Developing a Decision Analytic Framework Based on Influence Diagrams in Relation to Mass Evacuations

Ken McNaught and Adam Zagorecki

Department of Engineering Systems and Management
Cranfield University
Defence Academy of the United Kingdom
United Kingdom

In this paper, we examine the role which decision analysis can play in a situation requiring a mass evacuation. In particular, we focus on the influence diagram as a tool for reasoning and supporting decision-makers under conditions of risk and uncertainty. This powerful modelling tool can help to bridge multiple specialist domains and provide a common framework for supporting decision-makers in different agencies.

An influence diagram is also referred to as a decision network and can be considered as an extension of a Bayesian network. Like a Bayesian network, it contains chance nodes which represent random variables and deterministic nodes which represent deterministic functions of input variables. However, in addition, an influence diagram contains decision nodes which represent decisions under local control and utility nodes which can represent a variety of costs and benefits. These might be measured in several dimensions including casualties and monetary units. Advantages of Bayesian networks and influence diagrams over more traditional risk and safety modelling approaches such as event trees and fault trees are discussed - in particular, the ease with which they represent dependencies between many factors and the different types of reasoning supported at the same time, e.g. predictive reasoning and diagnostic reasoning.

An illustrative, generic influence diagram is presented of a situation corresponding to a CBRNE attack. We then consider how this generic model can be applied to a more specific scenario such as an attack at a sporting event. A variety of potential uses of the model are identified and discussed, along with problems which are likely to be encountered in model development. We argue that this modelling approach provides a useful framework to support cost-effectiveness studies and high-level trade-offs between alternative possible security measures and other resources impacting on response and recovery operations.

INTRODUCTION

The nature of both successful and attempted terrorist attacks since 2001 have changed the perception of terrorist risk and consequently re-defined the public's attitude and security professionals' approach to the problem of public security. One of the key challenges which decision-makers responsible for public safety face today is balancing the cost of security measures with acceptable levels of risk.

Whether facing a long-term decision regarding the desired balance of investment across a wide range of capabilities or a short-term decision under time-pressure regarding the evacuation of an area, decision-makers are expected to manage a large number of influential factors and constraints, to take account of multiple stakeholders and views, and to make trade-offs and choices which are coherent and defensible. Decision support tools, while leaving the final choice to the decision-maker, can nonetheless help the decision-maker to gain understanding of a complex problem situation. By helping to identify the most critical and sensitive aspects of the situation and by providing a framework in which trade-offs can be assessed in a transparent, structured fashion, a decision support model can help the decision-maker to better understand the nature of the problem and to navigate their way through its complexity in order to arrive at a more thoughtful decision.

The risk management of public events, such as sport events, is a complex enterprise requiring cooperation between many organisations. One of the challenges is to build a common picture of the situation from the various pieces that are spread over multiple specialist domains and are *owned* by multiple organisations. For example, medical services should be informed and kept updated on current threats in order to prepare necessary resources to help potential victims in a timely manner. Therefore in the risk management domain, including mass evacuation, a new comprehensive approach for modelling interactions between factors spread over organisational boundaries would be desirable. Hudson et al. (2001, p4) argue that "*The need for an innovative approach was clearly discernable through analysis of government information regarding terrorist events.*" In this paper we outline an approach intended to support the building of models which encompass multiple aspects of risk management and mass evacuation, including identification of relevant risks, measures to mitigate them, costs associated with preparedness and possible consequences of successful attacks. Our approach is based on a decision model called an influence diagram and it emphasises a comprehensive approach to identifying key considerations and related costs.

The influence diagram (ID) is a probabilistic decision model. The use of probabilistic models in risk analysis has been steadily increasing, giving rise to the term probabilistic risk analysis (PRA) (Bedford and Cooke, 2001). While event trees and fault trees come under this heading, so too do more modern approaches such as Bayesian networks (Pearl, 1988) and influence diagrams (Howard and Matheson, 1984). Originally conceived of as an alternative, more compact representation of a decision problem than a decision tree, IDs are now more commonly regarded as extensions of BNs. Within the field of PRA, increasing use is being made of BNs and IDs. For example Ale et al. (2009) develop an integrated model of the air safety domain using BNs. The authors discuss their reasons for preferring this approach to more traditional methods such as fault trees and event trees. Ayyub et al (2009) employ an ID in a different role as part of their risk analysis for hurricane-prone regions. It is effectively used as a qualitative conceptual model of the overall situation. They then develop a number of event tree models based upon it. The ID is used to build and communicate an understanding of how the various parts of the system are related to one another.

