

## Old papers: Intelligence Analysis for New Forms of Conflict

Another old friend from back in the days before old age and disillusionment (aka 1997). I don't do this sort of thing any more, but I'd really like to think about how it could be applied to more civilian activities.

### Abstract

As the volumes of information available from modern sensors and sources increases, processing all available intelligence data has become too complex and time consuming for intelligence analysts. There is a need to assess how technology can and should be used to assist them, and for a clear view of the issues raised by the data and processing methods available. This paper discusses automated intelligence analysis, its impact and its role in modern conflict analysis.

### 1. Intelligence Analysis

Before we can automate intelligence analysis, we need to know what it does. The output of intelligence analysis (by human or machine) is intelligence: information that is pertinent to the current area of interest of a commander or policy maker, in a form that he can use to improve his position relative to another, usually opposing, commander. The other output of intelligence work is counterintelligence, misleading information supplied to the opposing commander (well-managed counterintelligence should also improve the commander's position relative to his opponent). Simplistically, intelligence analysis is the collection and painstaking sifting of information to gain insight into and build a model of part of the world (a battlefield, country or other topic of interest ) that is relevant to a commander's needs and actions; intelligence is a set of beliefs about the state of that world and the actions and intents of another party within it.

#### 1.1 The need for intelligence analysis

To make decisions commanders need accurate and timely information based on as much relevant data as possible. The importance of good intelligence cannot be overstated; in a military situation, a commander is effectively blind without the battlefield awareness gained from intelligence. The view that a commander has of a situation depends on information pools and flows, as shown in table 1 and figure 1, where each OODA loop consists of Observe (using sensors and knowledge sources ), Orient (intelligence analysis ), Decide (command decision making using both learnt doctrine and individual style) and Act (move, oppose or contain a move). Note that in modern conflict, there may be 0, 1, or several other forces' OODA loops in a commanders viewpoint, and that too little may be known about their structures, doctrine or equipment for conventional (orbit and doctrine-based) analysis. Given that each commander in a battle has their own view of it, it becomes important for a friendly commander's battlefield awareness to be dominant (better than that of the opposition). Other considerations for intelligence analysts are that it also isn't enough for analysts to provide a commander with information if it deluges him (the commander is given too

much information to understand in the time he has available), changes too rapidly or he can 't trust it.

## 1.2 Why automate intelligence analysis?

Modern conflict focuses on the observation and control of other forces, where command and analysis relies on timely and accurate intelligence, Automated decision -making (currently at the research stage) will need fast, accurate sources of information to succeed. There is little argument about the need for intelligence in modern conflict, but before we consider automating intelligence processing, we need to decide whether, given the small scale uncertainty and high complexity of modern low intensity conflicts (Keegan's guerilla-style real war), and operations other than war, it is a worthwhile thing to do. There are few metrics available for intelligence analysis: for human analysts there are the principles of intelligence, and intelligence processing systems are generally judged on the speed of their message processing and accuracy of their outputs (although accuracy is usually judged using a model of the world's ground truth). These can be summarised by saying that intelligence processing should provide the commander with the most honest view possible of his area of interest, given the data, resources and time available.

### Table 1 One commander's information

- \* each force: World view including intelligence weaknesses, capabilities, intent, doctrine, deception, counterintelligence, available supplies and equipment, psychology, morale, coordination, allegiance,
- \* environment: terrain, possible changes (for example weather), human features (for example bridges and cities)
- \* situation: current state of play (situation and events), possible moves and events

Intelligence processing is a natural process for humans, but they have limits: when the input data size becomes too large to process within the time constraints given, or too complex (uncertain) to think clearly about, then automation of some of the processing must be considered. Given the increasing volume and complexity of information available from modern sensors, lower-level processing and open sources, it will soon be impossible (especially in a tactical situation) for analysts to process all of it efficiently and on time, and time now to start thinking about how automation can help. The second argument for automating intelligence processing concerns the advantages (mainly processing speed and uncertainty handling) that a reasonable intelligence processing system would give a commander. Concerns about the conflict superiority that technology gives are not new (indeed, they date at least from when the first arrow was made), but the emphasis has changed; recent warfare has moved from the production of larger, more efficient weapons to the observation and control of other forces (although this idea dates to Sun Tsu's predecessors). This is reflected in the focus of current technology / research, at the Orient (intelligence processing) and Decide (decision making) stages in figure 1 (the progress of defence automation, as measured on the OODA loop). It is perhaps preferable to understand or possess intelligence processing systems than to fight a force that is better prepared by using them.

