

EDITORIAL

The Terror of the “Black Box”

Michael R. Powers*

“Though there be no such thing as *chance* in the world; our ignorance of the real cause of any event has the same influence on the understanding, and begets a like species of belief or opinion.”

– David Hume (“Of Probability,” *An Enquiry Concerning Human Understanding*, 1748)

Random variables are mathematical constructs designed to represent “unknown quantities.” Although they can be drawn from an infinite number of probability distributions, one random variable is conceptually very similar to another in that each is characterized by two properties: (1) a sample space of possible values, and (2) a distribution function describing the relative likelihoods of these values.

Unknown quantities, on the other hand, form a class of objects that are conceptually more heterogeneous and mysterious. This is because the characteristics that restrict our knowledge of these quantities – i.e., the barriers, or “black boxes,” interposing themselves between us and the unknowns – can take on any number of a vast array of forms.

These black boxes range from the common to the rarefied, and include epistemological obstacles imposed by nature itself (e.g., time, distance, and even quantum uncertainty), as well as impediments imposed by our human limitations (e.g., resource restrictions, technological inadequacies, political expediencies, and psychological inhibitions). When the unknown quantity constitutes a risk, it is the job of the risk analyst/statistician to collect and analyze data regarding the unknown quantity (*qua* random variable) that may leak from the black box.^[1]

For most common risks – fire, disease, natural catastrophe, economic outlook, etc. – time is usually the most salient and insuperable barrier (i.e., we are substantially barred from

* Editor, *Journal of Risk Finance*; Professor and Director, Advanta Center for Financial Services Studies, The Fox School, Temple University; e-mail: michael.powers@temple.edu.

knowing about an event that has not yet occurred). However, it would be wrong to assume that time is *always* a barrier. For example, epidemiologists preparing for an international outbreak of a particularly pernicious disease (e.g., SARS, plague, Marburg virus, etc.) may find that the only black box obscuring knowledge of a *past* outbreak is the refusal of local governments to provide complete information.

Certainly, no category of risk is enshrouded by a denser and more opaque black box than the threat of terrorism. Like most risks, the terrorist attack lies in the future, and so is subject to time as a natural barrier. However, in addition to time, there are also frustrating inabilities to fathom (1) the activities of the complex networks of terrorists, (2) the terrorists' socio-psychological motives and objectives, and (3) the broad range of methods of attack that the terrorists are free to choose on a seemingly *ad hoc* basis.

Despite these difficulties, it *is* possible to transfer or finance losses associated with terrorism risk. In the United States, private insurance markets for this type of risk existed before the events of September 11, 2001, and they exist today, albeit with government support under TRIA. Even without government support, however, markets for terrorism risk would exist as long as insurers believed that total losses (in dollars and lives) could be forecast with sufficient accuracy.

Central to this requirement is that the underlying frequency and severity of terrorism losses not be perceived as fluctuating wantonly over time. To this end, the current state of risk-financing has been assisted by two significant developments: (1) the lack of a substantial post-September 11 increase in the frequency of major terrorist attacks (outside of delimited war-zones), and (2) the emergence of sophisticated models for forecasting terrorism losses by commercial risk analysts^[2] that, for the moment, afford market experts a degree of comfort in the statistical forecasts.

Extending a model proposed by John Major (2002) in a previous issue of this journal, the probability of a successful terrorist attack on a particular target, i , may be expressed as

$$\Pr\{\text{Successful Attack at Target } i\} = p_1 p_2 p_3 p_4, \quad (1)$$

where:

$$p_1 = \Pr\{\text{Attack Is Planned}\},$$

$$p_2 = \Pr\{i \text{ Is Selected for Attack} | \text{Attack Is Planned}\},$$

$$p_3 = \Pr\{\text{Attack Is Undetected} | \text{Attack Is Planned} \cap i \text{ Is Selected for Attack}\}, \text{ and}$$

$$p_4 = \Pr\{\text{Attack Is Successful} | \text{Attack Is Planned} \cap i \text{ Is Selected for Attack} \\ \cap \text{Attack Is Undetected}\}.$$

The first of the four probabilities on the right-hand side of equation (1), p_1 , is essentially the underlying probability of terrorist action during a given time period. In the commercial risk analyst's model, this probability is generally captured by an overall "outlook" analysis for a particular future time period. Unfortunately, the other – and more complex – probabilities are not handled so transparently. In fact, one could reasonably say that the methods used to calculate p_2 , p_3 , and p_4 are buried within their own "black boxes."

Essentially, the commercial risk analyst develops estimates of these last three probabilities by intricate processes combining the judgmental forecasts of terrorism/security experts with the results of complex mathematical models. In some cases, the risk analyst may employ techniques from non-cooperative game theory along the lines of Major's work. Regrettably, the largest parts of these estimation techniques remain unpublished and untested, ostensibly because of "proprietary" concerns.

But is it really a fear of losing the competitive edge that motivates this reticence? Or is it perhaps a fear that opening the black boxes to public scrutiny will undermine confidence in the statistical forecasts themselves?

In a global economic culture that praises the virtue of transparency, it is rather unsettling that both rating agencies and regulators routinely countenance the use of unseen and unproved mathematical methods. Can one seriously imagine a modern patient going to the doctor for an annual check-up and accepting a diagnosis based upon a battery of secret, “proprietary” tests?

Unless the black boxes obscuring terrorism forecasts are removed, and the market’s confidence justified for the long term, only one thing is clear: The next major terrorist attack will not only damage its intended target, but also destroy the private market for terrorism coverage.

Reference

Major, J. A. (2002), “Advanced techniques for modeling terrorism risk,” *Journal of Risk Finance*, Vol. 4, No. 1, pp. 15-24.

[¹] Interestingly, statisticians have their own private black box to contend with – the Cramer-Rao Inequality, which places a limit on the amount of information that can be “squeezed” from any collection of data.

[²] The largest commercial risk analysis firms include Risk Management Solutions (RMS), Applied Insurance Research (AIR), and Eqecat (EQE).