To illustrate this approach, we consider a scenario in which a radiological dispersal device, commonly called a *dirty bomb* is used in a terrorist attack at a major sporting event. First, a more generic model is presented which could serve as the basis of an ID for a wider range of scenarios. Then we present the more specific and detailed model. Rosoff and von Winterfeldt (2007) considered the likelihood of a successful dirty bomb attack on Californian ports and the likely consequences of such an attack, both in terms of casualties and economic damage. It is the latter which can be expected to be particularly high for this method of attack. However, the authors also showed that the chance of successfully mounting such an attack is much lower than for a conventional explosion.

BAYESIAN NETWORKS AND INFLUENCE DIAGRAMS

To explain IDs, it is convenient to introduce Bayesian networks (BNs) first, as IDs can be viewed as an extension of BNs to decision-theoretic problems. A Bayesian network (Pearl, 1988) is a graphical representation of probabilistic dependencies between a set of variables. BNs combine *graph theory* and *probability theory* to model complex domains involving uncertainty. The graphical part of a BN encodes domain variables which are represented as nodes and relationships between them shown as directed arcs (links). The graphical part, often referred as the qualitative part, allows for efficient and intuitive encoding of dependencies between entities and concepts (represented as variables) in the domain. All variables in the network have probability distributions associated with them – these probability distributions address the problem of encoding uncertainty related to variables and dependencies between them. The number of probability distributions required to quantify the model is dependent on the complexity of the graph. In this way, Bayesian networks bridge graph theory and probability theory to create a modelling tool that neatly combines both.

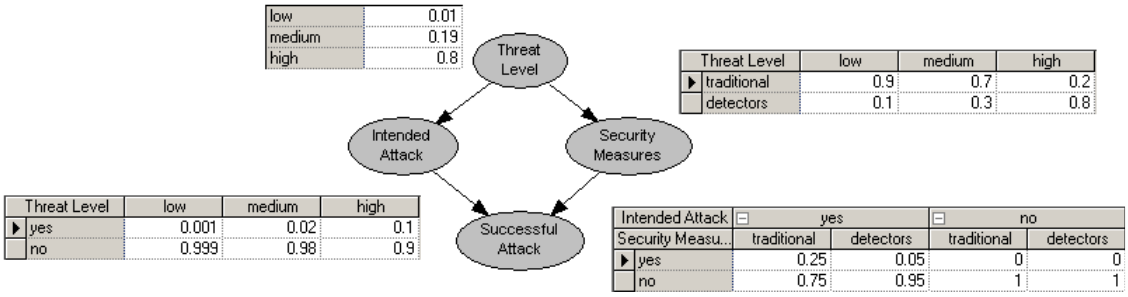

Figure 1 Example of a Bayesian network

A small example BN is shown in Figure 1. This simplistic model captures the probability of a successful terrorist attack given factors such as *Threat Level* and *Security Measures*. Since usually it is not known for certain if a particular event is a terrorist target, we should estimate the probability that the event will be subject to attack (probability distribution over the node *Intended Attack*). The challenge is to estimate that probability. One possible approach is to use the *Threat Level*, which summarises available intelligence at a high level and would typically be the result of in-depth analysis to describe a measure of current risk. For simplicity, we have assumed that there are three possible values: *low*, *medium*, and *high*, and we defined a probability distribution over these three states. The link between *Threat Level* and *Intended Attack* indicates that the

probability of attack is dependent on the threat level – and for every value of *Threat Level* one needs to define a corresponding probability of the attack taking place: for example, assuming that the threat level is high, the probability of attempted attack is assumed to be 0.1 (10%). Similarly we have assumed, for the sake of the example, *Security Measures* are dependent on the known threat level and there are two options: *traditional* and use of a special new detector system (*detectors*). Finally, the node *Successful Attack* defines the probability of the attack being successful given that the attack was intended and the security measures in place. In the BN graph, the node *Successful Attack* has two parent nodes – this indicates that the probability distribution over this node directly depends on both of these nodes. We need to specify the probability of a successful attack for each combination of the states of the parent variables. Two of these combinations are straightforward – if the attack is not attempted, it implies that there can be no successful attack. If an attack is attempted, we have assumed that there is a 25% chance of it being successful given traditional security measures and a 5% chance of it being successful given enhanced security measures, including use of the new detector system.

