Decision Support for Asymmetric Urban Warfare

Tracey Enderwick
Applied Maths and Operational Research Group
Royal Military College of Science
Cranfield University, Shrivenham
Swindon, Wiltshire
SN6 8LA
UNITED KINGDOM

t.c.enderwick@cranfield.ac.uk

Dr. Ken McNaught
Applied Maths and Operational Research Group
Royal Military College of Science
Cranfield University, Shrivenham
Swindon, Wiltshire
SN6 8LA
UNITED KINGDOM

k.r.mcnaught@cranfield.ac.uk

ABSTRACT

The deciphering of intelligence is a complex task and if not explained clearly can cause confusion in battle, ultimately increasing the probability of fratricide and loss. Various methods have been tried to simplify the deciphering of intelligence, many of which are simplistic and deterministic in their nature (e.g. fuzzy logic). In this paper, we employ two probabilistic techniques (Bayesian Networks and Influence Diagrams), widely accepted in a variety of industries, to aid decision makers by determining the most probable outcome based on the intelligence known at the time. The methodology described in this paper relates to an asymmetric urban warfare scenario and has proven to be robust and insensitive to reasonable changes in the data. The time taken to develop and understand a Bayesian Network or Influence Diagram makes it improbable for satisfactory use within a high tempo real life scenario. These tools are potentially useful during the intelligence preparation phase and as decision support tools for areas such as troop allocation and operational planning.

1.0 INTRODUCTION

"If you know the enemy and know yourself, you need not fear the result of a hundred battles. If you know yourself but not the enemy, for every victory gained you will also suffer a defeat. If you know neither the enemy nor yourself, you will succumb in every battle"

Sun Tzu [1]

Since the disbandment of the USSR in 1991 and the end of the cold war, there has been no major symmetric super power to threaten NATO. UK troops have withdrawn from the Central European Theatre and are increasingly willing to intervene in other areas of the world, e.g. Bosnia, Kosovo and Iraq.

The intervention of NATO/UN personnel in the Middle East has, in some cases, increased resentment to western actions (particularly towards the US). This resentment combined with a rise in the number of Islamic extremists and nationalists, many of whom have formed resistance groups against NATO/UN actions, has become a cause of concern to the NATO/UN coalition forces. The resistance groups are changing the nature of threats faced by NATO/UN personnel; battles fought in the Middle East are now becoming more asymmetric and more fragmented.

Unlike the more predictable Warsaw pact forces which NATO forces were long trained to counter, the resistance groups have no formal military doctrines and many are without formal training. The rise in

Enderwick, T.; McNaught, K. (2006) Decision Support for Asymmetric Urban Warfare. In *Information Fusion for Command Support* (pp. 6-1 – 6-12). Meeting Proceedings RTO-MP-IST-055, Paper 6. Neuilly-sur-Seine, France: RTO. Available from: http://www.rto.nato.int/abstracts.asp.

these resistance groups has resulted in a pronounced increase in unconventional (asymmetric) warfare. Asymmetric warfare occurs when there is a strong difference between the strengths and tactics of the two opponents. The conventional forces are facing smaller coalitions and militia with limited arsenals and combatants, rather than national armies. Hence, the nature of the battle is very different to conventional battles. The militia apply manoeuvres and use weapons that will circumvent the superiority of their opponents. The asymmetric attacks against the vulnerabilities of the conventional forces aim to impose strong psychological as well as physical damage [2]. The attacks in post war Iraq have seen a rise in the number of suicide bombers, ambushes and improvised explosive devices used against both NATO forces and regular civilians. This asymmetric nature of warfare presents NATO/UN personnel with the difficult task of trying to predict when and where the next attack will take place. The gathering and deciphering of intelligence aims to assist commanders in estimating the timing and location of potential attacks and provides an increased situation awareness of the scenario.

This paper will introduce two possible methods for intelligence deciphering: Bayesian Networks and Influence Diagrams.

