Threat Assessment in Tactical Airborne Environments

X. T. Nguyen

Airborne Mission Systems

Air Operations Division

Defence Science and Technology Organisation

PO Box 1500, Edinburgh, SA 5111, Australia

Email: thong.nguyen@dsto.defence.gov.au

Abstract - *The paper reports the results of a research program on target threat assessment. A threat assessment process will be discussed. There are basically two components in this process: intent assessment and capability assessment. Threat assessment was analysed using Cognitive Work Domain Analysis technique. A model of intent assessment based upon Bayesian Networks will be discussed with its test results.*

Keywords: Threat Assessment, Intent Assessment, Cognitive Work Domain Analysis, Bayesian Networks.

1 Introduction

One of the key factors for success on the battlefield of the future will be the effective use of information. Accurate and timely information is essential, although not all information will be able to be used. In order to counter an enemy's action, its threat must be assessed correctly. The assessment of the threat of adversarial targets is part of an overall assessment of the adversary's military capabilities [1]. Knowing the threat of a target is essential for an operator to prioritise target processing and to choose a suitable tactic to engage the target. The threat of a target is one of the main discriminators for classifying whether it is friend or foe. This task requires an operator to collect large amounts of often incomplete and uncertain information from multiple sources and use it to assess the target's threat. The difficulty of the task is high as the information is often distributed among many operators. Considerable effort is required to gather all isolated pieces of information for the intent assessment task. Under the pressure of time, this task can become very difficult and an operator may lose mental awareness of the current situation.

There is, in fact, no shortage of information. The rapid developments in avionics, communications, and computer technology have produced cockpit and back-end systems which can quickly saturate the aircrew with information. This may lead to a high workload, with the overall situation becoming more complex, more difficult to comprehend, and with less time available for assessing its impact [2]. These circumstances can be mitigated by employing computerised aids which efficiently process and filter out irrelevant

information before concise information is presented to the crew with a view to reducing information overload. Thus, computerised aids are critical in assisting the crew to become aware of real-time dynamic situations within the tactical environment. Furthermore, with the increasing complexity of battle scenarios, more capable on-board and off-board sensors, and the multi-role capability of modern aircraft, the requirement for crew support functions which rapidly evaluate all available target data has become essential [3][4].

The results of research into target threat assessment is represented in this report. A discussion of a process of threat assessment is followed by a Cognitive Work Domain analysis on threat assessment. The analysis of the work domain is needed in order to define any environment constraints and cognitive processes required by the threat assessment task, regardless of whether the threat assessment task is carried out by a machine or by a human operator. The insight from the analysis helped us model and test an intent assessment problem using Bayesian networks. The paper concludes with some remarks.

2 Threat Assessment

The threats to aircraft have been defined as those elements of a man-made environment designed to reduce the ability of an aircraft to perform mission-related functions by inflicting damaging effects, forcing undesirable manoeuvres, or degrading system effectiveness [5].

According to the data fusion model proposed and maintained by the Joint Directors of Laboratories' (JDL) Data Fusion Group, threat assessment involves capability assessment and intent assessment. In other words, the perception of the threat is in proportion to the level of danger it implies [6]. Threat assessment is now absorbed in to the impact assessment of the revised JDL Data Fusion Model [7][8]. For the research reported on here, the former definition of the threat assessment was preferred.

Figure 1 shows a threat assessment process where information from multiple sources is used for both intent and capability assessment. A threat is determined as a

Figure 1: Threat assessment process

combination of its intent and capability. Threats are further prioritised based on a set of mission-related criteria.

An essential part of this process is a set of knowledge libraries required for the task. Knowledge libraries exist in the form of the experience of operators or in the form of codified digital knowledge bases in machines.

2.1 Capability Assessment

The capability of a target depends on its platform capability whether, for example, it can manoeuvre fast or is a stealth platform and on the weapons it carries for the mission. Basically, the target must be identified first; then its capability can be inferred as shown in the bottom path of Figure 1.