Once the BN model is created, it can be used to perform reasoning using probabilistic inference. BN inference allows the calculation of posterior probabilities assuming that some variables in the model can be observed (*evidence* nodes) – for example: what would be the probability of a successful terrorist attack if we know that the traditional security measures are being used and the threat level is *high*? Inference in a BN can be both diagnostic (given a set of observations, determine the most likely states of some other variables, as in the example above) and predictive (calculating the effect of manipulations of some variables on other variables).

BNs have been applied to numerous domains resulting in a wide range of academic and industrial applications (Pourret et al., 2008). Hardware diagnosis is a flagship application of BNs, with real-world examples such as Hewlet-Packard printer diagnosis (Jensen, et al., 2001) and aircraft diagnosis (Przytula & Choi, 2007). BNs have also been applied to risk analysis in the context of terrorist attacks - (Neil, et al., 2007) and (Hudson, et al., 2001), for example.

As mentioned earlier, the influence diagram was originally devised by Howard and Matheson (1984) as an alternative representation to the decision tree. One of the main problems of working with decision trees is that they become very large, very quickly. Since in a decision tree, every decision alternative and every outcome of a chance event is explicitly represented by a branch, and the chronological sequence of events expands outwards from left to right with every possible path displayed, even relatively small problems involving only a handful of decision and chance events, quickly explode into ‘a bushy mess’. This is particularly relevant at the conceptual stage of modelling when being able to visualise the situation and communicate understanding is crucially important.

The influence diagram does not explicitly display every possible path through the problem and so permits a more compact representation. However, the original intention was to convert the influence diagram of the problem, once this had been agreed at the

conceptual modelling stage, to an equivalent decision tree in order to solve it. Shachter (1986) describes an alternative solution mechanism, operating directly on the influence diagram.

Nowadays, IDs are more often described as extensions of BNs (Jensen, 2001), particularly since the same junction tree algorithms can be applied to their solution. State-of-the-art algorithms (Huang & Darwiche, 1996) are capable of performing inference in models with hundreds of variables in a matter of seconds. While both BNs and IDs are represented by directed acyclic graphs, the main difference is that IDs permit additional types of nodes and arcs. As well as the chance nodes and deterministic nodes which we find in BNs, IDs also contain decision nodes and value or utility nodes.

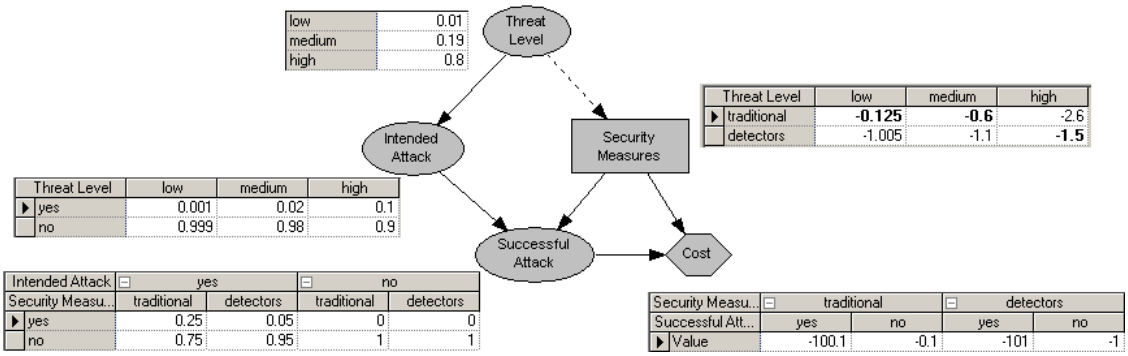

Figure 2 Example of an influence diagram

The meaning of chance nodes (represented by circles or ovals) and the arcs between them is exactly the same as for BNs. An arc between two chance nodes denotes probabilistic dependence and its direction indicates that the child node has been conditioned on the parent node. Consequently, to quantify the model, we will require a probability distribution of the child variable for every possible combination of the parent variables. While such arcs can indicate causality, they do not have to. Where a causal relation is present, it is usual to draw the arc showing the direction of causal influence as this normally results in a more efficient representation of the problem.

