- Identify the full set of adversary courses of action
- Evaluate and prioritize each course of action
- Develop each course of action in the amount of detail time allows
- Identify initial collection requirements

The adversary's likely objectives and desired end state are identified by analyzing the current adversary military and political situation, strategic and operational capabilities, and the sociocultural characteristics of the adversary, as identified in the previous steps. A consolidated list of all potential adversary COAs is then constructed. At a minimum, this list will include all COAs that the adversary's doctrine or pattern of operations indicates are appropriate to the current situation. The full set of identified adversary COAs is then evaluated and ranked according to their likely order of adoption. Subject to the a mount of time available for analysis, each adversary COA is then developed in sufficient detail to describe: the type of military operation; the earliest time military action could commence; the location of the action, and the objectives that make up the COA; the operational plan, to include scheme of manoeuvre and force disposition; and the objective or desired end state. The prediction of specific activities and the areas in which they are expected to occur affect the identification of initial intelligence collection requirements.

3.0 DRDC INFERENCE SYSTEM PROTOTYPE

This section provides a high level description of the research & technology roadmap that was derived following the knowledge acquisition sessions described in section 2. Since the main topic of this paper is not related to the generation of the threat COAs but rather to the evaluation of the threat COAs once they are generated, only a high level description of the SIIS will be given. This is actually a preliminary view, which will orient the development of a first SIIS prototype. This first prototype will provide inference mechanisms to support IPB/IPOE. The "self-improving" or learning aspects will be implemented in a future version of the system and are not depicted in figure 2.

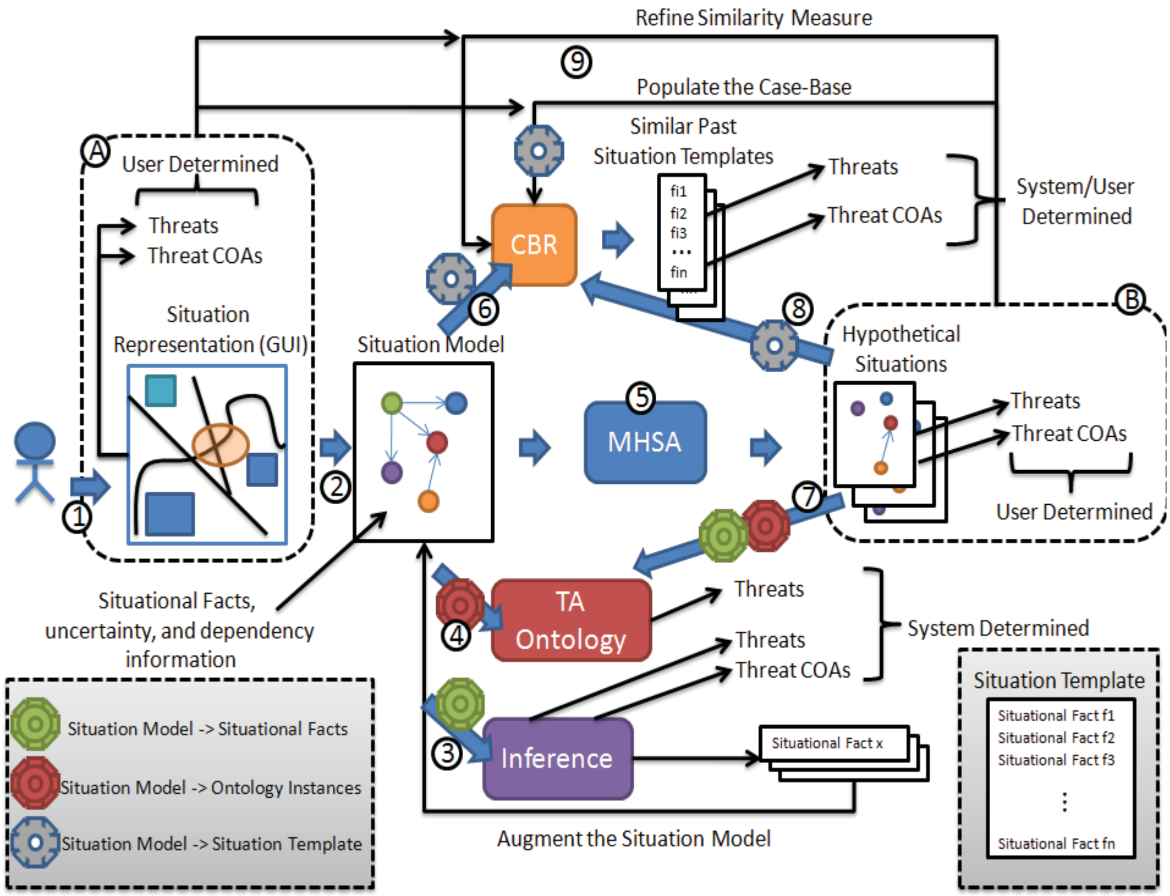

Figure 2: High Level Illustration of the SIIS.

Let us go over the process depicted on figure 2. This process can be decomposed into 9 separate steps:

1) The initial step is the description of the situation (battlefield or operational environment) by the user. With an appropriate graphical user interface (GUI), the user will be able to specify all the information that is relevant for a given situation (Situational Facts). There will also be a means for the user to specify uncertainty about the situation, and dependency between various components of the situation (e.g., in order for component A to be present in the situation, component B must also be present). From this original representation, the user will already be able to identify potential threats and specify possible COAs for them.