1.1 Methodology

1.1.1 Bayesian Networks

A Bayesian Network is a directed, acyclic, graphical model (DAG) containing both qualitative and quantitative features. The qualitative aspect is the representation of a real world scenario in a graphical form. The variables of interest in the domain of the scenario are represented by nodes[1] and the relationships between the variables are represented by arcs linking the nodes. The quantitative aspect uses data and/or domain expertise to derive prior marginal probabilities for each root node and conditional probability distributions for the remaining nodes. The root nodes have no parents and are not dependent upon any other factors within the domain (e.g. time of day); the probability distributions of nodes with parents (i.e. child nodes) are conditioned on the state of nature of each parent.

The main aim of a Bayesian Network is to provide estimates of certainties for events that are not observable (or are only observable at an unacceptable cost). These are known as hypothesis events, which are grouped into sets of mutually exclusive events and represented by *hypothesis variables*. *Information variables* are variables which can be observed; once instantiated the Bayesian Network updates other nodes which can ultimately result in a change in the distributions of the hypothesis variables. This method of belief updating is termed *propagation* and utilises Bayes' theorem to determine the updated marginal values. *Mediating variables* lie between the hypothesis variable and the observable information nodes and relate to things that are not directly observable but would be useful to know. See Figure 1 for an example of a generic Bayesian Network.

[1] The terms nodes and variables are used interchangeably throughout this document.

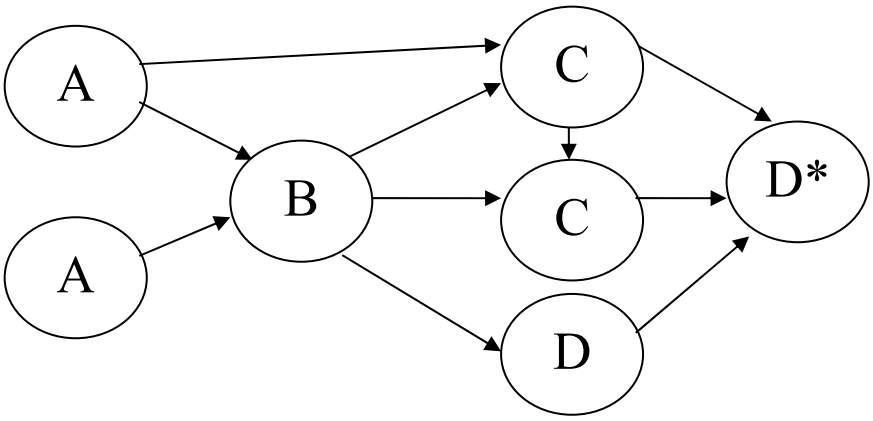

Figure 1: A simplified, generic Bayesian Network

In Figure 1, the A nodes represent the background prior nodes (root nodes), node B the hypothesis node, nodes C the mediating nodes and nodes D the observable information nodes. If node D* is known, i.e. *instantiated*, then the prior marginals, for the remaining nodes, are updated through propagation resulting in posterior marginals. A prior marginal is the initial overall probability of a state occurring given the initial information known about its parents. For example, if nodes A and B are the parents of node C (see Figure 2) and both have a 50/50 chance of occurring and node C has the following conditional probability table:

Node A	Node B	True	False
True	True	50%	50%
True	False	25%	75%
False	True	25%	75%
False	False	0%	100%

Table 1: Conditional Probability table for Marginal example

Without any instantiations the prior marginal values for node C are 25% and 75% for true and false respectively. If node A is instantiated as true then the resulting posterior marginals become 37.5% and 62.5% for node C; node B remains unchanged.

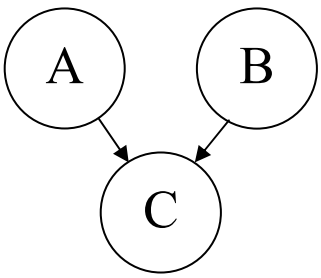

Figure 2: Simple Bayesian Network for Marginal Example

Definition: A Bayesian Network consists of the following ([3]):

- A set of *variables* and a set of *directed edges* between variables
- Each variable has a set of mutually exclusive states
- The variables and the directed edges form a *direct acyclic graph* (DAG). (A directed graph is acyclic if there is no directed path $A_1 \rightarrow \ldots \rightarrow A_n$ such that $A_1 = A_n$)
- To each variable A with parents $B_1,\ldots,B_n$, there is attached a potential table $P(A|B_1,\ldots,B_n)$