Decision nodes (represented by rectangles) represent a choice between alternative courses of action for the decision-maker. An arc from a chance node to a decision node is often called an informational arc. Such an arc means that the outcome of the chance node is known to the decision-maker before the decision is taken. The arc from a decision node to a chance node means that the decision taken will affect the chance node, i.e. the outcome of the chance node is somehow influenced by the decision.

In an influence diagram, there is always one terminal deterministic node called a value node which represents the decision maker's final goal or objective function. Value nodes are usually represented by hexagons. There may be more deterministic nodes, some possibly representing intermediate values, such as various benefits and costs, but there is always one terminal value node. This final value node is therefore required to weight the inputs from any intermediate value nodes in such a way that the decision-maker’s preferences can be represented and objective trade-offs can then be made between

competing choices. An influence diagram is therefore a BN with a terminal value node and at least one decision node. However, when displaying as opposed to solving an influence diagram with several intermediate value nodes, such as the one presented in this paper, we have chosen not to include the terminal value node and all of its associated arcs from the intermediate value nodes, in order to reduce the amount of clutter in the diagram.

Just like decision trees, IDs calculate an optimal set of decisions subject to the assumed probabilities of various chance events, the elicited preferences of the decision-maker for the various possible consequences and any evidence received from observable chance nodes ahead of those decisions. While such decisions are optimal in the mathematical sense, there will nearly always be additional factors not represented within the decision model which nonetheless have some bearing on the situation and which need to be accounted for by the decision-maker. This is one reason why decision support models can only ever advise and try to complement the experience and skills of a human decision-maker. It is instructive, however, to understand how such 'optimal' solutions are arrived at.

In order to identify the best course of action, we need to calculate the average or expected utility for each possible course of action. If a_k denotes the k^{th} alternative available to the decision-maker, e denotes the evidence available to the decision-maker at the time of the decision, o_i denotes the i^{th} possible outcome or consequence, and $U(o_i| a_k)$ denotes the utility which the decision-maker associates with outcome o_i given their choice of action a_k, then the expected utility of action a_k given the available evidence e is $EU(a_k \mid e) = \sum_i P(o_i \mid a_k, e)U(o_i \mid a_k)$. This is just a weighted average of the utilities which can be realised, with the weights corresponding to the estimated probabilities of the realisable outcomes given the alternative chosen and the available evidence. The alternative which produces the greatest expected utility can therefore be identified.

In the re-formulated example from Figure 1, presented in Figure 2, the node *Security Measures* is defined as the decision node. It no longer has a probability distribution defined over its states as the decision-maker chooses a state. Expected utilities associated with implementing the two security measures are calculated from the costs defined in the *Cost* node. The results of the expected utility calculations are shown next to the decision node. It can be seen that the traditional measures are more beneficial for the low and medium risk cases (expected utility -0.125 and -0.6, expressed in millions of £) and the new detector system is beneficial for the high risk scenario with the expected utility -1.5 versus -2.6 for the traditional security measures.

SCENARIO

In order to illustrate the application of IDs to the problem of mass evacuation, we present a simplistic scenario. The scenario concerns the evacuation plan for a large sporting event held at a stadium. The stadium is assumed to be located on a river bank, without any bridges in the vicinity allowing for evacuation to the other side of the river. The stadium

is otherwise surrounded by three areas which are different in character: a large park, a residential area characterised by a high density of small, private houses, and a small open space adjacent to the car park dedicated for the venue. A schematic map for the scenario is presented in Figure 3. Each of the three possible evacuation areas poses certain challenges and risks from the perspective of the evacuation. The park is characterised by large stretches of forested and relatively wild areas that can be accessed by vehicles and by the general public. The park offers large empty spaces that can easily accommodate crowds evacuating from the stadium. However, at the same time it is an area which cannot be easily cordoned off and it offers relatively good places for hiding explosives. The residential area features a high density of small, private buildings. The population living there undergoes constant rotation and does not create a strong community. Additionally, the area is characterised by a relatively high crime ratio and number of properties that are inhabited – ideal conditions for a terrorist group to perform their activities without drawing undesired attention. The car park area is relatively small, known to have insufficient capacity for larger events in the past.