2) The Situation Representation, specified by the user in step 1, will be transformed into a Situation

Model. A situation model is a formal representation of a situation, its dependencies, and its uncertainty. The situation model is a graph based representation, where situational facts can be represented as elements (vertices) or relations (edges) between elements. The Situation Model also contains the uncertainty and dependency information given by the user. More information on the Situation Description Language of the Situation Model can be found in (Bergeron Guyard and Roy, 2010) The information encoded in the situation model will then be fed to a variety of AI components (steps 3 to 6).

3) Situational Facts will be extracted from the Situation Model and given as input to an Inference component. This inference component, developed by DRDC Valcartier (Demers *et al.*, 2010), uses various automated reasoning approaches (rule-based, description logics, kinematic and geospatial analysis) to infer (potentially) new Situational Facts from existing ones. The inferred Situational Facts will be used to augment the initial Situation Model. In addition, it is possible that, provided with the right set of Situation Facts, the Inference Module can identify threats and COAs present in the Situation Model.

4) Certain Situational Facts contained in the Situation Model will also be identified as instances of a Threat Analysis (TA) Ontology. This TA Ontology will structure certain elements of a situation as representing the intent, capability or opportunity (IOC) of a threat. Having identified particular IOC, the Ontology reasoner will be able to identify a certain situation as representing a threat of a particular type.

5) The Situation Model will also be fed to the Multiple Hypothesis Situation Analysis (MHSA) module developed by DRDC Valcartier (Bergeron Guyard and Roy, 2010, Roy and Bergeron Guyard, 2010). The MHSA module is designed to derive every possible situation from an initial Situation Model (containing dependencies and uncertainty). Every Hypothetical Situation obtained using this tool will be stripped of any uncertainty or dependency, and will represent a possible actual "real-world" situation derived from the initial Situation Model. The derived Hypothetical Situations use the same situation description formalism discussed in step 2. At this point, the user can analyse the various Hypothetical Situations output by the MHSA module, and possibly identify threats and COAs relevant to each of them.

6) The Situation Model will be used to populate a Situation Template. A Situation Template is a collection of Situational Facts that is meant to depict certain aspects of a situation in order to perform Case-Based Reasoning (CBR). CBR can be used for situation analysis: it allows to identify past situations that are similar to the current situation (Bergeron Guyard, 2010). A CBR component was developed by DRDC Valcartier, and has effectively implemented CBR Situation Analysis (Abi-Zeid and Demers, 2010). Using the Situation Template along with the CBR component, it will be possible to identify past situations that share similarities with the situation at hand. This is done using a similarity measure. A similarity measure takes into account, and weighs, every Situational Fact present in the Situation Template. It compares them with the Situational Facts present in past situations. Each identified past situation will have a set of identified threats and COAs. The user can analyse the various past situations output by the CBR module, and possibly identify threats and COAs relevant to each of them. It is also conceivable that a similarity threshold could be set by the user in order for certain past situations (and their threat/COAs) to automatically be considered as relevant for the current situation.

7) The Situational Facts contained in every Hypothetical Situation (generated in step 5) can be fed to the TA Ontology and Inference module (the same way it was done in steps 3 and 4) in order to, potentially, automatically identify threats and COAs for the Hypothetical Situations.

8) The Hypothetical Situations (generated in step 5) can be fed to the CBR module (the same way it was done in step 6) in order to, potentially, automatically, or manually, identify threats and COAs for the Hypothetical Situations.

9) The user determined threats and COAs contained in boxes A and B, can be used by the CBR module in two ways. First the Situation Descriptions, along with relevant threats and COAs, can be used to populate the case base. That is to say, that the user will be able to perform assisted case-base authoring by selectively adding Situation Templates (and relevant threats and COAs) to the case base. Future situations can then be compared against the newly added situations. Secondly, the expert (human) identification of

threats and COAs for a given Situation Template could be analysed and used in order to tweak and enhance the effectiveness of the CBR similarity measure. This is a central topic for the second version of the SIIS prototype, and is out of the scope of the current research effort.

Taking a global look, one can notice that COAs are generated, or specified in various steps of the planned first iteration of the SIIS prototype. Steps 1 (box A), 5 (box B), and 6 can yield user determined COAs. Steps 3, 4, and 6 can yield system determined COAs. This effectively supports the initial part of step 4 of the IPB/IPOE process: Identify the full set of adversary courses of action. The following sections of this article detail an approach to support the next step: Evaluate and prioritize each course of action.

4.0 A RISK-BASED MULTI-CRITERIA APPROACH FOR THREAT COA EVALUATION

In this section, we will focus on threat COAs evaluation. The evaluation of threat COAs is a multi-criteria analysis problem under uncertainty where the risk component is omnipresent. First, the problem is multi-criteria by nature since the intelligence analyst has to evaluate each threat COA according to a variety of conflicting criteria (suitability, risk involved, complexity, loss of opportunity), to rank them, and to identify the most likely COAs. Second, the threat COAs evaluation problem often deals with uncertainty since the analyst evaluation on each criterion may not necessarily be a crisp value; there may exist many possible values for the outcomes; or, often, the values (scores and weights) can be difficult to express. Third, in the COAs ranking process, the analyst may have a different risk attitude (prone to risk, averse to risk, etc.) depending on the context, the significance and consequences of the COAs, etc.

This paper proposes a risk-based multi-criteria methodology for threat COAs evaluation taking into account i) multiple conflicting criteria ii) the risk attitude of the analyst, iii) the risk as a criteria for threat COAs evaluation and, iv) the uncertainty of the data. In section 4.1, we review the literature in the area of red teaming, computational analysis, multi-criteria analysis and multi-objective risk assessment. Then in section 4.2, we detail the proposed methodology for the risk-based evaluation of the threat courses of action.