1.1.2 Influence Diagrams

Although Influence Diagrams were originally developed by Howard and Matheson [4], as a compact representation of a decision problem to avoid the bushiness of decision trees, they are now becoming more popular as an extension of the Bayesian Network. Extending the Bayesian Network requires the use of decision nodes and utility nodes associated with the problem. The decisions are represented by rectangular nodes; whilst the utilities are represented by rhombus nodes. The decision aspect of an Influence Diagram is treated within the framework of *utility theory.*

Definition of Influence Diagrams ([3])

An Influence Diagram consists of a directed acyclic graph over chance nodes, decision nodes and utility nodes with the following structural properties:

- There is a directed path comprising all decision nodes
- The utility nodes have no children
- The utility nodes have no states but are a representation of the worth to the decision maker of every possible outcome, i.e. every possible combination of parent node states. Hence, each utility node U has a real-valued function over pa(U).
- The decision nodes and chance nodes have a finite set of mutually exclusive states
- For each chance node A there is either a conditional probability table P(A|pa(A)) or probability function *f*(A), where pa(A) represents all the parent nodes of A.

Simplified Influence Diagram

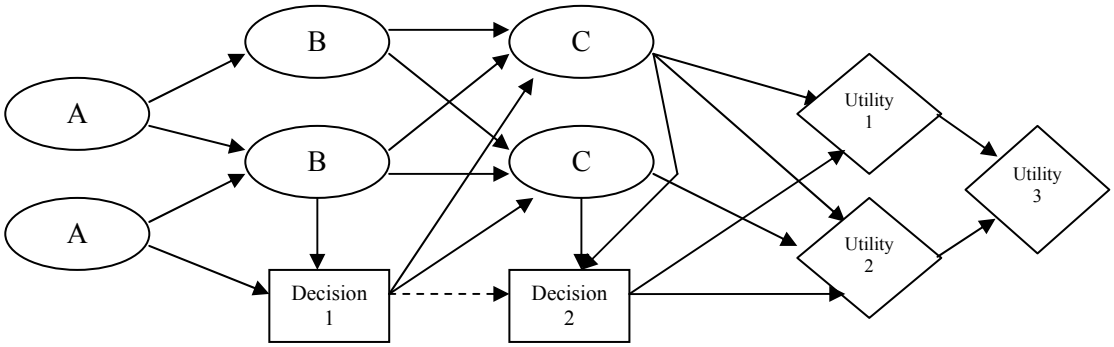

Figure 3: Simplified Influence Diagram

In the simplified Influence Diagram the A nodes represent independent root variables which are not directly effected by the domain of interest, e.g. time of day. B and C nodes can be information, mediating or even hypothesis variables conditionally dependent on the state of their parent nodes. The links leading into a decision node from a chance node are commonly known as information links whilst the dashed arc between the decision nodes is a precedence link. Whenever there are multiple utility nodes in an Influence Diagram it is common to have a "super" utility node combining the individual utilities into one overall utility.

2.0 SCENARIO DESCRIPTION

After the collapse of the old government regime, during a war with its neighbour, some of Country X's citizens have formed resistance groups opposing the new government. During a 24 hour period any resistance group has seven possible courses of action, within a large city in Country X:

1. Attack a checkpoint
2. Attack the police HQ
3. Attack the communication centre
4. Attack the power station
5. Attack the government/ Embassy buildings
6. Attack the railway station
7. Do Nothing

A map of the terrain showing the locations of the potential targets is provided below.

Figure 4: Country X terrain map

2.1 Model Specific scenarios

2.1.1 Bayesian Network

The Bayesian Network is designed to collate and interpret the relevance of information within the processing stage of the intelligence cycle. The aim of the Bayesian Network is to provide a reasonable estimate of the likelihood of each of the enemy courses of action taking place as a result of the information received during the intelligence collection phase. The Bayesian Network follows the probability of an attack by any number of insurgents/ militia.

2.1.2 Influence Diagram

The Influence Diagram scenario is an extension to the Bayesian Network scenario. After the identification of the most likely target (based on the information gathered in the Bayesian Network) the blue troops have been placed on a heightened state of awareness. During a routine patrol, a blue unit has become suspicious of a civilian within their line of sight and must decide which course of action to take: search and arrest, engage fire, watch or ignore. The Influence Diagram provides utilities for each of the different decisions depending on the additional information provided to the blue unit regarding the civilian.