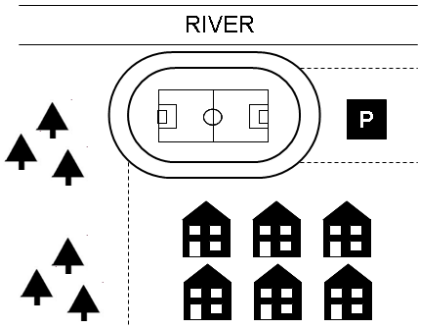

Figure 3 Outline of the scenario

For simplicity of the presentation, our scenario is limited to account for two types of terrorist threats: traditional explosives and the radiological dispersal device commonly called a dirty bomb. Since a bomb attack involving a traditional explosive can be viewed as a special case of the dirty bomb attack without the radiation aspect, we will further focus on the dirty bomb scenario, assuming that the model can account for the fact that there was no consequent radiation. Obviously, the model should account for cases where there was no resulting dispersion of the radioactive material due to improper construction of the device, even in the case of an attempted dirty bomb. The consequences of a dirty bomb can be categorised three-fold: (1) immediate fatalities due to explosion and/or high doses of radiation, (2) prolonged effects of exposure to radiation, and (3) economic impacts due to radiation hazards in the area, decontamination, etc. In our model we explicitly represent these three categories.

MODEL DEVELOPMENT

We propose the following approach to model development: first, a generic model would be developed to incorporate general factors that should be present for the typical case of a major sporting event. The generic model would consist only of a qualitative (graphical) part and the definition of the states of variables and probability distributions would be left for quantification in the specific model. Consequently, the generic model would be

customised to become the specific model based on a particular location, threats identified and the range of security measures available, etc. The model based on assumptions made in the above scenario is presented in Figure 4.

