Technosocial Modeling of IED Threat Scenarios and Attack

Paul Whitney, Alan Brothers, Garill Coles, Jonathan Young, Katherine Wolf, Sandy Thompson, David Niesen, John Madsen, Cindy Henderson

Pacific Northwest National Laboratory
902 Battelle Boulevard, Richland, Washington 99352
{ paul.whitney | alan.brothers | garill.coles | jonathan.young | katherine.wolf | sandy.thompson | d.niesen | john.madsen | cindy.henderson }@pnl.gov

Abstract

This paper describes an approach for integrating sociological and technical models to develop more complete threat assessment. Current approaches to analyzing and addressing threats tend to focus on the technical factors. This paper addresses development of predictive models that encompass behavioral as well as these technical factors. Using improvised explosive device (IED) attacks as motivation, this model supports identification of intervention activities 'left of boom' as well as prioritizing attack modalities. We show how Bayes nets integrate social factors associated with IED attacks into general threat model containing technical and organizational steps from planning through obtaining the IED to initiation of the attack. The models are computational representations of process models and associated social factors. When combined with technical models, the resulting model provides improved knowledge integration into threat assessment for monitoring. This paper discusses the construction of IED threat scenarios, integration of diverse factors into an analytical framework for threat assessment, indicator identification for future threats, and future research directions.

Introduction

Estimating the likelihood of future events based on current and historical data is essential to decision-making processes of organizations charged with deploying resources against known or suspected threats, such as IED prevention (Zorpette 2008; National Research Council 2007). Predictive tasks, if successfully accomplished, have significant value to all situations where human actions and beliefs influence their decision-making processes, such as national security deterrence concerns related to IEDs or other undesirable activities. Successfully modeling social elements as well as technical factors associated with human decision-making processes requires predictive tasks such as deterrence and risk characterization, and understanding competing options and cascading effects. These predictive tasks contain both technical and social components, in the sense that there are strong process models detailing the physical steps required as well as motivational aspects that drive the human activities. Many world events, such as IED attacks, involve a series of technical process steps that are precursors to the execution of the threat, as well as socio-cultural human-based influences that derive a threat-actors situation-dependent beliefs and behaviors.

The lack of an integrated modeling framework that encapsulates social as well as technical factors negatively affects decision-maker abilities to fully assess and predict the likelihood of future threat activities. This paper investigates such an integrated modeling framework, using an IED scenario as an example, and discusses the following:

- The Technosocial Modeling Approach, Linking Behavior and Process Models
- IED Scenario Development & Description
- The Bayes net General Threat Model and IED Process
- Summary and Future Research

Technosocial Modeling Approach, Linking Behaviors and Process Models

Our modeling approach focuses on integrating social and technical factors within Bayesian network models, along with associated information (threat related data and evidence) to drive the model. Bayes nets (BN) are graphical representations of relationships among variables, provide generalized, quantitative modeling capability with established methods for integrating data, and compactly represent causal interactions in a complex environment where uncertainty predominates, see Jensin and Nielsen, (2007).

Social Behaviors within the Model

BNs are process models that can incorporate social factors that influence threat such as capability, opportunity, and motivation. Integrating social/behavioral modeling within technical process models should improve threat likelihood modeling and traditional decision-making processes by enabling decision makers to account for the variety of uncertainty associated with various model components.

The IED scenario and model (described below) provide a preliminary application focus through which the research team can test the integrated modeling hypothesis. The demonstration integrated BN threat model includes technical and social components and processes, detailing the physical steps leading up to an IED event, as well as the motivational aspects that drive human activities, supporting likelihood assessments.

Why Bayesian nets

BNs are a powerful and well-developed technology that can potentially provide insight and predictive capability from the social aspect of the social-technical interaction. We base the quantification of the likelihood of events within a combined behavior and process model on probability calculus. This mathematical formalism provides the framework to combine the two probabilities (technical and social) into an overall probability of a successful execution of a single IED attempt:

P(Successful IED) =
P(Successful IED | Attempt) * P(Attempt)+
P(Successful IED| no Attempt) * P(no Attempt)
= P(Successful IED | Attempt) * P(Attempt).

Where the last equality follows from:

P(Successful IED| no Attempt) = 0.

IED Scenario Development & Description

IED attacks are possible anywhere in the world because they are effective weapons that are relatively cheap to procure or construct and can be as simple or complex as the people that employ them. Scenario characteristics are outlined in Walker (2006 – see slide 3), and Magness (2005 - see Figure 2). Although the characteristics of IEDs vary with time, geography, and technology, the overwhelming preponderance of IEDs have one mutual trait - they are the culmination of a networked effort. Additionally, since the materials and capabilities for IEDs are widely available, and since the rate of occurrence of IEDs varies – there is a strong suggestion that social and behavioral factors are the critical drivers for IED occurrence and rates.

