Journal of Bioterrorism & Biodefense

Melnick E, J Bioterror Biodef 2015, 6:2
DOI: 10.4127/2157-2526.1000134

Short Communication Open Access

Quantitative Decision Tools for the Management and Analysis of the Risk from Terrorist Attacks

Edward Melnick*

Statistics Group, 44 West 4th Street, Suite 8-56, New York University, New York, USA

***Corresponding author:** Edward Melnick, Statistics Group, 44 West 4th Street, Suite 8-56, New York University, New York, 10012, USA, Tel: 212-998-0444; E-mail: emelnick@stern.nyu.edu

Received date: January 30, 2015, **Accepted date:** March 20, 2015, **Published date:** March 27, 2015

Abstract

A natural epidemic is a disease that suddenly affects many individuals in a short time period, spreading from person to person in a locality where thedisease is not usually prevalent. The sudden outbreak of an epidemic is usually modeled as a random variable because it cannot be anticipated. Epidemics introduced by bioterrorists are planned events by intelligent adversaries, who might also introduce other terrorists' activities that dependon the responses of the defenders. Since these events are not random, models maybe helpful for anticipating terrorist attacks. Since defendingagainst such attacks does not fit into the classical modeling paradigmbecause there is a scarcity of data, the defender must respond quickly, the attacker can also adapt new strategies in response to the actions of thedefender, new modeling strategies are required to improve the strategies of the defender. In this article, a Stackelberg model combined with fault trees is proposed for determining sequential optimal defense strategies for thedefender by identifying minimal cut sets of events that would most likely lead to a successful terrorist attack. Further, if the model can be formulated as a sequence of Markovian state changes based on default trees, a dynamic programming problem with the Bellman equation reduces the solution from evaluating a complex model to evaluating a sequence of simple problems.

Keywords: Risk; Reliability; Fault trees; Sequential games

Introduction

Risk is the potential negative impact (disease) on an individual or asset of value that may arise from a present process or future event. An operational definition of risk is the expected loss (debilitating sickness or death) resulting from the consequence that a hazard (epidemic) has occurred.

Risk assessment consists of tools for determining potential risks as well as the strategies and costs for managing them [1]. It requires an analysis of the underlying process to identify limitations and conditions that contribute to risk. In the study of reliability (engineering) fault trees are graphical representations of cause and effect relationships within a system, and are commonly used for analyzing cost benefit strategies. These trees have an inverted structure with the catastrophic event at the top and possible causes underneath as the mode events. The branches of the tree spread downward, beginning with sub-system failures and ending with component or elementary events. The root cause of the failure is the top event. Once constructed, minimal cut sets are identified that consist of necessary and sufficient combinations of component failures which, if failed, cause the system to fail. Based on simulations and sensitivity studies, cost effective strategies are tested for reducing the risk of system failures. The bottom-up analysis of fault trees, called event trees, is used in system design to evaluate potential risks associated with sets of component failures. Thus, the top-down analysis is used in fault diagnoses once the catastrophic event has occurred, and the branches are studied bottom-up for designing a defense system. Trees are now being developed for dynamically changing systems such as those found in economics and issues related to homeland security.

Game theory is a model for studying decision making strategies of intelligent rational competitors, especially in the presence of minimal data. The Stackelberg model is a specially defined game where the competitors act in sequence rather than at the same time. In the game of defender versus terrorist where the defender lives in a democracy with a free press, the terrorist observes the actions of the defender. At each further iteration the first mover knows the options available to his opponent and based on the competitor's constraints (financial resources, manpower, technical resources for transportation and armaments, etc.) the mover computes the optimal strategy for his opponent and in a deterministic setting, determines his options from the default tree. In the more common setting the 2 players have different amounts of information and must use subjective probabilities to determine the expected choices made by an opponent. The solution for each opponent is based on the expected optimal choice of his opponent where the terrorist has at least one option (pure strategy) and the defender might not know all of the potential targets available to the terrorist (mixed strategy occurs when the defender uses a probability distribution to determine how he will protect a subset of targets). Under the additional assumption that once an opponent has made a decision it cannot be undone then, after each iteration of the game, the optimal solution is found by backward induction (dynamic programming) and is known as Nash equilibrium. Further, if a mixed strategy is applied to the lowest level (levels determined by the default trees) of the game, then after each iteration, the probabilities are updated by Bayes theorem. Finally, if the options from one level of the default tree to the next level are Markovian, the computational problem is greatly simplified by expressing the objective function (utility function) as a Bellman equation. In this setting, dynamic programming computes to an optimization strategy by transforming a complex problem into a sequence of simpler problems.