3.0 ANALYSIS AND RESULTS

The qualitative aspect of designing the Bayesian Network and the Influence Diagram relied on the information provided by various sources. The relationships described by the models were, at first, constructed from the judgement of the author supported by the literature review and information gathered through various conversations with Army personnel. The variables used within the models were again from various sources including detailed discussions with three Army officers.

The quantitative formulation of the models proved to be the most difficult task in the modelling and relied on information obtained via the internet, media services, historic literature and, most importantly, the expertise of a number of Army personnel.

3.1 Data gathering

Information regarding the frequency of attacks on different targets was obtained via the media coverage of the post war situation in Iraq; these numbers were used to provide an estimate of the likelihood of a terrorist attack on the different targets given in the scenario description above. Other information obtained via the internet and media coverage relates to the types of weapons used in the attacks, for example, the weapon used in an attack on a police station is mostly likely to be a suicide bomber with a car bomb. The three officers substantiated the relationships and probabilities gathered from the media and internet against their expertise. A number of websites were used to collate numbers of the time and type of attacks and to gather an understanding of the attackers' beliefs and reasons for conducting the attacks.

To help elicit probabilities from the Army personnel, a number of simulations of the above scenario were conducted using the URBAT simulation tool. The players were provided with a simulation information pack containing a detailed scenario description. Using only the scenario description, the players were asked to provide a probability distribution for the suspected targets, via the question "without any additional information, what is the likelihood of the enemy choosing each of the possible courses of action?". The players were then asked to update their beliefs every time a new piece of information was provided, e.g. player x was told 'there is increased activity at the police station'. Given this additional information, player x updated his initial probability distribution of the likely courses of actions. The information supplied to the players, and the order in which it was supplied, varied for each simulation.

3.2 Model descriptions

The modelling of the scenario, as a Bayesian Network or an Influence Diagram, has two aspects: qualitative and quantitative. The qualitative aspect is the representation of the relationships of the information gathered in the intelligence collection phase. With this in mind the first stage in creating the network is to determine the aim of the model. For the Bayesian Network, the aim is to determine the likelihood of the enemy attacking any of the six locations or doing nothing. The second stage in the construction is to determine which information is the most relevant and what the impact this information will have on the aim of the model. The final stage of the model construction is to collate the information together to graphically visualise the relationships between different variables and the aim of the model.

The final design of the Bayesian Network is provided below. Indicators include observations of unusual activity at each of the possible target locations, rumours and signs of enemy reconnaissance in preparation for an attack. Some targets might be at greater risk at certain times of day (e.g. during shift changes) or when certain events are taking place (e.g. elections). The quantitative aspect of a Bayesian Network utilises the obtained data to derive probability tables for each of the nodes within the network; as mentioned in the previous section, data used to populate the probability tables was obtained via open sources, the judgement of the author and the subjective expertise of Army officers.