4.1 Review of relevant approaches

We provide in this section a review of the main approaches that could benefit to our study such as the computational red teaming, the multi-objective evolutionary computation and the multi-criteria analysis approaches.

Red Teaming (RT) is used in military planning and decision making. It consists of a simulation of blue and red teams where a blue team represents the intent, objectives and interests of the friendly force and a red team emulates enemies and reproduces their motivations, intentions, behaviours and anticipated actions. Computational Red Teaming (CRT) is concerned with the computational side of RT in order to augment a human-based RT exercise with computational models and methods. Abbass *et al.*, (2011) define five different levels of red team modelling. These levels represent increasing degrees of red team adaptability and system complexity. CRT0 equips agents with a generic decision-making model. CRT1 introduces learning (social and evolutionary), in the sense of the agent's ability to change its decision-making process. CRT2 level of red modelling consists of evolutionary algorithms searched for communication strategies that would give the blue team a competitive advantage over a fixed red team. When system-level adaptation occurs within an environment that itself changes and evolves, then we have a red team adaptation at level CRT3. The highest level CRT4 provides the full potential of "learning about competitors" by adding mechanisms of reflection (Abbass *et al.*, 2011). In the context of this work, these computational techniques could benefit to the IPB/IPOE processes and in particular in the threat decision-making process and choice of the threat courses of action.

On another side, when dealing with red team decision-making problems, multiple points of view (objectives, criteria, etc) could enter into consideration in order to best predict the red team best compromise decisions. Multi-objective evolutionary computation and multi-criteria decision analysis (MCDA) are interesting computational approaches that could be of interest for this topic. Multi-objective computation consists of solving decision-making problems under multiple objectives (to be optimised) where the set of solutions is defined by a set of constraints. The MCDA approaches are discrete approaches that consider decision-making problems where a set of discrete alternatives are pre-defined and the decision-maker has to choose among these alternatives.

Multi-objective evolutionary computation is a set of techniques capable of searching for the set of solutions that represent the non-dominated solutions considering the competing objectives. In the last decade, the field of multi-objective evolutionary computation has grown with significant number of efficient algorithms (Abbass, 2006; Tan *et al.*, 2006; Jensen 2004, Coello *et al.*, 2002, Abbass *et al.* 2001). Miettinen (1999) categorises the main approaches in the multi-objective optimisation literature into four categories. The first approach does not use preference information and is called no-preference. The second approach finds all possible non-dominated solutions and then applies the user's preferences (posterior approach). The third approach incorporates user preference prior to the optimization process (a priori approach). The fourth approach combines the posterior and a priori approaches (interactive approach).

In the discrete case when the alternatives are pre-defined, the MCDA discipline is relevant. Two main approaches are developed in the multi-criteria domain: the single criterion approach and the outranking synthesising approach (Roy, 1985). The single criterion approach consists of building an aggregation function using the individual scores with regard to each criterion in order to represent the global score of each alternative. This approach aims at constructing a value system that aggregates the analyst preferences on the criteria (attributes) based on strict assumptions (only strict preference and indifference are considered). The outranking synthesising approach is inspired from the social choice theory. It is based on the pairwise comparison of the COAs along each criterion. Each criterion is considered as a voter, with a particular voting power fixed accordingly with the analyst, and each COA as a candidate (Roy, 1985). The analyst preferences are modeled throughout a set of parameters (thresholds) and the aggregation is partially compensatory. With outranking methods, the preference relation system obtained could include the indifference, the preference and the incomparability between alternatives. In general, MCDA methods lead either to a choice of the best alternative, or to a ranking of the alternatives according to their performances, or to a sorting of the alternatives into different categories. Most MCDA methods assume that the ratings of alternatives and the weights of criteria are crisp numbers. For COAs evaluation, this assumption is unrealistic because uncertainties could arise from information that is not quantifiable, incomplete, or difficult to obtain because of partial ignorance. The review of the literature shows that probabilistic methods were explored in dealing with MCDA under uncertainty (Fenton and Neil, 2001; Watthayu and Peng, 2004) as well as fuzzy set theory (Bellman and Zadeh, 1970, Robert and Fuller, 1996; Ribeiro, 1996; Yager, 2002). More specifically for fuzzy multi-criteria analysis, there exist four different methodologies: the fuzzy ranking methods, the fuzzy analytic hierarchy process (AHP) methods, defuzzification based methods, and fuzzy outranking methods. Some examples of fuzzy methods have been developed in Yager (2002); Yager (2000); Chen (2000); Deng (1999); Cheng *et al.* (1999); Yeh and Deng (1997); Ribeiro (1996). Fuzzy methods were derived from the approximation approach as the fuzzy max-min (Yager 1977) and the fuzzy weighted sum (Baas et Kwakernaak, 1977; Dubois and Prade, 1982; Tseng and Klein, 1992). The methods related to the symbolic approach as the LOWA - Linguistic Ordered Weighted Averaging and ILOWA - Inverse Linguistic Ordered Weighted Averaging (Herrera *et al.*, 1997) were developed. Other research also generalized some classical methods to the fuzzy context such as fuzzy TOPSIS (Chen, 2000) and fuzzy AHP (Cheng *et al.*, 1999).

In this paper, the proposed approach in Section 4.2 will be based on MCDA because in general, the set of alternatives with which the threat is concerned is a discrete set for which each alternative is evaluated according to a set of conflicting criteria. In future works, Computational Red Teaming would be considered for the simulation of red decisions and the assessment of the interaction with blue forces.