Preliminary

The classical approach to risk assessment is the organization and analysis of scientific knowledge and information of potentially hazardous activities or substances that might pose risks under specified circumstances. Although many tools have been developed for quantitatively analyzing risk, the tools are often inappropriate for assessing terrorism. In terrorism, the occurrence of a hazardous event to a society is not random but initiated by an intelligent agent, who has had the opportunity to analyze potential targets to find the setting where the attack will create the greatest damage. Further, each attack has its unique characteristics that do not allow for the capturing of useful amounts of data. One strategy for analyzing complex events is to develop a game theory model with the goal of finding optimal allocation of defensive resources to minimize the effect of a terrorist's attack. In the classical game theory model opponents know all strategies available to both players, decisions are made simultaneously, and the result of all decisions is known by both players where a gain for one opponent is a loss for the other one. In contrast, The Stackelberg model [2] is a variant game theory sequential model where the range of strategies for each opponent is unknown to the other opponent and the consequences of the strategies of both opponents are not symmetrical. The model is analyzed by backward induction; i.e., the starting event is the attack and then working backwards to identify the steps taken by the terrorists that led to the attack. Based on the assumption that both the attacker and defender are rational with the goal of winning the game according to their objectives, the solution to the model is known as Nash equilibrium; i.e., neither player is willing to change strategies under the condition that no new information about the opponents is available.

Stackelberg Model

The modeling process begins after a terrorist attack. To the defender, the event appears to occur randomly. The strategies and targets open to the attacker are unknown to the defender and in an open democracy the strategies used by the defender are usually known to the terrorist because they are in the public domain. Unfortunately, the more secretive the strategies of the defender, the more the terrorist wins because he is forcing changes in the basic principles of freedom.

Constructing a model after an attack (occurrence of a hazardous event) by an intelligent opponent is unique to the study of terror. The attack was not anticipated, the goal of the attacker is unknown, the attacker might even be unknown, there is nothing to indicate that the attack was an isolated event or a series of events, and there is no useful history to provide answers to these and other questions about the attack. The study of risk and the prevention of future negative events are often modeled based on probabilities and the principles of game theory. The first problem is determining the "payoff", objectives of the terrorists and the defenders. The second problem is determining the mechanism for promoting the attack.In the case of terrorism the goals of the attacker and defender differ. The defender wishes to minimize the damage resulting from an attack. The payoff for the attacker can depend on the effect of the attack on one of all of the following criteria:

- Attacker's population – show its superiority
- Defender's population - fear of bioterrorism or beheadings
- Symbolic motivation - reaction to the cartoons of Mohammed
- Maximizing damage - World Trade Center Buildings.

Understanding the terrorists' objectives requires knowing their culture and understanding the goals of previous attacks. The second problem is the determination of the delivery system used to create the attack. For example, airplanes were used in the World Trade bombing, passengers on commercial vehicles transported concealed destructive devices, automobiles were used to smuggle terrorists into the country, and ships could be used to transport heavy equipment into a vulnerable area. In the past, mail has been used to send deadly viruses (anthrax) and there is the constant fear of deadly pathogens being sprayed into the air or put into water systems. Although the above lists are only subsets of possible strategies available to terrorists, the more accurate the lists, the better prepared are the defenders. Because the strategies of the terrorists are unknown to the defenders, the defenders can at best try to state probabilities associated with each strategy. Again, this too is difficult because of the lack of data. However, there are other sources of data that can provide insights into the identity of potential terrorists and their capabilities. One way this has been studied is through the development of networks where individual cells are the modes. In this structure, defenders study the individuals in a cell as well as the changes of its members through time. This information is useful for determining the capabilities of a cell and the changing of the members can indicate plans and capabilities for an attack. Further, the defenders can also have some influence on the terrorists' strategy by how they construct their defenses. Advanced screening methods at airports will lower the probability that they will be point of entries to the defender's country. Writings about defense systems at different ports and roving heavily armed soldiers at subway stations will discourage attacks at these sites. This strategy has been in use at the Los Angeles International Airport where a computer program has been developed that assigns random monitoring sites for armed security guards based on the solution of the Stackelberg model. Another strategy has been the profiling of suspected individuals; however, this compromises the basic principles of an open society. Bier [3], suggested identifying components in the default tree that were most often employed by the terrorists and developing defenses around these components in all possible settings. Her argument is that reducing the same components in all targets reduces the options of the terrorists and results in more accurate estimates of the probabilities available to the terrorist when planning an attack. The point is that subjective probabilities of terrorists' strategies can be determined based on an analysis of relative risks, upgraded through Bayes theorem as new information becomes available, and tested through simulations.