IED networks can be as varied as the IEDs they employ from small isolated groups to loose associations of action cells and large, highly structured organizations. Motivations vary across the process – potentially ranging from personal (revenge), criminal (monetary objectives), or ideological. However, the common attribute of every IED network is the threat they present, and by dissecting that threat, the technical and social dimensions of IED networks can be examined.

We developed representations and linkages between behavior and process (technical) models, IED scenarios, and inferences and examples. IED's were selected based on the potential impact to a target (infrastructure), the fact that they represent simple attacks (simple to model), while from a social/behavioral perspective, IED's as an attack tool include numerous motivational elements that are challenging to model.

A precursor to modeling IED attacks was constructing a realistic scenario. The general ingredients of a scenario, with examples, include who (insurgency, religious or political extremists), what (selection of one or more explosive materials), where (specific geographic location), when (date/time, perhaps associated with a preceding observational event), why (the desired outcome), and how (the method of attack execution). Scenarios need not be long or complex, so long as they contain the critical elements necessary for a modeling framework. After identifying the critical elements for an IED scenario, a notional example scenario was developed:

> Group X has the objective of repelling and limiting the efficiency of a well-armored occupying force in order to preserve the sanctity of their way of life from the corrupting influences of the occupying force. This group has access to a wide variety of demolitions and explosives as well as experts in employing them, having had many of their members trained in military service and universities across the world. To send a message to the occupying forces, a low-level recruit places an IED in a roadside mailbox – well aligned to target a passing vehicle, on a route frequently traveled by the occupiers. After placing the device, an observer remains nearby to set off the charge at the appropriate time when a target vehicle passes the mailbox (detonation in this case done by command wire) and to also record the attack for effects analysis and future training, motivational, propaganda, and recruitment purposes.

The Bayes Net General Threat Model and IED Iteration

A model designed to represent generic threats was constructed – see Figure 1 for a representation of this model in the GeNIe (2008) software. The model is general in the sense that the elements/components are relevant to IEDs but are also the criteria considered for other threats; see Paté-Cornell and Guikema(2002) for a similar model. The model computes relative risk across scenarios based on currently available information and predicts scenario occurrences.

This General Threat Model (GTM) is a Bayes net representation of the relationship among these concepts contributing to an overall threat – Motivation, Capability and Target Characteristics. Grey boxes are critical concepts for understanding threats. The black represents risk, and white represents consequence. Technical aspects in the model are represented in capabilities and in the consequence parts of the models. Social aspects are captured in the Motivation & Intent and the Target Selection nodes. This model (and similar models) provides a view that integrates over a period of time. This particular model is constructed to reflect that motivation and intent can provide the drives to seek capabilities.

The model constituents within Figure 1 include:

- Violent Scenario Likelihood: This component represents the probability of a specific scenario, conditionally based on intent, the target accomplishing the intent goal, and the capability to accomplish the goal.
- Motivation and Intent: The degree to which an organization or individual is motivated to execute biological terrorism, including contextual as well as intrinsic information.
- Target fits Group Goals: This component considers, for example, whether the successful execution of a scenario against a specific target advances the group's agenda and is consistent with group ethics.
- Target Select: The perception of vulnerability associated with a potential target and whether it's a factor in the threat, as (presumably) an attack would be made only if success against the selected target was possible.
- Perception of Vulnerability: This component considers whether the group believes they can gain access to the target.
- S&E Knowledge: The group's access to the fundamental Scientific and Engineering knowledge to execute a specific threat scenario. This could be decomposed into various compartments related to understanding, constructing, and delivering devices, sufficient to carry out the threat.
- Capability for Scenario: Whether the group has the capability to execute the threat, based on the contributions of contributing indicators.
- Success of Scenario: The likelihood of success, given threat and opportunity, and measures the extent to which the group objectives are achieved.
- Equipment: The gear necessary to handle, process, and weaponize the material (for example, beakers, test tubes, personal protective equipment, etc.).
- Operational: Planners (thought / group leadership) and resources (people, money) required for executing an attack scenario.
- Material: Any raw materials that contribute to a terrorist attack tool. For a bio-threat, this could be anthrax spores, or E. coli samples, or hoof & mouth slurry. For an IED, it would include the trigger and explosive. For a chemical threat, it could be the chemical, or a set of precursor chemicals.

