A Threat-Response Model of Counter-Terrorism: Implications for Information Security and Infrastructure Risks

William C. Wood, Department of Economics, James Madison University, Harrisonburg, VA, USA

J. Brian O’Roark, Department of Economics and Legal Studies, Robert Morris University, Pittsburgh, PA, USA

Lauren M. DeLaCruz, James Madison University, Harrisonburg, VA, USA

ABSTRACT

This paper critically reviews the literature and best practices to develop and apply a qualitative model for managing terrorism threats. The research shows how risk is too complicated to be reduced to a binary system of safe and unsafe attributes. The researchers show how uncertainty can be reduced through the application of resources, by using a protection profile. The second component in the model is a damage profile, which shows how, as security increases, the additional value of more security decreases. When this relationship is adjusted for the costs of security (reflected in the protection profile), the result is an equilibrium showing an economically-rationalized level of security but generally short of complete safety. The model is then simulated to show how the equilibrium is shifted by such factors as an increase in vulnerability or consequences, a more effective adversary, changed costs and advances in technology. Although an equilibrium model with known functions is useful, a number of real-world limitations prevent straightforward application of the model to calculate a security equilibrium. These limitations include discontinuous risks and distributed decision-making authority. Finally, the model is analyzed to estimate the likely effects of litigation and security mandates on counter-terrorism.

Keywords: Counter-Terrorism, Information Security, Infrastructure Security, Risk, Terrorism

INTRODUCTION

In a world of uncertainty, security is very much on people’s minds. Given the constant threats to lives and property, especially critical infrastructure, these are pragmatic concerns, yet security itself can be imperfect and uncertain. Terrorist attacks, and sweeping programs to prevent them, highlight the tradeoffs between economically balancing security and privacy.

The political system, however, invites people to ignore or deny these tradeoffs (Michaels, 2013). Some politicians demand assurances of safety, as though safety were an all-or-nothing quality of complex systems. Other politicians get elected by saying they will do everything
possible to promote security, even though we know that literally it does not make sense to do everything possible. For example, the government could ban all sales of nitrogen fertilizers (Bartlett, 2004) because of their potential diversion to bomb-making uses.

This is not only unlikely, but also impractical because of the impact on agriculture and food production. Still, leaving nitrogen fertilizers on the market means that not everything possible has been done to increase security. Scarcity forces a society to have less than the unconstrained optimum of many goods and services, and security is no different.

Statement of the Problem

Little progress can be made in having informed discussions about security as long as security is presented as a binary condition, safe or unsafe. This paper presents a qualitative model to promote thought about security, how it is achieved, and how much of it is worthwhile. As public understanding of the true nature of security grows, at some point public figures will be able to speak in much more realistic terms.

The Nature of Security

Security is different from many other products and services. A manufacturing firm makes its money by selling a good, but the security with which it operates is often an afterthought at best. When firms increase their security, the positive costs often offset the usually unobserved benefits.

Therefore, security can become a casualty of the bottom line. If security is working well, then a firm has a very low probability of experiencing the adverse events it is guarding against. However, when security works best, it is often taken for granted by managements and customers alike, who may only observe a higher cost or price tag.

The output of a security system is not easy to characterize, but it can be summed up in a distribution of losses by examining combinations of probabilities and consequences. More security means, in some sense, a smaller distribution of probabilities and consequences.

Expected value can be used to make these comparisons by simply multiplying the probability of an event occurring by the size of the loss. In a very simple example where there is a 1/10 chance of a security breach properly valued at $1000, the expected value of the damage is $100 (1/10 x $1000). A risk-neutral decision-maker would be willing to spend up to $100 to prevent the breach.

In theory it would be simple to multiply each adverse event’s probability times its consequences, getting an expected value to be summed over all possible events. However, such a computation would be misleading, for reasons examined later in this paper.

For now, security can be taken to be a continuous variable with higher and lower amounts understood by participants even if it is not precisely quantified. Regardless of how we choose to measure the output of a security system, it is clear that no system can simply be declared safe or not safe.

Methodology

The authors critically review the counter terrorism literature and best-practices to inform the development of an improved risk management security model. An equilibrium model is constructed, based on two fundamental functional components: a protection profile showing the costs of achieving security against terrorism, and a damage profile showing the benefits of varying levels of security.

The Protection Profile

The beginning of a model of security rests in an organization’s preparation. The organization knows much more about its preparedness and its costs than it knows about potential threats. Thus we begin forming our model as illustrated in Figure 1.

Here, the horizontal axis represents a continuously adjustable level of security. At the left, there is only a basic level of security. From there, additional measures such as securing gates to facilities and changing computer passwords regularly can add significantly to security as low cost.
Computer Security Practices and Perceptions of the Next Generation of Corporate Computer Users
www.igi-global.com/chapter/computer-security-practices-perceptions-next/45815?camid=4v1a

On Access-Unrestricted Data Anonymity and Privacy Inference Disclosure Control
www.igi-global.com/article/access-unrestricted-data-anonymity-privacy/2490?camid=4v1a