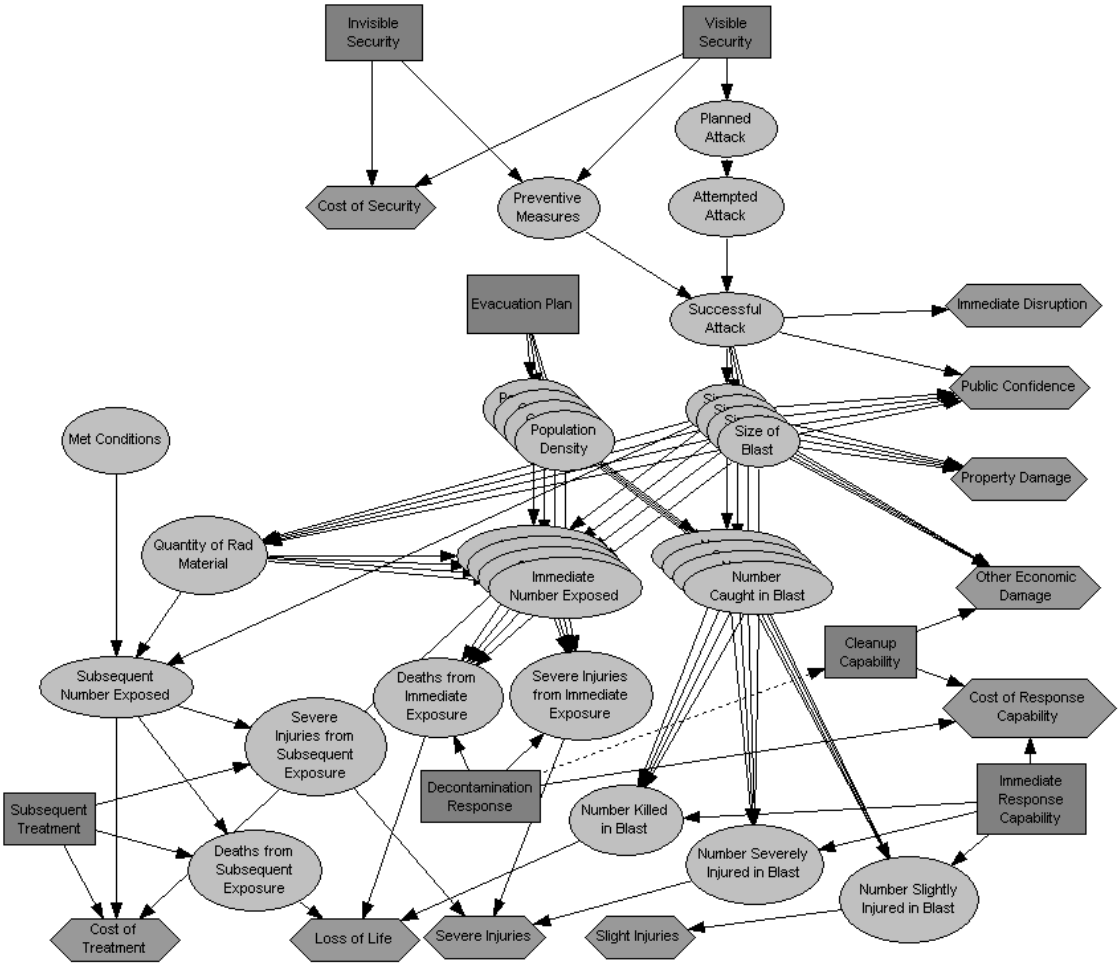

Figure 4 Model for venue evacuation

The model should be viewed as a decision support tool at the stage of formulating security and evacuation plans. However, other possible uses will be discussed in subsequent sections. It is easiest to explain the model when a chronology of (potential) events is considered. In the upper part of the model, there is a set of nodes related to a possible attack and its prevention. In the middle part, nodes such as *Population Density, Size of Blast, Number of Caught in Blast,* etc. are specific for particular zones under consideration and define probability distribution over effects of attacks in the context of each given zone. In our example there would be four areas under consideration: the stadium, and the three possible evacuation zones: the park, the residential area, and the car park. Therefore, in Figure 4 these nodes are repeated four times. The remaining nodes in the model concern the overall and long-term consequences of the attack which are not specific to the location of blasts, therefore no distinctions between zones is made for these nodes.

In the model there are several decision nodes, that define alternatives regarding: *Visible Security* and *Invisible Security*, *Evacuation Plans*, *Immediate Response*, *Decontamination Response*, and *Subsequent Response*. This set of decision nodes itself emphasises the potential of the model as a tool for combining expertise and data from different organisations involved in the emergency management process to create a comprehensive picture of the risk mitigation and response processes.

The complexity of trade-offs is highlighted by a relatively large number of different utility nodes that represent various financial concerns (*Cost of Security, Cost of Response Capability, Cost of Treatment, Property Damage, Other Economic Damage*), human life and health concerns (*Loss of Life, Severe Injuries, Slight Injuries*), and other public concerns (*Immediate Disruption*, *Public Confidence*). As mentioned earlier, utility nodes can represent different and conflicting criteria (such as monetary value, human causalities, perception of safety by general public, etc.). In principle, combining these criteria is very challenging and tools such as Multi Criteria Decision Analysis have been developed (Linkov et al., 2006). In the framework of IDs, different utility criteria can be combined using multi-attribute utility nodes to provide a tool for trade-offs.

The definition of each variable's states and the assignment of particular values to probability distributions would be done in the specific model. The most effective approach to model development would start with an initial version of the model to be developed by a knowledge engineer. Then this initial draft would be presented to the subject matter experts for comments and review. Mahoney and Laskey (1996) present a good discussion of the model development process

One of the key challenges with the problem of risk assessment and evacuation modelling is related to the nature of the problem, which is highly uncertain (terrorist intent, weather conditions, etc.), no reliable data is available (e.g. terrorist attacks are rare with constantly evolving strategies, no actual incidents of executed dirty bomb attacks), many aspects of the problem are highly qualitative in nature (e.g. public perception of events), and every instance of the problem is unique. In this context, subjective assessments are a necessity. Therefore, quantitative tools that support subject matter experts with knowledge elicitation and that support deeper understanding of the problem can be valuable. At this point it should be emphasised that the probabilities required to quantify the model do not need to be precise, rather *rough estimates* provided by experts may be sufficient in most cases. Sensitivity analysis can be used to identify parameters in the network for which the results are particularly sensitive and subsequent refinements of the model can be focused on only those parameters.