The platform capability refers to its ability to perform its basic firing/launch functions and other inherent capability such as threat mobility, locational adaptability, and weather capability. The firing and launch capabilities include slew rate, rate of firing, and intercept envelope [5].

The weapon capability is also a complex subject that requires a thorough analysis. It depends on weapon characteristics such as types, warhead descriptor such as armour-piercing or shaped charge, damage mechanism such as blast or fragments, and threat lethality. The threat lethality refers to those factors related to the fire control, trajectory, and terminal effects of the threat in the process of directing, projecting, and activating threat mechanisms designed to cause damage to a target [5].

2.2 Intent Assessment

2.2.1 Meanings of Target Intent

Intent refers to the assumed future behaviour of a target. Knowing the intent of a target is essential for an operator to prioritise the processing of a target and to choose suitable tactics and appropriate weapons to engage the target. Target

intent is one of the main discriminators for classifying whether a target is friend or foe since a particular type of aircraft may be in service in both forces. For example, identification of an aircraft as a MiG-21 or F-5 in the Middle East does not automatically indicate whether the target is friend or foe [9]. Intent assessment is a critical step in a process of determining a target's lethality.

It is important to point out the term “intent” is understood in many different ways by different people. From the operator's point of view, there is more concern about whether a target is a friend, foe, or neutral. In this research, the scope of target intent is broadened to include missions that target is intended to achieve. It is defined as a particular mission that an adversary intends to complete with a particular platform.

2.2.2 Intent Assessment Task

Target intent cannot often be observed directly. What can be observed are signs that the enemy is engaged in particular actions or behaviour. Therefore, to infer the intent of a target, operators get as many clues as possible from different information sources such as radar, identification friend or foe (IFF) interrogation, intelligence, visual inspection, etc. Operators generally carry out a number of sequential activities within the overall task. Consider the activities of an operator from “initial detection” to “intent assessment” of a single target. The activities include recognition that the target exists, assessment of the environment in which the target is operating, and assessment of the target behaviour within the environment, leading to an assumption about its intentions. A conclusion about the intent of a target may lead to actions of further investigation or to intercepting and neutralising the target.

Context evaluation involves the establishment of whether or not the target is coordinating with other targets. For example, fighters usually escort strikers into an area. Often large numbers of fighters are sent in from one axis to distract friendly forces from a more threatening activity on a

completely different axis. So if there appear to be related activities, the track would be assessed with that context in mind.

Cue analysis starts with a check of routine things such as IFF squawks¹, target's location and speed, a check if any flight plan which has been submitted matches the track, and a check whether the target is operating on a flight route or in a known region of a particular activity.

Sometimes, available information about a target is not sufficient for an operator to assess the state of a target, so direct voice communication may be established with the target. If this procedure does not produce any results, an intercept by a fighter for the purposes of identification may be considered.

It is also possible that the evidence at hand is conflicting. For example, confusion about the identity of a target may happen because of garbling. This kind of confliction is rare however. More commonly, operators get a combination of clues that suggest several possible intentions and the difficulty lies in narrowing down the intent to the one most likely to be correct.

3 Understanding Threat Assessment with the Ecological Approach

3.1 Ecological Approach

Any computer-based system for human work is based on a certain set of assumptions about the work that it is intended to support. Rather than making those assumptions implicitly, the design of information systems should be based upon an explicit analysis of work [10]. A thorough analysis of work helps us to understand work demands. The work demands come from two major sources, namely the physical environment and cognitive constraints. Physical environment constraints originate from the context in which operators are working. They define what the operator cannot do. The physical environment constraints, also known as behaviour-shaping constraints, specify what should not be done, rather than what should be done. In contrast, cognitive constraints are work demands governed by human cognitive systems.

Another important aspect of military work systems is that they have to function in, and adapt to, a dynamic environment. When the environment changes, unanticipated events which can occur may pose a particularly difficult challenge to the system. Rather than automating systems to replace the human operator in such circumstances, a computer-based tool should be created to help operators adapt to unexpected and changing demands in the

environment. It is, therefore, of paramount importance to explicitly identify all possible environment constraints. There are different ways to conduct a work analysis, however, the *Ecological Approach* suggests that work analysis should begin with, and be driven by, an explicit analysis of the constraints that the environment imposes on a resulting action [10].