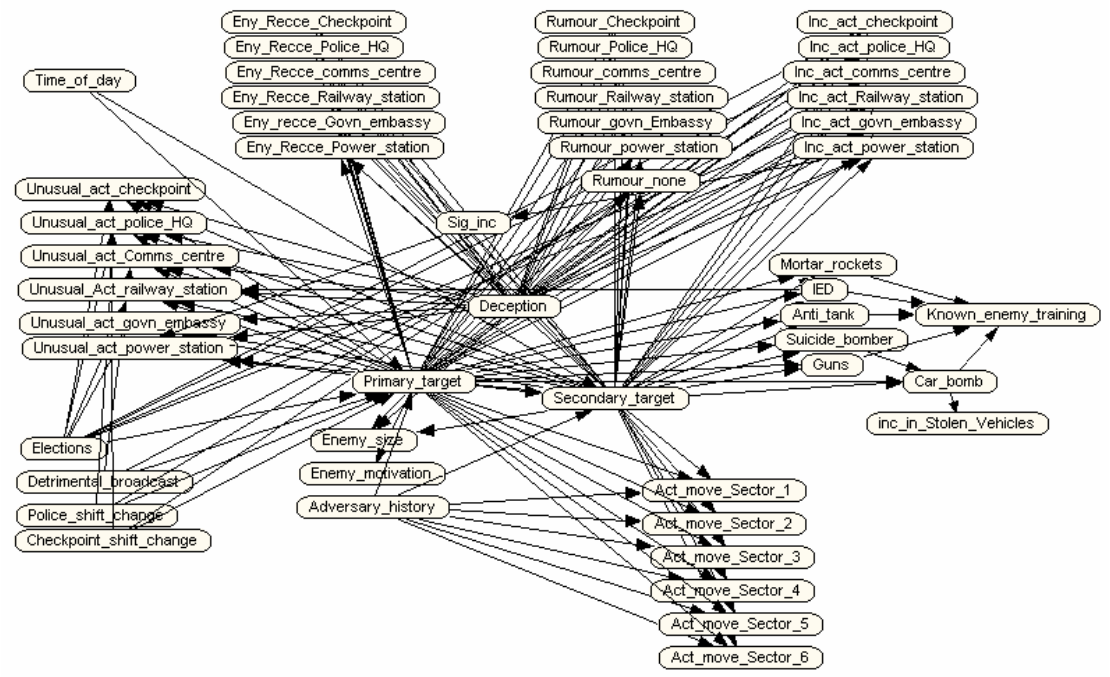

Figure 5: Final Bayesian Network for the Asymmetric Urban Warfare Scenario

Following a similar qualitative construction method to the Bayesian Network, the final version of the Influence Diagram can be found in Figure 6 below. The structure of the Influence Diagram is defined by the inclusion of the decision and utility nodes.

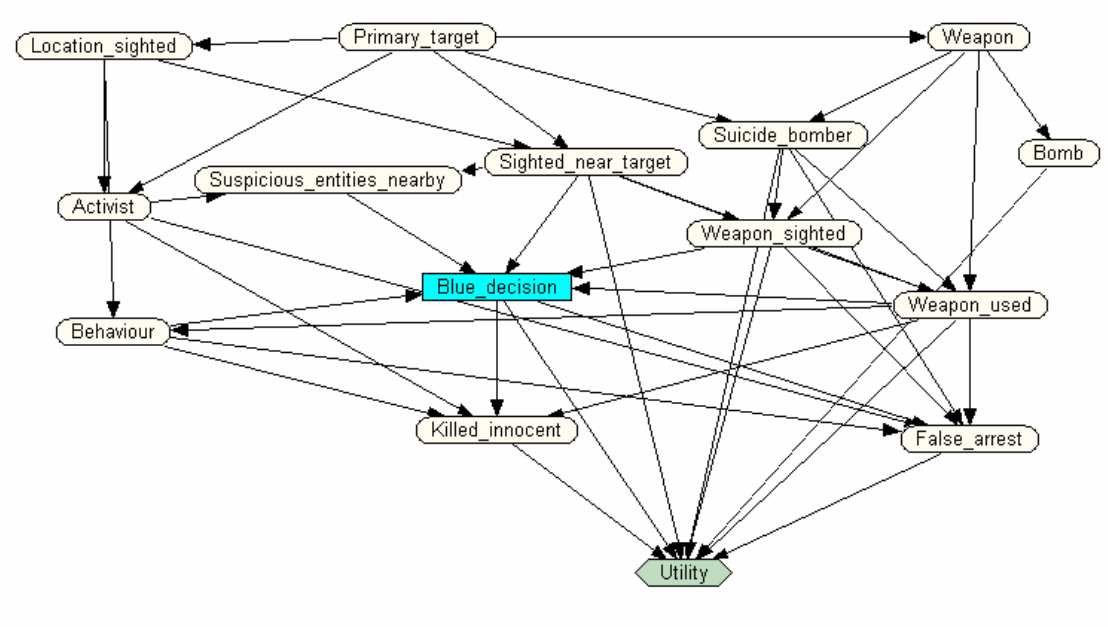

Figure 6: Influence Diagram for the Asymmetric Urban Warfare Scenario

The variables of interest in the Influence Diagram are split into two categories: those known before the decision is made and those influenced by the decision. There are two variables falling into the latter category, measuring the effects of the decision on the likelihood of the blue entity killing or arresting an innocent civilian. The remaining variables are related to the location, weapons and the behaviour of the civilian.