MODEL USES

One of the particularly useful properties of IDs is that they define a domain model rather than a set of specific scenarios. An ID encodes a joint probability distribution and corresponding utilities over the exhaustive set of possible combinations of states of all variables, which in practice means that it encodes all possible scenarios that can be described by the model variables. It achieves this by decomposing the problem into local

interactions between related variables (through the model's graphical part) and reducing in this way the number of required numerical parameters. Therefore, it is not limited to a small number of considered scenarios, as is the case with some techniques for risk management.

Firstly, without any quantification, the ID can serve as a conceptual model of a complex decision problem. This aids communication and understanding between problem stakeholders and provides a convenient, common mechanism for the decision analyst to elicit and synthesise subject matter expertise from several different domains, e.g. police, venue security, health services and radiology. The intuitive nature of the ID also helps both the decision analyst and the domain experts to check what assumptions are being made, particularly regarding dependencies and independencies between variables in the model.

Once quantified, a process requiring the estimation of probability distributions (either based on available data or the subjective opinions of domain experts) and the elicitation of preferences and utilities from decision-makers, the ID becomes a powerful decision support tool. Its most obvious use is to identify the 'optimal' course of action for a decision-maker given whatever evidence is available, in the manner described above. As noted previously, this mathematically optimum solution arises from an imperfect model of the real world situation and it is the decision-maker's responsibility to judge how close the model's assumptions are to reality. In doing so, the decision-maker should understand the basis on which the ID arrives at its suggested solution. While this requires some initial investment of time and effort from the decision-maker, the authors would argue that this is very likely to be handsomely repaid. It is worth pointing out that decision-makers in many fields, from medicine to maintenance, are increasingly receiving advice and support from decision aids such as these.

Our illustrative example concerned capabilities in hazard prevention, protection, response and recovery. Which of the many possible investments in each of these areas are likely to provide the greatest benefit within a given available budget? Following the elicitation of costs and their likely benefits for each alternative in these domains, and taking into account the dependencies within the domain, the ID helps to address just these issues. We contend that decision-makers and the analysts who advise them have much to gain by adopting a decision analytic approach to this type of question.

As well as identifying a preferred course of action, a quantified ID can also suggest how important any unobserved information variables are. Indeed, it can put an actual value on such information variables. Comparing these to the expected costs of obtaining such information allows the decision-maker to identify which information variables are worth pursuing and which are not. Those worth pursuing can then be prioritized. This process makes use of the concept of value of information. This is simply the difference between the expected utility calculated with the information variable in question known and the expected utility calculated without this information.

The ID could also be used to aid evacuation planning decisions. In the scenario presented here, there were several possible evacuation zones. However, given the danger of a multiple attack scenario, evacuation planners need to be wary of moving the evacuees to a zone at high risk of a secondary attack. Any evacuation plan should consider the attractiveness of the chosen zone to terrorists mounting such an attack. The likely population density of the evacuation zone and knowledge of its whereabouts, together with its proximity to sites where bombs could be placed and security is lower are just some of the factors to be considered. Red-teaming exercises involving terrorism and security experts trying to think like terrorists in order to identify weak spots and assess terrorist preferences could also inform such modelling and planning.

An additional use of such models, or at least the BN part of such models, is forensic diagnosis. For example, by observing the effects of a blast, inference can be made about the quantity and type of materials used. In some cases, inferences about the skills, capabilities and resources of the group responsible might also prove valuable, particularly when combined with information from police and intelligence agencies. Taroni et al. (2006) present a variety of applications of BNs in forensic science more generally.

CONCLUSIONS

Even though BNs and IDs are powerful tools for modelling risk and can provide many benefits, as discussed earlier, not all aspects can be sufficiently modelled and captured within this framework. In particular, aspects related to the physics of explosives, their lethality, radiological material dispersion and radioactivity, weather considerations, etc. can be modelled more accurately and efficiently with other modelling techniques. In our opinion these models should be viewed as complementary.