A particular framework that was used is called Cognitive Work Analysis. Cognitive Work Analysis comprises five phases of identifying behaviour shaping constraints in a complex system, each phase related to a different aspect of the work done in the system. The phases are work domain analysis, control tasks, work strategies, social organisation and cooperation, and competencies. Further detail can be found in [10].

3.2 Basic Description of Work Domain Analysis

Work domain analysis (WDA) includes modelling the physical and objective properties of a problem domain in which activities take place. Therefore, the analysis of a work domain is independent of any actions. There are typically three dimensions in WDA which are: abstraction hierarchy, decomposition, and sub-domain.

In the abstraction hierarchy, a work domain is described using levels of abstraction ranging from the highest level of abstraction to the most concrete level of physical abstraction. The connections between the abstract levels are structural means-end relations. In general, higher levels of the abstraction hierarchy represent the work domain in terms of its functional purposes, whereas lower levels of abstraction represent the work domain in terms of its physical properties. Thus, the abstraction hierarchy is a structural map which describes how an outcome is achieved by employing some of the physical forms of abstraction as illustrated, for example, as shown in Figure 2.

The decomposition describes a part-whole hierarchy with different levels of resolution, ranging from the coarsest level of the total system to the finest level of the system components. The decomposition hierarchy has been used like it would be used in the systems engineering discipline for the purpose of managing the complexity of the systems.

No work system exists in isolation. It has to interact with the environment to receive inputs that affect the behaviour of the work system. The environment within which a work system is located can be as complex as a work domain itself. On the sub-domain axis, a work domain can be broken down into different sub-domains that couple one with another [11][12].

In essence, the domain representation is a map that shows all the functional resources of the work in terms of

1. *Squawk* is a term used to describe the radio transmission of an IFF code.

Figure 2: Work domain analysis of target threat.

categories for which the functional capabilities, required knowledge, and limitations can be identified with reference to the various objectives they serve. In other words, the abstraction hierarchy can be used to identify the set of goal-relevant constraints governing the operation of the controlled system [10].

Work domain analysis is also applied to the development of decision support systems in which a work domain representation is used to form the knowledge base upon which the reasoning mechanisms will act [13] [14]. This is also the main application of WDA in our research. With the ecological approach in mind, we first looked at a sub-domain of target intent from an environment perspective and then at a sub-domain of intent assessment from a defence system perspective.

3.3 Sub-Domain 1: Target Threat from the environment and an offensive system

On a battle field, targets are deployed according to their missions. Therefore, the functional purpose of the target intent abstraction hierarchy is mission completion. To achieve the intended mission a target's survivability and capability are normally important. One of the objectives of an adversary is to maximise its chances of survival and to make its intent unpredictable to its potential battle victims. This property of hiding intent can also be one of the properties of an adversary's capability. The level below the overall function, shown in the centre of Figure 2, is the purpose-related functions which include location, capability, tactics, manoeuvrability, as well as opportunities or limitations provided by a changing environment. A target will use as many of these purpose-related functions as possible to obtain its overall function. At the physical level,

targets are objects in their own right, but so too are political tension and environmental conditions. Figure 2 shows the work domain analysis of target intent. It is worth noting that this analysis is limited to the reference of target intent which is one of many general functions of the whole mission. Therefore, the analysis is not complete for any other purpose.

3.4 Sub-Domain 2: Threat Assessment from a defensive system

An air asset will be deployed to achieve a certain purpose. In broad terms, the aircraft is required to complete its intended mission whether it be reconnaissance, surveillance, strike, or something else. A strike aircraft needs to be adequately equipped to execute its intended mission, but also needs to be adequately equipped to survive the mission. The emphasis on strike ability and survivability will be different in a defensive aircraft. The difference between a defensive and offensive system are clearer at the level of overall functions in the abstraction hierarchy. One of primary overall functions of a defensive system is its ability to recognise and evaluate threats accurately and early. It uses intelligence, tactical information, and track information as well as allowable procedures from the rules of engagement to obtain its overall function. At the lowest level, physical objects include operators, communication channels, on-board sensors, rules of engagement, threat libraries, mission data bases, and hardware and software facilities within the mission system. Figure 3 shows the work domain analysis of intent assessment for a defensive system. It is worth noting that this analysis is limited to the reference of intent assessment which is only one of many overall functions of a whole mission. A detailed work domain analysis related to the AEW&C platform can be found in [15].