3.3 Sensitivity Analysis

To test the sensitivity and robustness of the models, a number of sensitivity methods were applied to both models. This section provides a description of the methods used.

3.3.1 Notation

Throughout the sensitivity analysis the following notation is used:

Q = the hypothesis variable (i.e. Primary target)

q = a state of the hypothesis variable (e.g. checkpoint)

F = a findings variable (e.g. eny_recce_police_HQ)

f = a state of the findings variable (e.g. true)

e = evidence that an event has occurred

3.3.2 Root Mean Squared

The Root Mean Squared (RMS), [5], is a measure of the standard deviation between p(q) and p(q|f) given a finding at F; this value is calculated per state in the hypothesis variable and a large RMS change represents a greater spread of the probabilities relating to that state. The formula used to determine the RMS change is provided below, (1).

$$\sqrt{\sum_i p(f_i)[p(q \mid f_i) - p(q)]^2} \qquad \textbf{(1)}$$

3.3.3 Variance of the node belief

The variance of the node belief, [5], represents a measure of the deviation from the original hypothesis distribution given a finding on an information variable; a small value represents little sensitivity of the hypothesis node in relation to the finding node. The formula is shown below, (2).

$$\sum_f \sum_q p(f)p(q \mid f)[p(q \mid f) - p(q)]^2 \qquad \textbf{(2)}$$

3.3.4 Entropy

The entropy reduction of a hypothesis variable provides a guide to the worth of the information associated with another node, within a Bayesian Network (e.g. see Jenson [3]). In some cases, entropy reduction provides an ability to prioritise data collection during the intelligence cycle.

The entropy for the hypothesis variable is found using (3), as follows:

$$H(Q) = -\sum_{i=1}^{n} P(q_i) \log_2 P(q_i) \qquad \textbf{(3)}$$

The formula below, (4), calculates the entropy reduction of an information variable against the hypothesis variable. An entropy value of 0 implies the state of a variable is known, i.e. instantiated.

$$H(Q) - H(Q \mid F) = \sum_{j=1}^{m} \; -\left[-\sum_{i=1}^{n} P(q_i \mid f_j) \log_2 P(q_i \mid f_j) \right] \times p(f_j) \qquad \textbf{(4)}$$

3.3.5 Data conflict

Jenson [3] suggests the following measure to indicate any possible conflicts in the data contained within the network. If the resulting value is positive this represents either a potential conflict or a rare case.

$$conf(\{e_1, \ldots, e_m\}) = \log_2 \left(\frac{p(e_1)p(e_2)\ldots p(e_m)}{p(e_1, \ldots, e_m)} \right) \qquad \textbf{(5)}$$

The values for $p(e_1)$ to $p(e_m)$ are the individual marginal probabilities for each of the nodes considered within the conflict calculation. The values for $p(e_1,\ldots,e_m)$ are the joint probabilities of these findings.

To determine if there is a conflict in the data or if in fact it is a rare case we look at a new hypothesis variable that may explain the findings in the conflict. By including the new hypothesis variable, h, (5) becomes

$$conf(\{e_1,...,e_m,h\}) = \log_2\left(\frac{p(e_1)p(e_2)...p(e_m)p(h)}{p(e_1,...,e_m,h)}\right) \quad \textbf{(6)}$$

$$= conf(e) + \log_2 \frac{p(h)}{p(h \mid e)}$$

Therefore, h can explain away the conflict if:

$$\log_2 \frac{p(h \mid e)}{p(h)} \geq conf(e) \quad \textbf{(7)}$$

3.3.6 Value of Information

The value of information associated with a chance variable in an Influence Diagram provides the decision maker with the worth of obtaining more information. This is similar to the entropy functionality in the Bayesian Network sensitivity analysis. While entropy provides information regarding the loss of uncertainty, the value of information provides an indication of the improvement of the quality of the decision.