## 2. Models for automating intelligence analysis

The cognitive theory of intelligence analysis has been well studied. Not surprisingly, the intelligence cycle has much in common with models of human perception and processing. These are useful starting points in defining what is needed in an intelligence processing system. We learn that intelligence models are incomplete (we can never model the entire world), disruptible (models will always be vulnerable to external influences and counterintelligence), limited (models will always be limited by sensor capabilities), uncertain (input information and processing are usually uncertain) and continuously changing (models must deal with stale data and changes over time).

Requirements for future intelligence processing systems include rigorously handling uncertainty, partial knowledge (of inputs, area, opponent behaviour, training and equipment), detecting and cleanly retracting misleading information (including counterintelligence), giving credible and understandable explanation of reasoning; handling data that changes over time and including quantitative sensor -derived data in a symbolic reasoning framework. How much the computer should do, and how much should be left for the analyst is also an interesting problem. The analysis of and attempt to automate 'judgement' is a necessary step for the automation of low-level command decisions, but the change from assisting analysts to automated intelligence processing will redefine the operating procedures of military staff, and is expected to meet opposition. Since intelligence must be timely to be useful, the control of reasoning in these models must also be addressed : for example, since the creation of intelligence models is cyclic (as more intelligence is generated, so the gaps in the commander's knowledge are pointed out, and more intelligence gathering is needed), when to stop processing and where to focus processing attention may be issues.

Decisions to be made include whether to distribute processing, and the acceptability of anytime algorithms (these output timely but less accurate information). To be useful, information must also be relevant to its user. Relevance is difficult to define; attempts to model it include user modelling and user profiling, and these should be allowed for in models if possible. Both the intelligence cycle and high-level data fusion models have been considered as a basis for intelligence processing models. These are not the only models that may be appropriate ; the design of generic intelligence models and processing should, as far as possible, incorporate techniques from contributing areas like cognitive psychology (mental models), detective work (psychological profiling), data mining (background information processing and user profiles) and data fusion (situation assessment ).

### 2.1 High-level data fusion

Data fusion is the combination of separate views of the world (from different information sources, times or sensors bandwidths) into a big picture of the world. Data fusion can occur at different levels of processing, from combining sensor outputs (low level) to combining processed information (high level). Intelligence processing, in its combination of information from different sources, is equivalent to and can gain from high-level (and also low-level) data fusion techniques.

## 2.2 The intelligence cycle

The Intelligence Cycle describes intelligence processing in stages. Three models are considered here : the UK and US models (which have different names for essentially the same stages), and Trafton's model which adds an extra stage (utilization) to reflect use of the intelligence. The UK model with direction and utilisation stages added (as shown in figure 2), will be used in the rest of this section. The intelligence cycle isn't just a description of the processes of intelligence, it also shows the flow of information within intelligence analysis, from commander to intelligence analysts and back. Within the cycle there are subcycles, the most important of which is the redirection of sensors, data collection to cover areas of ignorance found during processing, The rest of this section describes automation of each part of the intelligence cycle.

### 2.3 Planning, Direction and Collection, deciding what intelligence to collect

Information that analysts use to produce intelligence includes sensor data and intelligence reports, but there are other less obvious inputs : the information that a commander has requested ,both now and in the past, stored knowledge about the area of interest, and knowledge of opponents resources, training and expected behaviour. Input information is usually uncertain and often untrustworthy. Intelligence sources are classified into human, image, signals and measurement intelligence, the inputs from which are often labelled with uncertainties (source and information credibility for human intelligence, sensor errors for other categories of data). Since there is often a larger requirement for intelligence data than collection agencies can meet, there is scope for automating collection management with a constraint satisfaction algorithm, reasoning system using the priority and cost of data as inputs (Currently available tools include the JCMT system).