Figure 3: Work domain analysis of intent assessment.

4 Modelling Intent Assessment

4.1 Computational Technique

4.1.1 Rationale

One of the challenges we faced was to select a computational technique which was capable of processing different types of uncertain, incomplete, and conflicting information. Uncertainty arises when we do not know the true state of the world, of the consequences of our actions, or of unforeseen interactions between the two. Information incompleteness occurs when we receive a sub-set of information describing properties of an object. Information conflict occurs when we have a framing problem either in the time or in the spatial dimension [16][17].

Proper management of these properties of information is essential to the modelling of the selected subset of intent assessment problems. A modelling concept based on problem characteristics allows synergistic matching of the Artificial Intelligence uncertainty management technique. The concept should define: (1) how to organise the knowledge for solving the intent estimation problem, (2) how to represent a state of belief in any hypotheses drawn from the current scenario, (3) how to update the state of belief given the evidence, and (4) how to make decisions given the current state of belief [9][18].

There are several different artificial intelligence technologies which are suitable for handling uncertain information [17]. However, probabilistic reasoning techniques seem to satisfy all of the aforementioned requirements and were discussed at the concept level in

relation to assessing enemy intentions and situations, and resolving conflict [19][20][3].

4.1.2 Bayesian Networks

A Bayesian network is a directed acyclic graph which represents the probabilistic dependencies between a set of random variables. Each node which represents a random variable in the Bayesian network defines alternative propositions. The propositions must be mutually exclusive and collectively exhaustive for probabilistic formalism. Collectively exhaustive means that all possibilities are represented. The directed connections between nodes represent the conditional probability (or likelihood) of inferring the existence of one node (being pointed to) given the existence of another node. Each node can have multiple inputs, that is many parents. Each node in the network stores its probability distribution given its direct parents and any associated evidence.

Bayesian networks provide a formal method for reasoning about partial beliefs under conditions of uncertainty. In this method, propositions are given numerical parameters signifying the degree of belief accorded them from a given set of knowledge. The parameters are combined and manipulated according to the rules of probability theory. In the context of Bayesian statistics, the probability is interpreted as the degree of belief.

The essential principle of Bayesian networks lies in the classical inversion formula:

$$P(H/e) = \frac{P(e/H) \times P(H)}{P(e)}, \quad (\text{EQ } 1)$$

Figure 4: Implemented Bayesian network for assessing target intent.

which states that the belief we accord a hypothesis H upon obtaining evidence e can be computed by multiplying our previous belief $P(H)$ by the likelihood $P(e/H)$ that e will occur if H is true [21][22]. $P(H/e)$ is called the posterior probability and $P(H)$ is the prior probability. This formula allows the network to update the states of its beliefs once new evidence enters the network.

The Bayesian network can handle available expert knowledge as well as data. The expert knowledge is translated into some prior probability of some of the nodes of the network and into conditional probabilities of the connections between the nodes.

4.2 Assumptions

In this version, four assumptions were made.

- Only tangible evidence is considered. Typically, the evidence includes altitude profile, speed, heading, location, IFF squawk status, air-to-surface or air-to-air radar status, and possible platform types. Other intangible evidence such as environmental and economical factors are not considered. While environmental factors are not considered in this model, it does not mean that these intangible factors are not important.
- A political climate of tension is assumed, in which targets may exhibit complex behaviour. Political tension means that an adversary is more likely to be deployed on a hostile mission.

- A defensive scenario is considered in this study.
- Only four possible missions which are mutually exclusive, and assumed to be exhaustive are considered. In reality, there are many other possible missions.