4.2 Risk-based multi-criteria methodology

The methodology that will be used in order to evaluate, compare and rank the different COAs previously generated by the prototype consists of the following five steps. First, we define the list of criteria and how we will model the analyst preferences. Then, we present the way uncertainty in outcomes will be modelled with fuzzy sets, as well as the analyst risk attitude. The final step of the methodology will consist of applying the fuzzy multi-criteria TOPSIS model to rank the different COAs.

Step 1: Evaluating the COAs according to the set of criteria
Step 2: Modeling the analyst preferences
Step 3: Representing uncertainty in outcomes as fuzzy sets
Step 4: Modeling the analyst risk attitude
Step 5: Applying a fuzzy multi-criteria method to rank the COAs

4.2.1 Evaluating the COAs according to the set of criteria

Once the set of COAs is well defined, the analyst has to evaluate and rank/prioritize the COAs. Before starting the prioritization process, the analyst needs to analyze two constraints: the feasibility and the uniqueness of each COA. If the COA is not feasible or not unique (significantly different from others), it will be eliminated from the set of COAs in the further steps. Uniqueness refers to the fact that each threat COA must be significantly different from the others. Otherwise, the threat COA will be considered as a variation rather than a distinct COA. Feasibility refers to the availability of the necessary conditions for the accomplishment of COA (time, space, resources, and physical means). Before discounting the threat COA, the analyst has to analyze if there is any action or radical measures the threat might take to create the conditions needed for success. Examples from the doctrine (IPB Field Manual, 1994) refer to the fact that the threat might conduct economy of force operations in some sectors in order to generate sufficient combat power for offensive operations in others. The threat's lack of resources might force it to violate its own doctrine in order to accomplish its objective. In these cases, the COA will not be eliminated.

<u>The set of criteria</u>

In order to prioritize threat COAs, the analyst needs to substitute himself to the threat and to evaluate how well each COA meets the criteria of suitability, complexity, risk, and loss of opportunities/cost. The threat will prefer the COA that offers the greatest advantages while minimizing risk. The criteria are regrouped in 4 categories:

- **Suitability**: This category includes five different criteria. The first criterion refers to the degree to which the threat COA has the potential for accomplishing the threat's likely objective or desired end state. The second criterion consists of the degree to which the COA is consistent with the doctrine, TTPs and past activities. While evaluating the COA on this criterion, the analyst should take into consideration the option that the threat would eventually want to achieve surprise by deviating from known doctrine or using "wildcard" COAs. The third, fourth and fifth criteria refer to the extent to which the COA takes advantage respectively of threat capability (equipment, weaponry, training, etc.), battlefield environment, and friendly disposition.

Suitability		
C1	Accomplishing threat's objectives	Maximise
C2	Consistency with doctrine and past activities	Maximise
C3	Taking advantage of threat capability (equipment, weaponry, training)	Maximise
C4	Taking advantage of the battlefield environment	Maximise
C5	Taking advantage of the friendly disposition	Maximise

- **Risk**: This category refers to the amount of risk that the COA involves in term of threat personnel loss, collateral damage, confrontation risk, equipment reliability, and personnel effectiveness. This category, called "Acceptability" in the doctrine, evaluates the degree to which the threat forces accept the amount of risk entailed in adopting the COA and the degree to which they can afford the expenditure of resources for an uncertain chance at success. Evaluating this kind of risk is a subjective judgment based on knowledge of the threat and its doctrine.

Risk		
C8	Threat personnel loss	Minimise
C9	Collateral damage	Minimise
C10	Confrontation risk	Minimise
C11	Equipment reliability	Maximise
C12	Personnel effectiveness	Maximise

- **Complexity**: This category encompasses both operation and logistic complexity. It refers to the degree to which conducting such COA could be complex and difficult in term of C2, logistic, etc.

Complexity		
C6	Operation complexity	Minimise
C7	Logistic complexity	Minimise

- **Loss of opportunities/cost**: This criterion refers to the cost of material resources involved in the COAs.

Loss of opportunities		
C13	Cost of resources	Minimise

COAs Evaluation

In practice when evaluating the threat COAs, it is more natural for the intelligence analyst to describe the COAs ratings according to each criterion in linguistic terms, e.g. "very low", "medium", "high", "fair", etc. Within the prototype, the analyst will still express his ratings in linguistic term.

Suppose we have m courses of action *COAi* (*i*=1,..,*m*) and n criteria *Cj* (*j*=1,..,*n*). The evaluation matrix is expressed by:

$$\begin{array}{cc} & C_j \\ COA_i & \begin{bmatrix} \tilde{x}_{11} & \cdots & \tilde{x}_{1n} \\ \vdots & \ddots & \vdots \\ \tilde{x}_{m1} & \cdots & \tilde{x}_{mn} \end{bmatrix} \end{array} \quad (1)$$

$\tilde{x}_{ij}$ represents the linguistic rating of alternative A_i with respect to criterion C_j. The relative importance of criteria is given by $\widetilde{W} = (\widetilde{w}_i)$ where $\widetilde{w}_j$ represents the weight of criterion C_j.

4.2.2 Modelling the analyst preferences

Once the multi-criteria matrix is completed with the linguistic variables, the next step will consist of articulating and modelling how the analyst would prefer a COA over another when he compares them on a given criterion. The assessment of a model reflecting, at best, these preferences could be done using: utility theory, valued functions, pairwise comparison, tradeoffs, discrimination thresholds, etc. Three types of criteria could be considered:

- ✓ True criteria: actions are indifferent only in the case where the evaluations of the two COAs are equal.
- ✓ Quasi-criterion: could be considered by the analyst in case of hesitations, doubts, indecision, etc. In that case, there will be indifference between two COAs alternatives if the difference between the ratings differs by less than a q_j indifference threshold.
- ✓ Pseudo-criterion: In addition to the indifference threshold defined in the quasi-criterion, the pseudo-criterion adds a preference threshold. Strong preference occurs if the ratings of two alternatives differ by at least p_j; weak preference occurs if the difference of ratings is between p_j and q_j.