### 2.4 Collation and Analysis, processing the input information

Intelligence processing covers the stages of the intelligence cycle where intelligence is created from information. Processing by analysts is broken down into collation (sorting input data into groups, for example by units or subject),and analysis (making sense of the data and producing the big picture from it). Analysis is sometimes broken down into evaluation, analysis, integration and interpretation . Overall, intelligence processing uses input information to update knowledge about the situation, and create relevant intelligence reports. Intelligence processing doesn't have to be very sophisticated to make a difference to an overworked analyst ; typical intelligence processing requirements are classification and matching reports to units, both of which are within the capabilities of current systems (although there is always some expected error). A good intelligence processing system should be capable of at least these two functions, with room for extension to techniques like recognising counterintelligence, behaviour and intent as research progresses. Intelligence processing is a large part of the reasoning in an intelligence analysis system, and has been given a separate (later) section in this paper.

### 2.5 Dissemination and utilisation, getting intelligence to the user

Intelligence is no use if it doesn't get to the user on time and in a comprehensible, credible form : dissemination is essentially an attempt to adjust the user's mental models of the situation - something which will not happen if the user does not trust the system. Utilisation is a catch-all term for using the data ; any actions taken by the user will affect the state of the real world and may change the commander,s intelligence needs, restarting the intelligence cycle (at the collection stage).

Automating intelligence processing will change the style and types of output available from it. Rigorously handling uncertainty in inputs and processing will improve the accuracy of intelligence processing outputs, but will also give the system designer a difficult choice between providing definite but inaccurate information to the user (this approach is preferred in, for example [10]) and more accurate but possibly confusing information (for example "T123 is a tank with 90 percent accuracy), or a set of possible explanations for the current data.

### 3 Automating Intelligence Proccesing

Table 3 shows some of the problems and issues in processing intelligence data. The most pressing of these (uncertainty handling) is discussed further in [4].

#### 3.1 Processing frameworks

Frameworks in existing intelligence processing systems include assumption-based maintenance systems, blackboards and graphical belief networks. Of these, belief networks seem most promising as a generic intelligence processing framework, since they can be used to combine uncertain sensor-derived data and knowledge within a probabilistic framework, and have a body of theory behind them that includes sensitivity analysis. The use of belief networks in intelligence processing is discussed in a separate paper; recommendations from it include further research into processing frameworks that includes study of :

- \* Focus of processing attention
- \* Handling of time-varying information
- \* Retraction of information and its ,traces, within the system
- \* Explanation of reasoning, including extraction of alternative explanations
- \* Multiple viewpoints and values
- \* Recognising and analysing group behaviour
- \* User profiling

#### Table 3 Problems for intelligence processing

- \* Input: multiple reports about the same event,object, information incest ,repeated and single,source reports, untrustworthy information, its removal and effects, varying credibility of information
- \* Representation: mixture of text,based reports and sensor data, several possible explanations for data, handling large numbers of parameters
- \* Speed: increasing amounts of complex information,data need for accurate, timely information

combinatorial explosion

\* Interface: credible and understandable explanation of reasoning, human inspection of data and intervention in reasoning

\* Time: data that becomes irrelevant , deciding and removing it data and situations that change over time.

More than one framework could be used to split processing into essential and background work. This would provide opportunities for analysis of the patterns and flow of intelligence data, including dominant routes, behaviour and counterintelligence.