4.3 Structure

The hypothesis variable is a target's mission and its information variables are typically altitude profile, speed, heading, location, IFF squawk status, air-to-surface (AS) or air-to-air (AA) radar status, and possible platform types. The variables and their possible values are summarised in Table 1.

The target's mission has a direct causal impact on IFF squawking, location, heading, AS and AA radar status, altitude profile, and possible platform types. In other words, the behaviour of a target may vary according to its mission. Furthermore, the altitude profile and platform type also have a direct causal impact on platform's speed and status of its AS and AA radar. Using the Hugin modelling software, a Bayesian network models this mission estimation problem as shown in Figure 4.

4.4 Assignment of Degrees of Beliefs

An assignment of prior probabilities to nodes and conditional probabilities to links is a critical step in the process of constructing a Bayesian network. There are

different ways to acquire these probabilities [22]. In this study, probability is expressed as a measure of personal belief. That is, the probability of the occurrence of an event is a measure of a person's degree of belief in the occurrence of the event, given the information available to that person. According to this perspective, probabilities are properties of the state of knowledge of an individual rather than properties of a sequence of events (e.g., tosses of a fair coin) [23]. In fact, the conditional and prior probabilities are provided by a domain expert in this research.

Table 1. Variables and their possible values used in the model of target mission estimation.

Variable	Possible Values
Target mission	Strike Reconnaissance Troop lodgement Fighter escort
Altitude profile	High to low High to high Medium to low
Air to air radar	On Off
Heading	Ingress Egress
Location	Outside Controlled Airspace (OCTA) Flight Route Military Zone Sovereign Airspace
Platform type	Bomber Fighter Transport
Air to surface radar	On Off
IFF squawking	Yes No

4.5 Evaluation

The purpose of testing this Bayesian network is to examine the accuracy in deriving "intent". Accuracy is the degree to which this network can draw a conclusion that is consistent with one reasoned by an operator given the same information. The network was tested with 27 different cases. The test results obtained by this model are plotted against the estimate given by an operator viewing the same data as shown in Figure 5. The machine predictions are reasonably consistent with those obtained from a human operator, although some inconsistencies were evident. There are at least two factors that contribute to these differences. First, there may be errors in the process of converting human beliefs into numerical values. Second, humans are usually very good at handling uncertainty and abstraction but are poor at generating numbers from their beliefs. Therefore, the

human predictions used as benchmarks are also subjective as are the accuracies themselves.

5 Conclusion

A research program on target threat assessment was presented. Threat assessment is a process that comprises of two components: capability and intent assessment. Each component presents its own complexity and challenges to researchers.

The application of work domain analysis from the ecological point of view was proved useful. WDA helps capture different coupling parts of a work system which can be used as focal points to identify constraints which are either environmental or cognitive. In fact, the work domain analyses were helpful when information related to the task of intent assessment was identified.

The application of Bayesian networks in assessing target intent from uncertain and incomplete evidence was proved useful. There is some objection on the processing of probabilities on the grounds that there is no evidence that human beings do not employ the probability theory in their reasoning process [24]. It is a debatable issue. However, it is believed that an assistant, whether it is a person or a machine, should be judged on the quality of the performance rather than the technique employed. In this particular research, accuracy is one of the qualities to be employed for assessing the performance of the model.

However, further work is needed in the area of learning in order to compensate for some mismatches in the process of constructing the knowledge base for the model. It would also be desirable to model the whole problem in order to increase the usefulness of the model. Work on capability assessment and threat prioritisation is also needed to complete the research program.

6 References

- [1] Keightley, H. B. (1996), "Intelligence Support for Air Operation," Royal Australian Air Force, Air Power Studies Centre, Canberra.
- [2] Endsley, M. R. (1993), "A Survey of Situation Awareness Requirements In Air-to-Air Combat Fighters," *Int Jour. Aviation Psychology*, 3, 157-168.
- [3] Pew, W. R. & Mavor, A. S. (Eds) (1998), "Situation Awareness," Ch 7 in *Modelling Human and Organisational Behavior*, National Academy Press.
- [4] Lovesey, E. J. and Davis, R. I. (1991), "Integrating Machine Intelligence into the Cockpit to Aid the Pilot," AGARD Proc. 499, Lisbon.
- [5] Ball, R. E. (1985), "The Fundamentals of Aircraft Combat Survivability Analysis and Design," AIAA, New York.
- [6] Waltz, E. and Llinas, J. (1990), "Multisensor Data Fusion," Artech House, Norwood, MA.