In addition, the analyst will express the weights (relative importance) for each criterion. When expressing these weights, he should deduce what are the most and less important criteria from the threat's point de view and could rely on his understanding of the threat's priorities and risk assessment. He can express these weights either numerically or with linguistic terms.

4.2.3 Representing uncertainty in outcomes as fuzzy sets

Many types of uncertainty and risk exist. Stewart (2005) defines two categories of uncertainty: external and internal uncertainty. External uncertainty refers to the lack of knowledge about the consequences of a particular choice (decision). This includes i) random uncertainty that arises because of unpredictable state of the nature (this is outside the control of the analyst) and ii) epistemic uncertainty that is due to lack of data and knowledge about different phenomena. Internal uncertainty is related to ambiguity/imprecision of the data because it refers to human judgments, preferences, values and risk attitudes.

The IPB process in COIN context is concerned with both external and internal uncertainty. On one side, external uncertainty, as defined by Stewart (2005), exists because insurgents do not behave according to a predictable template. For instance, even if the parameters for their equipment could be known, their tactics are variable and almost never rely on group formations as a traditional formed effort. On the other side, internal uncertainty is omnipresent because the intelligence analyst deal with imprecise data that is usually subjective, determined based on human judgments and which depends on the analyst risk attitude.

In this paper, we consider internal uncertainty due to imprecision and subjective human judgment. The ratings of the threat COAs are expressed in linguistic terms, e.g. "very low", "medium", "high", "fair", etc. Then, the linguistic decision analysis approach (Tong and Bonissone 1980; Herrera and Herrera, 2000, Herrera *et al.*, 2000) will be used as an approximative way to represent natural words or sentences used in human judgment and perception. Accordingly, the linguistic description of the analyst will be transformed into fuzzy numbers in order to deal with the ratings uncertainty. A fuzzy number is a convex fuzzy set, characterized by a given interval of real numbers, each with a grade of membership between 0 and 1. In this paper, we consider triangular fuzzy numbers, whose membership function is defined as:

$$\mu_{\hat{a}}(x) = \begin{cases} (x-a_1)/(a_2-a_1), & a_1 \le x \le a_2 \\ (a_3-x)/(a_3-a_2), & a_2 \le x \le a_3 \\ 0, & Otherwise \end{cases} \qquad (2)$$

The triangular fuzzy number is based on a three-value judgment: the minimum possible value a_1, the most possible value a_2 and the maximum possible value a_3.

Example of linguistic variables modelled with fuzzy numbers

Term	Membership function
Very low	(0.00, 0.10, 0.25)
Low	(0.15, 0.30, 0.45)
Medium	(0.35, 0.50, 0.65)
High	(0.55, 0.70, 0.85)
Very high	(0.75, 0.90, 1.00)

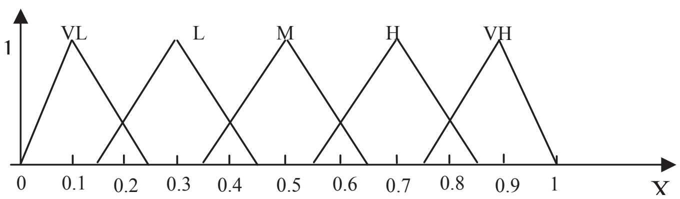

Figure 3: Fuzzy triangular membership functions

4.2.4 Modelling the analyst risk attitude

Another source of uncertainty is related to user preferences, in particular his attitude towards risk. The set of best compromise solutions should account for different attitudes towards risk and should be robust against variations in the attitude to risk of the decision-maker (Bui and Abbass, 2010). Step 4 of the methodology consists of modelling the attitude to risk of the intelligence analyst in a multi-criteria discrete context.

When evaluating and ranking different threat COAs, the intelligence analyst could express different risk attitudes (from absolutely optimistic to absolutely pessimistic), depending on the context, on the significance of the COA, and on its consequences. The attitude towards the risk of the analyst will have an impact on the ranking of the different COAs. The intelligence analyst's risk attitude could also differ from one criterion to another depending on the relative importance of each criterion. Ultimately, the analyst would not like to take risk for the evaluation of the criteria with high relative importance.

To model the risk attitude of the intelligence analyst, we consider the work of Fenton and Wang (2006) that proposes how to incorporate the DM's risk attitudes into the general fuzzy MCDA approach. The authors use natural language to describe an appropriate range of attitudes between the extremes of "optimism" and "pessimism". In this work, nine terms expressing nine different attitudes towards risk were considered based on Miller's theory of cognitive retention (Miller, 1956). Then for each term, the fuzzy number expressing the linguistic variable (ratings of the COA on a certain criteria) is modified to model the extent to which the evaluation is impacted by the risk attitude.

To incorporate the risk attitude to the triangular fuzzy number (a_1, a_2, a_3), Fenton and Wang (2006) use an ordered structure. As shown in table 1, the COA evaluation will be modeled with (a_1, a_2, a_3) for neutral attitude, with (a_1, a_3, a_3) and (a_1, a_1, a_3) respectively for absolutely optimistic (AO) and absolutely pessimistic (AP) for criteria to be maximized. If the criteria has to be minimised, (a_1, a_3, a_3) and (a_1, a_1, a_3) will respectively model the fuzzy number for absolutely pessimistic (AP) and absolutely optimistic (AO).