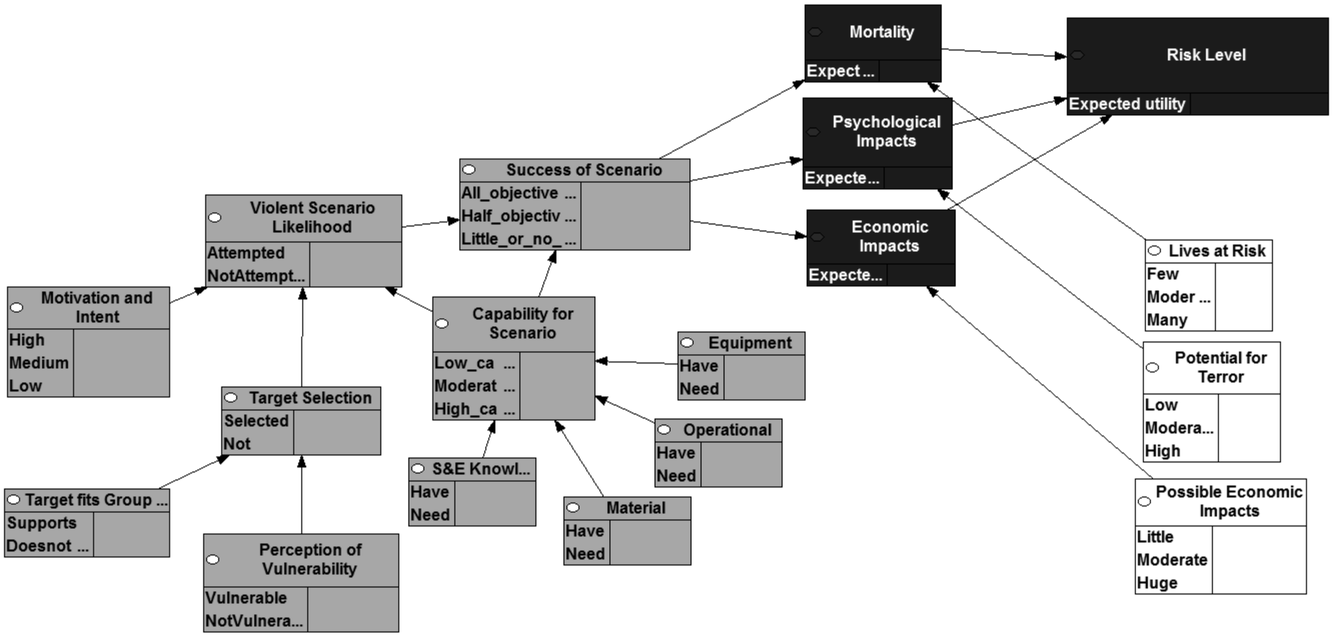

Figure 1. General threat model

The threat model results in a calculation of the likelihood of the scenario being successfully executed. Note – without calibrating the model against empirical observations, the primary utility of this calculation is to compare the *relative* likelihoods of distinct scenario variations to be successfully carried out. The likelihoods are multiplied against the consequences to estimate a risk.

Risk is equal to likelihood×consequence. For this effort, consequence has three components, measure of human harm in terms of causalities or mortality, the economic cost, and the sociological/psychological consequences from implementation of the scenario. Risk has the same three corresponding dimensions. Relative risk assessment includes estimation of probabilities or likelihoods associated with each scenario as well as estimation of the consequences from implementing the scenario.

The model in Figure 1 is an interesting 'meso-scale' view of threats. To understand what is being aggregated, we develop and compare this model with a more detailed IED threat model. Figure 2 depicts the IED process model.

This notional process model (Figure 2) is based on a variety of resources (Magenss 2005, Walker 2006, National Research Council 2007, Zorpette 2008). This process model shows an IED attack as a number of explicit steps. These steps includes obtaining funding and bomb materials, recruiting people, constructing the device, selecting the target, delivering the device to its target, carrying out the attack, and escaping. The steps in the process model are roughly sequential except that in the early stage the obtaining of human, financial physical resources can occur in parallel and are interdependent. All of the steps of the process have logical connections to other steps and the ultimate degree and likelihood of success is based on the outcome of each step. As recognized by a variety of researches – BNs can be used to represent process models (e.g. see Bobbio et al 1999). We take advantage of this to represent the IED process in GeNIe – as shown in Figure 2.