Figure 5: Estimates obtained from the model are shown on a blue o-dashed curve and those from an operator are shown on a red *-solid curve.

- [7] Steinberg, A. N., Bowman, C. L., and White, F. E. (1998), "Revisions to the JDL Data Fusion Model," Proc. Joint NATO/IRIS Conf. Quebec, Canada.
- [8] Roy, J., Paradis, S., and Allouche, A. (2002), "Threat Evaluation for Impact Assessment in Situation Analysis Systems," SPIE Proc. Signal Proc. Sensor Fusion Target Recog. XI, **4729**.
- [9] Barrette, A. K., Jamerson, L. C., and Rogers, R. A. (1989), "Artificial Intelligence Techniques Applied to the Non-Cooperative (NCID) Identification Problem," Proc. AIAA Computers in Aerospace VII.
- [10] Vincente, K. J. (1999) "Cognitive Work Analysis: Towards Safe, Productive, and Healthy Computer-based Work" Lawrence Erlbaum & Associates, Inc.
- [11] Sanderson, P. M. and Watson, M. (1999), "Cognitive engineering modelling of C2 and Commander Decision Making: A Cognitive Work Analysis Approach," DSTO Contract Report, Swinburn Human-Computer Interaction Lab., School of Information Technology, Swinburn University of Technology, Australia
- [12] Watson, M. and Sanderson, P. M. (1998), "Work Domain Analysis for the Evaluation of Human Interaction with Anaesthesia Alarm Systems," Proc. Australian Computer-Human Interaction OzCHI'98, Adelaide, 228-235.
- [13] Sharp, T. D. (1997), "Progress towards a Development Methodology for Decision Support Systems for Use in Time-Critical, Highly Uncertain, and Complex Environment," PhD Dissertation, Dept. Electrical and Computer Engineering, University of Cincinnati.
- [14] Bisantz, A. M. and Vincente, K. J. (1994), "Making the Abstraction Hierarchy Concrete," Int. J. Human-Computer Studies, **40**, 83-117.
- [15] Sanderson, P. M., Naikar, N., and Bryan, T. (1999), "Cognitive Engineering Evaluation of Human-System Integration in the ADF's Proposed AEW&C System," Final Report.
- [16] Post, S. and Sage, A. P. (1990), "An Overview of Automated Reasoning," IEEE Tran. Syst. Man Cybern., **20** (1), 202-224.
- [17] Krause, P. and Clard, D. (1993), "Representing Uncertain Knowledge", Kluwer Academic Publishers, London.
- [18] Fox, J. (1996), "Expert Systems and Theories of Knowledge," In M. A. Boden (Ed.), Artificial Intelligence, 157-182, Academic Press.
- [19] Laskey, K. B., Stanford, S., and Stibio, B. (1994), "Probabilistic Reasoning for Assessment of Enemy Intentions," Tech. Report, GMU-PUB-94-25, George Mason University, USA.
- [20] Yang, L. C. and Kuchar, J. K. (1998), "Using Intent Information in Probabilistic Conflict Analysis," Proc. AIAA Guidance, Navigation, Control Conf., 797-806, Boston, USA.
- [21] Pearl, J. (1988), "Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference," CA: Morgan Kaufmann.
- [22] Jensen, F. V. (1996), "An Introduction to Bayesian Networks," UCL Press.
- [23] E. J. Horvitz, J. S. Breese, and M. Henrion (1988), "Decision Theory in Expert Systems and Artificial Intelligence," Int. Journal Approximate Reasoning, **2**, 247-302.
- [24] Solso, R. L. (1998), "Cognitive Psychology," Allyn & Bacon.