Table 1: Linguistic terms of risk attitudes and their related fuzzy numbers

Linguistic term	Triangular fuzzy number derived from (a_1, a_2, a_3) for criteria to be maximised	Triangular fuzzy number derived from (a_1, a_2, a_3) for criteria to be minimised
Absolutely optimistic (AO)	(a_1, a_3, a_3)	(a_1, a_1, a_3)
Very optimistic (VO)	$(a_1, (a_2 + 3a_3)/4, a_3)$	$(a_1, (a_2 + 3a_1)/4, a_3)$
Optimistic (O)	$(a_1, (a_2 + a_3)/2, a_3)$	$(a_1, (a_2 + a_1)/2, a_3)$
Fairly Optimistic (FO)	$(a_1, (3a_2 + a_3)/4, a_3)$	$(a_1, (3a_2 + a_1)/4, a_3)$
neutral	(a_1, a_2, a_3)	(a_1, a_2, a_3)
Fairly Pessimistic (FP)	$(a_1, (3a_2 + a_1)/4, a_3)$	$(a_1, (3a_2 + a_3)/4, a_3)$
Pessimistic (P)	$(a_1, (a_2 + a_1)/2, a_3)$	$(a_1, (a_2 + a_3)/2, a_3)$
Very pessimistic (VP)	$(a_1, (a_2 + 3a_1)/4, a_3)$	$(a_1, (a_2 + 3a_3)/4, a_3)$
Absolutely pessimistic (AP)	(a_1, a_1, a_3)	(a_1, a_3, a_3)

4.2.5 Applying the fuzzy TOPSIS method

To perform the ranking of the different COAs, we make the choice of the TOPSIS (technique for order performance by similarity to ideal solution) method. The primary concept of TOPSIS approach relies on the fact that the most preferred alternative should not only have the shortest distance from the ideal solution, but also have the farthest distance from the anti-ideal solution. The crisp TOPSIS method was first developed by Hwang and Yoon (1981). TOPSIS was then extended in a fuzzy context using the Euclidean distance between any two fuzzy numbers as defined by Chen (2000). In this work, we make the choice of the fuzzy TOPSIS method because of its numerous advantages. It is a simple method that uses a comprehensible concept and has good computational efficiency.

More specifically, here are the main steps in the ranking process.

Step 1: Evaluate the linguistic COAs ratings for each criterion (considering the risk attitude as modeled in section 5.2.3) and the appropriate linguistic variables ($\widetilde{w}_j, j = 1, \dots, n$) for the weight of the criteria.

Step 2: Construct the weighted fuzzy decision matrix $\tilde{V} = [\tilde{v}_{ij} = \widetilde{w}_j . \tilde{x}_{ij},\ i = 1, \dots, m; j = 1, \dots, n]$. Let us note that the ranges of triangular numbers belongs to [0,1], thus there is no need for normalization. The multiplication of two fuzzy numbers will use the basic operation on fuzzy triangular numbers as follows $\tilde{a} * \tilde{b} = (a_1 * b_1,\ a_2 * b_2,\ a_3 * b_3)$.

Step 3: Identify the fuzzy ideal A^+ and the fuzzy anti-ideal solution A^-. The fuzzy ideal solution has the maximum ratings at all the criteria and the fuzzy anti-ideal solution has the minimum ratings at all the criteria.

$$A^+ = \left(\widetilde{v_1}^+, \widetilde{v_2}^+, \dots, \widetilde{v_n}^+\right) = \left[max_i\left(\tilde{v}_{ij}, i = 1, \dots, m\right), j = 1, \dots, n\right] \quad (3)$$

$$A^- = \left(\widetilde{v_1}^-, \widetilde{v_2}^-, \dots, \widetilde{v_n}^-\right) = \left[min_i\left(\tilde{v}_{ij}, i = 1, \dots, m\right), j = 1, \dots, n\right] \quad (4)$$

Step 4: Calculate the distance of each alternative from the ideal and the anti-ideal. To do so, the Euclidian distance defined by Chen (2000) is used. Let us consider two triangular fuzzy numbers $\widetilde{m} = (m_1, m_2, m_3)$ and $\tilde{n} = (n_1, n_2, n_3)$, the Euclidean distance is computed with Eq. (5).

$$d(\tilde{m},\tilde{n}) = \sqrt{1/3[(m_1-n_1)^2+(m_2-n_2)^2+(m_3-n_3)^2]} \qquad (5)$$

The distances to the ideal solution $d_i^+ = \sum_{j=1}^{n} d(\tilde{v}_{ij},\tilde{v}_j^+),\ i=1,\dots,m$ and to the anti-ideal solution $d_i^- = \sum_{j=1}^{n} d(\tilde{v}_{ij},\tilde{v}_j^-),\ i=1,\dots,m$ are computed using Eq. (5).

Step 5: Calculate similarities to ideal solution, which is a crisp value computed by Eq. (6).

$$S_i = \frac{d_i^+}{d_i^+ + d_i^-} \qquad (6)$$

Step 6: Rank the different alternatives according to S_i in decreasing order.

5.0 CONCLUSION

This paper focuses on the IPB/IPOE process in a COIN context and more specifically deals with the generation and evaluation of threat COAs. First, it presents a high level description of a self inference system prototype which aims at supporting the threat and COAs generation of the IPB/IPOE process. The research & technology roadmap for the prototype development is described. In particular, the paper explains how the self inference prototype will generate threat COAs. The involved reasoning techniques are also discussed: inference components (rule-based, description logics, kinematic and geo-spatial analysis), case-based reasoning, multiple hypothesis situation analysis, and threat analysis ontology.