Distinct groups with their distinct motivations can potentially play across the process shown in Figure 2. A group with a political agenda might be driving the planning and/or finance (steps 1 and 2). A group (or individuals) with financial motivations might be engaged in placing the IEDs (step 12). At each step of the process – there must be willing and capable individuals to carry the process forward.

Contrasting the models – the primary perspective for the GTM is that there is a single driving organization, and that part of the necessary capabilities and resources are other people or organization to carry out the steps in the process model.

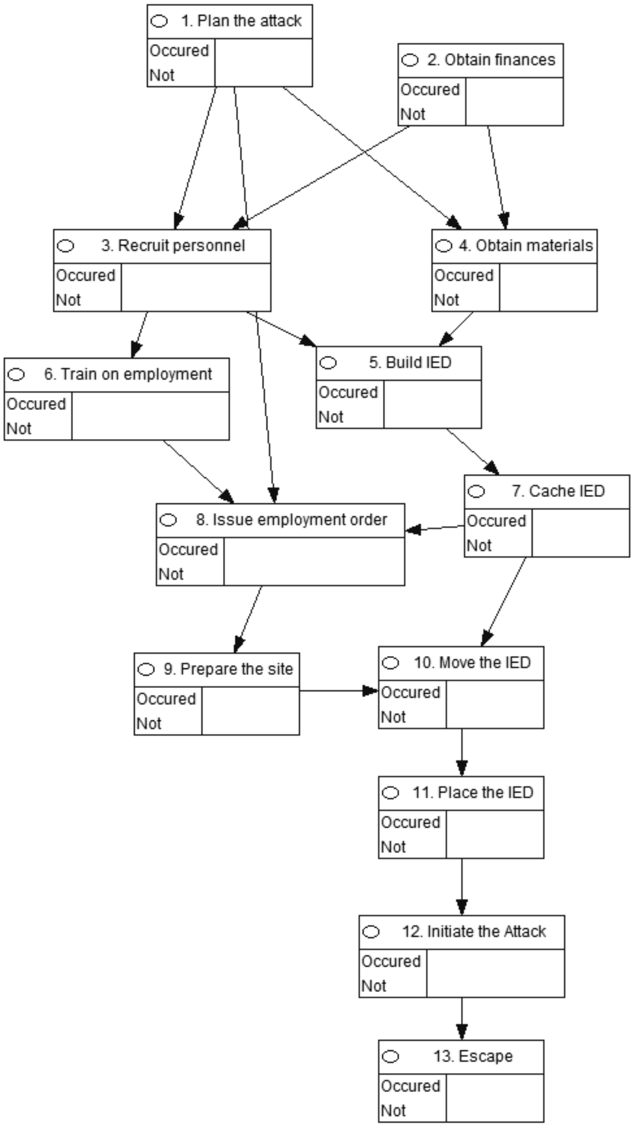

Figure 2. IED process model

Detection Model

The process model lays out the sequence of steps required to carry out an IED attack. Making explicit the activities involved in carrying out an attack is the first step in the development of a detection model. While the GTM can be used to evaluate scenarios based on relative risk, the process model provides insight into the activities necessary to execute the threat. This model can be augmented to (potentially) support detection and associated interventions to disrupt the process. The detection model can be used by analysts monitoring specific groups to detect the intent to carry out an attack and assesses the imminence of that attack.

Figure 3 shows how the process model can be augmented to support detection. Directly-observable indicators are connected to indicators (steps) in the process model. In particular – the figure shows – for one of the nodes (Step 9) in the process model some of the types of observable indicators that may be relevant to showing that the scenario is in progress. The particular observables are related to new people, faces and physical changes in a potential IED site. Other steps in the process have their associated observable indicators.

Any number of indicators could be associated with each of the nodes in Figure 2. Of particular interest within the IED process model are those nodes that have clear social/behavioral elements:

- Plan the Attack: This node requires one or more "mastermind planners" that are joined by one or more levels of social fabric that unites them in a common cause to attack.
- Obtain Finances: Resourcing an attack requires monetary funds or some other tangible item of value that the planners can acquire to finance their activities. Financial and contractual exchanges generally are accompanied by some type of transactional trail that contains multiple levels of human involvement.
- Recruit Personnel: How do the attack planners attract and retain like-minded individuals, or at least individuals whose circumstances dictate that they accept questionable employment. Are participants willing or unwilling?
- Obtain Materials: IED attacks require numerous components such as but not limited to explosive materials. These materials must be obtained through some type of supply network that involves humans, transportation, and financial/contractual exchanges.