General formulation

Given a hypothesis variable H, there is a value function, V, attached to the distribution of P(H). The value function usually relates to the maximal utility for a variable, A.

$$V(P(H)) = \max_{a \in A} \sum_{h \in H} U(a,h)P(h) \quad \textbf{(8)}$$

If another variable, T, yields an outcome t, then the value of the new information found by:

$$V(P(H \mid t)) = \max_{a \in A} \sum_{h \in H} U(a,h)P(h \mid t) \quad \textbf{(9)}$$

However, since t is generally not known, the expected value is calculated using:

$$EV(T) = \sum_{t \in T} V(P(H \mid t)) \cdot P(t) \quad \textbf{(10)}$$

The expected benefit, i.e. the value of the information, is the difference between (10) and (8). (8) represents the expected value of the optimal decision with no information provided and (10) represents the expected value given information on T.

3.3.7 Sensitivity to Parameters

The creators of GeNIe [6] have included a capability to test the sensitivity and robustness of an Influence Diagram to different parameters within the network. A decision maker may be uncertain of the distributions of specific variables and would like to know if any change in the distributions effects the

recommended decision. A change in decision for a slight adjustment in a distribution would imply a sensitive network; whilst no changes in the decision will arise from an insensitive network.

Although the changing of a parameter or distribution is a simple task, it is time consuming to conduct a number of changes. GeNIe's sensitivity analysis functionality allows the user to make a number of changes simultaneously, thus reducing the time taken.

4.0 CONCLUSION

A Bayesian network and an Influence diagram have been developed representing scenarios of asymmetric warfare in urban terrain. Bayesian Networks and Influence Diagrams have a number of desirable characteristics. They are flexible in design and can be tailored to numerous different scenarios, using either collected data or expert judgement. They can handle random and deterministic elements in both static and dynamic environments. They are probabilistic in nature and offer a compact, visual representation of the real-world scenario represented.

Bayesian Networks and Influence Diagrams have qualitative and quantitative aspects. The qualitative aspect is the representation of a real-world scenario in a graphical form. The variables of interest are represented by nodes and the relationships represented by arcs (links between various nodes). The quantitative aspect is the use of data (either empirical or judgemental) to derive probability distributions for each of the nodes.

Bayesian Networks may contain hypothesis variables, which are either unobservable or only observable at an unacceptable cost, information variables, which can be observed and mediating variables, which lie between the information and hypothesis variables and are not directly observable but are useful to know.

Influence Diagrams were once mainly used as a compact representation of decision trees. They are now viewed more as an extension to the Bayesian Network, with the addition of decision and utility nodes, to measure the impact of a decision.

All levels of command could be trained to interpret the models without an in-depth knowledge of Bayesian Networks or Influence Diagrams. The relationships described by the models are, for the most part, intuitive and by instantiating various nodes the decision maker can easily build up a good situation awareness of the most likely scenario.

Although effective and easy to understand at all levels, the construction of the models is time consuming and it is impractical to assume analysts will be able to construct a scenario specific model in real time. To overcome this limitation, work by Laskey [7] and others is being directed at developing a number of small models, known as fragments, which can be combined rapidly in different ways to model different situations as they develop.

6.0 REFERENCES

[1] "Proposal Information Package (PIP) – Real-time Adversarial Intelligence and Decision-making (RAID)", DARPA, BAA 04-16, March 2004.
http://dtsn.darpa.mil/ixo/solicitations/raid/file/RAID_BAA_PIP.pdf

[2] John Russell, "Asymmetric Warfare", The Occasional Number 45, "The big issue: command and combat in the information age (a view from Upavon)", Chapter 17, pp 243-265, Edited by David Potts, Strategic and Combat Studies Institute, reprinted by CCRP, March 2002

[3] Finn V. Jensen, "Bayesian Networks and Decision graphs", Springer - Verlag, New York, 2001

[4] Howard, R., and J. Matheson. 1981. Influence diagrams. Pages 721-762 in Howard, R., and J. Matheson (editors). Readings on the principles and applications of decision analysis, Volume II. Strategic Decisions Group, Menlo Park, CA.

[5] Norsys Software Corp, "Sensitivity to findings", personal email correspondence with Jennie Yendall.

[6] GeNIe software for influence diagrams, developed by Decision Systems laboratory, University of Pittsburgh. http://www.sis.pitt.edu/~genie/

[7] K.B. Laskey, "Network Fragments: Representing Knowledge for constructing Probabilistic Models", Department of Systems Engineering and C^3I Center, George Mason University, 1997.