Then, the paper focuses on the evaluation of the threat COAs and proposes a risk-based multi-criteria approach under uncertainty to solve the problem and prioritize the COAs. The proposed evaluation methodology takes into account i) multiple conflicting criteria, ii) the risk attitude of the analyst, iii) the risk as a criteria of evaluation, and iv) the uncertainty (ambiguity, imprecision) of the data. This kind of uncertainty is due to subjective human judgments, preferences, values and attitude towards risk. For the evaluation of the threat COAs, the proposed approach considers a panoply of conflicting criteria related to suitability, risk, complexity and loss of opportunities. The ratings of the threat COAs are expressed in linguistic terms and then transformed into fuzzy numbers in order to properly deal with the uncertainty of the ratings. In addition, the methodology takes into consideration the risk attitude of the intelligence analyst. To do so, the fuzzy ratings of the COAs are modified to model the extent to which the evaluation of the analyst could be impacted by his risk attitude. Finally, the ranking of the different COAs is performed using the fuzzy TOPSIS method.

In future work, we aim to extend the risk-based multi-criteria approach used in this paper to a dynamic context where random uncertainty, which arises because of the unpredictable state of nature (not under control), is present. In fact, another factor that adds considerably to the complexity of IPB/IPOE step 4 in COIN context is the dynamic nature of such operational environments. Dynamic situations not only exert some time pressure for the analyst to provide recommendations due to their continuously and rapid changing nature but also require frequent re-assessments of the threats and the COAs. For instance, the initial priority order of threat COAs does not account for the friendly COA, since one has not yet been selected. Friendly dispositions may change as the command moves to adopt its own COA, which will change the likelihood of each threat COA. Thus, after the commander has selected the friendly COA, the intelligence analyst should reprioritize the initial list of threat COAs to reflect changed friendly dispositions and activities. Similarly, any action in the operational environment from blue or white actors may have immediate and significant consequences on the situation.

7.0 REFERENCES

[1] Abbass, H.A., “An economical cognitive approach for bi-objective optimization using bliss points, visualization and interaction”, *soft computing*, vol 10, no 8, pp. 687-698, 2006.

[2] Abbass, H.A., Sarker R., and Newton C., “PDE: A pareto frontier differential evolution approach for multi-objective optimization problems, In Proceedings Evolutionary Computation, Seoul, Korea, IEEE Service Centre 2001, vol. 2, pp.971-978.

[3] Abbass H., bender, A., Gaidow S., (2011), Computational red teaming: past, present and future, IEEE Computational intelligence Magazine, IEEE Press, vol 6, Februray 2011.

[4] [Abi-Zeid and Demers, 2010] Abi-Zeid, I., Demers, H., *Enhancing Reasoning Capabilities for the Multi-Intelligence Tools Suite – Maritime (MITS-M) - A Case-Based Reasoning Analysis*, OODA Technologies, DRDC Scientific Authority: Alexandre Bergeron Guyard, DRDC-Valcartier CR 2010-234, Defence R&D Canada - Valcartier, June 2010.

[5] [Baas and Kwakernaak, 1977] Baas, S. M. et Kwakernaak, H., “Rating and Ranking of Multi-Aspect Alternatives Using Fuzzy Sets”, *Automatica*, vol. 13, pp. 47-58, 1977.

[6] [Banbury *et al.*, 2011] Banbury, Becking, I., Bentahar, J., *Study of SNA, IPB/IPOE and COIN - IPB/IPOE Reasoning Requirement Inventory Report*, Thales Systems Canada, DRDC Scientific Authority: Alexandre Bergeron Guyard, DRDC-Valcartier CR 2011-094, Defence R&D Canada - Valcartier, March 2011.

[7] Bellman R.E., Zadeh, L.A., Decision Making in a fuzzy environment, Management Science, vol 17 (1970), pp 141-164.

[8] [Bergeron Guyard and Roy, 2010] Bergeron Guyard, A, Roy, J. Multiple Hypothesis Situation Analysis: Governing Principles and Support System, DRDC Valcartier TR 2010-525, December 2010.

[9] [Bergeron Guyard, 2010] Bergeron Guyard, A., *Case-Based Reasoning for Maritime Anomaly Detection*, COGnitive systems with Interactive Sensors (COGIS 2010), Crawley, United Kingdom, November 2010.

[10] Bui, L.T., Abbass H.A., Barlow M., Bender A., “Robustness against the decision-maker’s attitude to risk in problems with conflicting objectives, IEEE Transactions on evolutionary computation, In print, available from IEEE TEVC online first, 2010.

[11] [Cheng *et al.*, 1999] Cheng, C.H., Yang, K.L., Hwang, C.L., Evaluating attack helicopters by AHP based on linguistic variable weight, European Journal of Operational Research 116, pp. 423-435, 1999.

[12] [Chen, 2000] Chen C.T., Extensions of the TOPSIS for group decision-making under fuzzy environment, Fuzzy Sets and Systems 114 pp. 1-9, 2000.

[13] Coello, C.A.C., Veldhuizen, D.A.V., and Lamont G.B., *Evolutionary algorithms for solving multi-objective problems*, New York, Kluwer Academic, 2002.

[14] [Demers *et al.*, 2010] Demers, H., Allard, Y., Davenport, M., Abi-Zeid, I., *Enhancing Reasoning Capabilities for the Multi-Intelligence Tools Suite – Maritime (MITS-M) -Final Report*, OODA

Technologies, DRDC Scientific Authority: Alexandre Bergeron Guyard, DRDC-Valcartier CR 2010-236, Defence R&D Canada - Valcartier, June 2010.

[15] [Deng, 1999] Deng, H., Multi-criteria analysis with fuzzy pairwise comparison, International Journal of Approximate Reasoning 21 pp. 215-231, 1999.