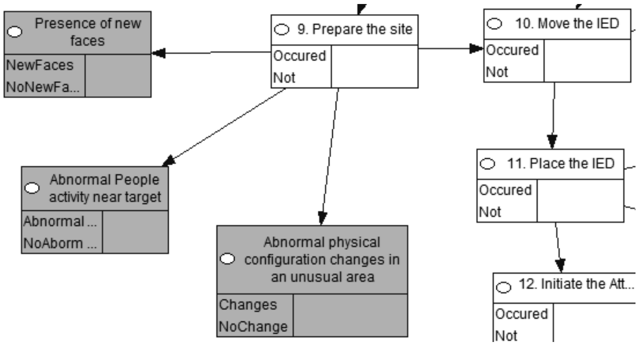

Figure 3. Observable Indicators related to the IED process model

The detection 'mode' of the process model is meant to be used by intelligence analysts for monitoring whether the particular IED scenario is underway. The model has been quantified with conditional probabilities that give reasonable behavior first approximation behavior.

Summary and Future Research

The IED models addressed in this paper consist of three elements: 1) a general threat model 2) a process model, and 3) a detection layer on the process model. The process model represents a technical model. The other two models start to model the associated human element. These models, when provided with data, provide likelihood information for outcomes (e.g., the relative likelihood of each IED attack scenario in a threat model) or a measure of imminence for the detection model (e.g., how likely is it that a particular activity in the IED process model is being carried out based on human activity).

Topics for our future investigations focus on validation and information integration. A key point for validation of models is that each of the models is based on 10's to 100's of parameters. This characteristic (a large number of parameters) is shared by other approaches in computational technosocial modeling, be it Systems Dynamics, Agent Modeling etc. To estimate and/or empirically validate a model with that number of parameters requires independent data on the order of a multiplier of the number of parameters. So, doing a case study on a particular group can be viewed as '1' observation. There are databases of observations that can be used to validate aspects of some of the models developed for DHS. This aspect of the work is ongoing. Another key point for validation is that the models are of a mathematical form (Bayes networks) that they can be empirically validated. Even better, if we have models for the same broad phenomena from distinct, and perhaps competing, papers, and if data are available to validate these models, an assessment can be made of which model fits the data better.

In addition to empirical observations, the type of information commonly brought to bear on graphical models is (expert) opinions. Opinions are used as inputs for the form of model construction and for the probability parameters. In addition to how to most effectively elicit the information, there are issues of combining information from multiple opinion providers, and how to weight or combine that information with direct empirical observations.

Finally, each of the models, the meso-scale model represented in Figure 1 and the more detailed process model in Figure 2, are presented and calculate without explicitly considering the context. For instance, the group engaged in retrieving finances for a particular scenario might at the same time be engaged in obtaining finances for a number of scenario events. The area of placement for attacks might be influenced by social or technical factors, such as the willingness of local populace to report IED placement and ease of surveillance observation based on physical conditions and available technology. A critical next step is placing such models in context.

References

Bobbio, A., Portinale, L., Minichino, M., and Ciancamerla, E. 1999. Comparing Fault Trees and Bayesian Networks for Dependability Analysis. In *Proceedings of the 18th international Conference on Computer Computer Safety, Reliability and Security* M. Felici, K. Kanoun, and A. Pasquini, Eds. Lecture Notes In Computer Science, vol. 1698. Springer-Verlag, London, 310-322.

Committee on Defeating Improvised Explosive Devices: Basic Research to Interrupt the IED Delivery Chain, 2007, *Countering the Threat of Improvised Explosive Devices: Basic Research Opportunities*, National Research Council. http://www.nap.edu/catalog.php?record_id=11953

GeNIEe & SMILE [Web Page]. Available at: http://genie.sis.pitt.edu.

Jensen, Finn V. and Thomas D. Nielsen, 2007, *Bayesian Networks and Decision Graphs, Second Edition.* Springer, New York.

Magness, Thomas H. "IED Defeat: Observations from the National Training Center" *Engineer: The Professional Bulletin of the Army Engineers* Jan-Mar 2005. 28-31. http://www.wood.army.mil/ENGRMAG/PDFs%20for%20 Jan-Mar%2005/Magness.pdf

Paté-Cornell, M.E. and S.D. Guikema. "Probabilistic Modeling of Terrorist Threats: a Systems Analysis Approach to Setting Priorities Among Countermeasures," Military Operations Research, Vol. 7, No 4, December 2002

Walker, Starnes – Presentation delivered to the AAAS Forum on Science and Technology Policy. http://www.aaas.org/spp/rd/Forum_2006/walker.pdf

Zorpette, Glenn "Countering IEDs", *IEEE Spectrum*. September 2008; 26-35.