### 3.2 Existing intelligence processing systems

System designs and studies of how to automate Intelligence Processing are increasing in response to the need to take some pressure off the users and analysts. Although systems that handle intelligence data exist, some (for example GIFT, AUSTACCS) assist users to access information and don't attempt processing; many (for example ASAS, DELOS) do not process it beyond the correlation (sorting data into groups) stage of the intelligence cycle, and most are vulnerable to uncertainty in their inputs and missing data in their knowledge of tactics and equipment. Systems that attempt full intelligence processing (for example HiBurst, IMSA, TALON and Quarterback) are usually based on Artificial Intelligence methods which include assumption-based truth maintenance systems, argumentation and expert systems augmented with fuzzy logic. Although probabilistic networks seem a promising base representation for intelligence processing, research on intelligence fusion using probabilistic networks appears to be confined to teams at the UK Defence Research Agency, George Mason University and some US commercial sites.

### 3.3 Using Data Mining as a testbed for Intelligence Processing

There is a vast amount of electronic data even in a single company. Most of it is distributed across several systems /formats, and is useful but inaccessible. Data Mining is the process of extracting implicit and relevant information from data sources, which are usually databases, but can be open sources ,e,g, the internet. Data Mining gives us the opportunity to test intelligence fusion algorithms using open source information as input.

## 4 Automating counterintelligence

As counter-terrorism and infiltration units have discovered, getting inside the opponent's OODA loop is more subtle than destroying communication links : his information can be manipulated to our commander's advantage. We can view his Observe process using stealth and EW technology : we can disrupt it using deception. Counterintelligence also affects the Orient and Decide processes, both by data deluge of processing resources and the creation of uncertainty in an opposing commander's mind. The creation of models of an enemy commander from his known doctrine and reactions also allow us to anticipate his moves rather than just react to them - it also

makes the targeting of counterintelligence (for instance, in information warfare) possible. This augments the current countermoves of defending against enemy actions (e.g. using air and ballistic missile defences). As conflict can be viewed as an interacting series of these pairs of OODA loops, this is also a useful starting point for the automation of low-level command decisions.

## 5 Conclusions

Intelligence processing creates a belief in the state of a world (ie a battlefield) from uncertain and often untrustworthy information together with inputs received from sensors. This is a natural process for humans, but they have limits : when the input data size becomes too large to process within the time constraints given, or too complex (uncertain) to think clearly about, then automation of some of the processing must be considered. This paper outlines issues to be considered in designing the next generation of UK intelligence analysis systems. Future systems should allow analysts to concentrate on high-level analysis rather than clerical operations like duplication elimination. Automated intelligence techniques and systems are being designed in response to this need. Most of them assist analysts by providing better information retrieval and handling tools. The automated processing of intelligence is beginning to be addressed, but lacks a mathematically sound representation ; techniques based on data mining, cognitive psychology and graphical networks are promising, but need further research effort. This work also unites sensor-based data fusion systems with knowledge-based intelligence processing and decision support. Possibilities arising from using a complete and efficient representation include the ability to use most of the information available to a system, the analysis of patterns of behaviour and the generation/ recognition of counterintelligence data.

## Bibliography

1. Nato Intelligence NATO report AINTP
2. Canamero D Modeling plan recognition for decision support European Knowledge Acquisition Workshop
3. Companion M A and Corso G M and Kass S J Situational awareness an analysis and preliminary model of the cognitive process Technical report IST TR University of Central Florida
4. Farmer S J Uncertainty handling for military intelligence systems WUPES Prague
5. Katter R V and Montgomery C A and Thompson J R Cognitive processes in intelligence analysis a descriptive model and review of the literature Technical report US Army Research Institute for the Behavioural and Social Sciences
6. Keegan J A History of Warfare Random House London
7. Keegan J Computers can t replace judgement Forbes ASAP December
8. Laskey K B and Mahoney S and Stibio B Probabilistic reasoning for assessment of enemy intentions Technical report C I, George Mason University
9. Shulsky A N Silent Warfare understanding the world of intelligence Brassey s US
10. Taylor P C J and Strawbridge R F Data fusion of battlefield information sources Royal Military College of Science Shrivenham

11. Trafton D E Intelligence failure and its prevention Naval War College Newport RI
12. Sun Tsu date unknown The Art of War Oxford University Press