In this paper we discussed application of IDs to the problem of risk management and mass evacuation. A generic ID model for CBRNE attack was developed. The generic model was customised for a simple scenario concerning a dirty bomb attack on a sporting event in order to discuss the benefits and challenges of developing ID models for risk management and evacuation planning. Several potential alternative uses of the model were also discussed.

ACKNOWLEDGMENTS

The authors would like to thank to Matthew Healy and Keith Weston for providing invaluable insights into terrorist risk assessment for large public events. All models were developed using the GeNIe software developed at the Decisions Systems Laboratory, University of Pittsburgh (genie.sis.pitt.edu).

REFERENCES

Ale, B. J. M., Bellamy, L. J., van der Boom, R., Cooper, J., Cooke, R. M., Goossens, L. H. J., Hale, A. R., Kurowicka, D., Morales, O., Roelen, A. L. C., & Spouge, J. (2009). Further development of a causal model for air transport safety (CATS): building the mathematical heart. *Reliability Engineering and System Safety*, 94, 1433-1441.

Ayyub, B. M., Foster, J., & McGill, W.L. (2009). Risk analysis of a protected hurricane-prone region I: model development. *Natural Hazards Review*. pp. 38-53.

Bedford, T. & Cooke, R. (2001). *Probabilistic Risk Analysis: Foundations and Methods*. Cambridge University Press, Cambridge.

Howard, R. A., & Matheson, J.E. (1984). Influence Diagrams. In: Howard, R. A. and Matheson, J.E. (eds.) *The Principles and Applications of Decision Analysis Vol. II* Strategic Decisions Group, Menlo Park, CA, pp. 721-762.

Huang, C. & Darwiche, A. (1996). "Inference in Belief Networks: A procedural guide", *International Journal of Approximate Reasoning*, 15(3). pp. 225-263.

Hudson, L. D., Ware, B. S., Mahoney, S. M., Laskey, K. B. (2001). *An Application of Bayesian Networks to Antiterrorism Risk Management for Military Planners*. George Mason University.

Jensen, F.V. (2001). *Bayesian Networks and Decision Graphs*, Springer-Verlag, New York.

Jensen, F. V., Skaanning, C. & Kjærulff, U. (2001). The SACSO System for Troubleshooting of Printing Systems. In *Proceedings of the Seventh Scandinavian Conference on Artificial intelligence*. Lund, H. H., Mayoh, B. H. & Perram, J. W. (eds.) *Frontiers in Artificial Intelligence and Applications*, 66. IOS Press, Amsterdam, The Netherlands, pp. 67-79.

Linkov, I., Varghese, A., Jamil, S., Seager, T. P., Kiker, G. & Bridges, T. (2006). Comparative Risk Assessment and Environmental Decision Making. *Nato Science Series: IV: Earth and Environmental Sciences*, 38. pp. 1568-1238.

Mahoney, S.M., & Laskey, K.B. (1996). Knowledge Engineering for Complex Belief Networks. *Uncertainty in Artificial Intelligence: Proceedings of the Twelfth Conference*. San Francisco, CA. Morgan Kaufmann. pp 289-396.

Pearl J. (1988), *Probabilistic Reasoning in Intelligent Systems: Networks of Plausible Inference*, Morgan Kaufmann, San Francisco, CA.

Pourret, O, Naïm, P. & Marcot, B. (eds.) (2008). *Bayesian Networks: A Practical Guide to Applications*. ISBN: 978-0-470-06030-8. Wisley.

Przytula, K. W. & Choi, A. (2007) Reasoning framework for diagnosis and prognosis. In *Aerospace Conference* IEEE, pp. 1-10.

Rosoff H., & von Winterfeldt, D. (2007). A Risk and Economic Analysis of Dirty Bomb Attacks on the Ports of Los Angeles and Long Beach. *Risk Analysis* 27(3). pp. 533-546.

Shachter, R. (1986). Evaluating influence diagrams. *Operations Research* 34. pp. 871-882.

Taroni, F., Aitken, C., Garbolino, P. & Biedermann, A. (2006). *Bayesian Networks and Probabilistic Inference in Forensic Science*. Wiley, Chichester.