The formation of the model begins by identifying all possible targets, n, terrorists might attack. A fault tree is then developed for each target with the goal of finding the best defense system in terms of the probability of effectiveness and cost of implementation. Next, the defender identifies all strategies, m, suggested for defending the potential targets.In each of the n by m cells are 2 numbers: the expected loss for each target given that it is attacked, and the expected loss for each target given that it is attacked and protected by a specific strategy. A preferred strategy is the one that minimizes the maximum expected loss.

Examples: Simple Default Tree: Early Warning System for the West Nile Virus

An outbreak [4] of West Nile Virus occurred in New York City in 1999. The problem was to find the carriers of the virus and take appropriate action.Based on laboratory studies, it was believed that the virus was carried by birds and mosquitos. Because of the time and costs involved, it was not practical to randomly collect potential

carriers and run laboratory tests for the presence of the virus. Instead, data were collected in a stepwise process.

- Collect all non-pigeon dead birds over a 7 day period
- Identify areas of large cluster of dead birds
- Restrict the search to areas where at least one human infection was identified
- Test birds in these areas for the presence of the virus
- Initiate a larvae control program in the areas where positive results were obtained

The strategy was considered successful as measured by the reduction of the number of new reported West Nile cases while minimizing the population's exposure to the toxins injected into the atmosphere to kill the larvae.

Bioterrorism in Subways and Water Distribution Networks

A subway system is an attractive target for terrorists. The stations are relatively small constrained areas overflowing with passengers, especially during rush hours. Further, they move large numbers of people quickly over large distances making them ideal for a bioterrorist attack because of the ease with which the passengers could be used to spread a contaminate. A preemptive strategy might include random scheduling uniform and non-uniform police to different stations, to install sensors in areas that have the highest traffic density especially at certain times (rush hour, school dismissal, etc.), and mount recognizable time cameras. Additional preemptive strategies that are effective in attacks like the release of sarin gas in the Japanese subway station require emergency carts that can be rushed to the point of attack.

A potential attack from a terrorist who releases a pathogen into the environment is best defended based on the output from Stackelberg model, especially if many sites such as subways, other transportation centers, and water distribution networks are prime targets. In these cases where there is limited data at best, syndromic data are often useful.These data are collected by healthcare officials, who are looking for spikes in the data. Data often used are:

- Absences at work/schools
- Locations of schools
- Sales in over the counter pharmaceutical products
- Increased visits to hospital emergency rooms
- Look for common complaints/symptoms
- Monitor the environment
- Bring antidotes to be distributed in the suspected locations

The constraints include addressing the disease as soon as possible without responding to a false positive warning signal.

Conclusion

Terrorists' objectives, targets, and strategies are many and they have the advantage of deciding when and how to attack. The defenders have limited resources, too few to protect all potential targets. The strength of the defender is the intensity available to the defender when attacking the terrorist. But this can be a two headed sword.Although killing terrorists reduce their numbers, an intense attack, especially one that kills innocent people, can also be a recruiting tool for terrorists. The goal of this paper is to present preemptive strategies that improve the probabilities of the defenders to protect themselves by minimizing potential loses.

References:

1. Melnick EL, Everitt BS (2008) Articles on Homeland Security, Encyclopedia of Quantitative Risk Analysis and Assessment, John Wiley and Sons, USA.
2. Korzhyk D, Yin Z, Kiekintveld C, Contizer V, Tambe M (2011) Stackelbergvs Nash in Security Games: Interchangeability, Equivalence, and Uniqueness, J Art Intel Res 41: 297-327.
3. Bier V (2006) Game-Theoretic and Reliability Methods in Counter – Terrorism and Security, Statistical Methods in Counter terrorism, Master File for Review, Create research archive, USA.
4. Mostashari F, Kulldorf M, Hartman J, Miller J, Kulasekera V (2003) Dead Bird Clusters as an Early Warning System for West Nile Virus Activity, Emerg Infect Dis 9: 641-646.