[16] [Dubois and Prade, 1982] Dubois, D. and Pra de, H., "The Use of Fuzzy Numbers in Decision Analysis", In: Gupta, M.M. et Sanchez, E. (eds.), *Fuzzy Information and Decision Processes*, North-Holland, pp.309-321, 1982.

[17] [Fenton and Wang, 2006] Fenton, N., Wang W., "Risk and confidence analysis for fuzzy multicriteria decision making", Knowledge Based systems, Vol 19, issue 6, pp 381-446, October 2006.

[18] Fenton N., Neil, M., "Making decisions: using Bayesian nets and MCDA", Knowledge Based Systems vol 14 (2001), pp. 307-325.

[19] [Herrera and Herrera-Viedma, 1997] Herrera F. and Herrera-Viedma, E., "Aggregation Operators for linguistic Weighted Information" *IEEE Transactions on Systems, Man and Cybernetics*, vol 27, 1997.

[20] Herrera F., Herrera-Viedma E., Lin guistic decision analysis: steps for solving decision problems under linguistic information, Fuzzy Sets and Systems, vol 115 (2000), pp. 67-82.

[21] Herrera F., Herrera-Viedma E., Martinez L., A fusion approach for managing multi-granularity linguistic term sets in decision making, Fuzzy Sets and Systems, vol 114 (2000), pp. 43-58.

[22] [Hwang and Yoon, 1981] Hwang, C. L. et Yoon, K., Multiple Attribute Decision Making, Methods and Applications : a State of the Art Survey, Springer Verlag, New York, 259p, 1981.

[23] [Intelligence Field Manual, 2001] B-GL-357-001/FP-001, *Intelligence, Field Manual*, Land Forces Information Operations, January 2001.

[24] [IPB Field Manual, 1994] FM 34-130, Intelligence Preparation of the Battlefield, Field Manual, July 1994.

[25] Jensen M.T., "Helper-objectives: Using multi-objective evolutionary algorithms for single-objective optimization", *Journal of Math. Model. Algorithms*, vol. 1, no. 25, 2004.

[26] Miettinen K. (1999), Nonlinear multiobjective optimization, Boston, MA: Kluwer Academic.

[27] Miller, G.A., "The magic number seven, plus or minus two, Psychological review 63 (1956), 81-97.

[28] [Ribeiro, 1996] Ribeiro, R.A., Fuzzy multiple attribute decision making: A review and new preference elicitation techniques, Fuzzy Sets and Systems 78, pp. 155-181, 1996.

[29] Robert C.C, Fuller R., Fuzzy multiple criteria decision-making: recent developments, Fuzzy Sets and Systems, vol 78, (1996), pp. 139-153.

[30] [Roy and Be rgeron Guyard, 2010] Roy, J., Bergeron Gu yard, A., *Multiple Hypothesis Situation Analysis Support System Prototype*, 13th International Conference on In formation Fusion (Fusion

2010), Edinburgh, United Kingdom, July 2010.

[31] [Roy, 1985] Roy, B., "Méthodologie multicritère d'aide à la decision", Economica, Paris, 1985.

[32] Stewart TH. (2005) "Dealing with uncertainties in MCDA", In International Series in Operations Research & Management Science, Vol. 78, Jose´ F, Salvatore G, Matthias E (eds). Springer: New York; 445–466.

[33] Tan K.C., Yang Y. J., Goh C.K., « A distributed cooperative coevolutionary algorithm for multi-objective optimization, *IEEE Transaction on Evolutionary Computation*, vol. 10, no. 5., pp 527-549, 2006.

[34] Tong R.M., Bonissone P.P "A linguistic approach to decision making with fuzzy sets, IEEE Transactions on Systems Man and Cybernetics, vol SMC-10 (1980), pp. 716-723.

[35] [Tseng and Klein, 1992] Tseng, T.Y. et Klein, C.M., "A New Algorithm for Fuzzy Multicriteria Decision Making", vol. 6, pp. 45-66, 1992.

[36] [Tremblay *et al.*, 2011] Tremblay, S., Rousseau, R., Bentahar, J., Banbury, S., Miller, J., Becking, I., Rioux, F., *Study of SNA, IPB/IPOE and COIN - IPB/IPOE Chapter*, Thales Systems Canada, DRDC Scientific Authority: Alexandre Bergeron Guyard, DRDC-Valcartier CR 2011-091, Defence R&D Canada - Valcartier, March 2011.

[37] [US Joint IPOE, 2009] US Joint Intelligence Preparation of the Operational Environment, Joint Publication 2-01.3, June 2009.

[38] Watthayu W., Peng Y., "A Bayesian network based framework for multi-criteria decision making", in MCDM 2004, Whistler, B.C. Canada August 6-11, 2004.

[39] [Yager, 2000] Yager, R.R., Fuzzy modeling for intelligent decision making under uncertainty, IEEE Transactions on Systems Man and Cybernetics – Part B: Cybernetics 30, pp. 60-70, 2000.

[40] [Yager, 2002] Yager, R.R., On the valuation of alternatives for decision-Making under uncertainty, International Journal of Intelligent Systems, 17, pp. 687-707, 2002.

[41] [Yager, 1977] Yager, R. R., "Multiple Objective Decision-making Using Fuzzy Sets", *Int. J. Man-Mach. Stud.*, vol. 9, pp. 375-382, 1977.

[42] [Yeh and Deng, 1997] Yeh, C.H., Deng, H., An algorithm for fuzzy multi-criteria decision making, Proc. of the IEEE International Conference on Intelligent Processing Systems, pp. 1564-1568, 1997.