# Chapter 7.13
# Simulating Complexity-Based Ethics for Crucial Decision Making in Counter Terrorism

**Cecilia Andrews**
*University of New South Wales, Australia*

**Edward Lewis**
*University of New South Wales, Australia*

## ABSTRACT

*"Counter-terrorism refers to the practices, tactics and strategies that governments, militaries and other groups adopt in order to fight terrorism." Counter Terrorism (CT) is a complex system driven by political, stress and time pressures that contribute to the enormous difficulty that involved people face in making sustainable ethical decisions. This chapter proposes a systems planning approach for enhancing the sustainability of crucial ethical decisions in CT. First, we describe the need for enhancing crucial ethical decision-making using some recent cases. Next, we evaluate the relevance and utility of a systems planning approach in providing such enhancements for CT. We develop the "ideal state" for tools and techniques to be used for crucial ethical decision-making in CT. We propose the POWER systems planning framework as a model for advancing towards this ideal state Finally, we consider how games and simulation could be used to envision and inform, aid synthesis of and support evaluation of decision-making through the POWER model.*

## INTRODUCTION

Ethics and values form the basis for the evolution of systems in society, such as military, information, political, control, economic and cultural. Values, along with moral strategies and agents (people), form Belief Systems. The conflict between different Belief Systems is the real battlefield of terrorism, and if we can understand this conflict, then we can counter terrorism more effectively.

This chapter considers CT as risk management within a complex, adaptive systems model. CT is

about determining terrorist risk and evaluating options for the mitigation of that risk. However, CT approaches commonly focus on the consequence of the risk to particular assets—those things that could be targeted by terrorists—rather than what conditions fertilize the growth of that risk and the motive for identification of those targets. If we understand these conditions influencing the risk, then we might be more successful in countering terrorism.

The potential for risk can emerge from a combination of Belief Systems, involving factors like individual disenfranchisement and group compliance. Social psychological literature provides tools and insights into risk potential, both at the individual and group level (Pynchon & Borum, 1999). Group attitudes and opinions, group decision-making, motivations to group action and diffusion of individual responsibility in a group context all contribute to the development of a Belief System. Examples of the formation of Belief Systems include the unity of purpose in the faithful that can help overcome uncertainties in their environment that threaten individual existence (Bloom, 1999). The Belief Systems of closed groups can enable these groups to be led into violence.

How can we come to understand the very embedded and complex nature of belief in societies? Complex systems may give us the tools we need.

Complex systems can use systems dynamics and other systems modeling techniques to develop a picture of the influences and pressures on individuals within groups to inform intelligence on key agents and drivers in operations. An example of the use of complex systems includes the Social Network Analysis (SNA) of the 9-11 Terrorist Network undertaken by Krebs (2004) from public domain information. These kinds of analyses are interesting to develop a picture of who, what and where terrorist cells are developing, but they do not provide information on why. An understanding of Belief Systems might give us the insight into "why" that we can use for the effective risk management of terrorism.

If we can develop models that help to identify those pervasive and persistent patterns of Belief Systems that evolve into terrorist motives, we can provide counter measures well before risk potential develops into risk reality. As well, such models can help us to develop war games that can be used to understand or train for the complex interactions within the terrorism problem (Smith, 2002).

## RISK MANAGEMENT IN COUNTER TERRORISM

A number of components exist for a risk analysis of terrorist threats across a number of models. The higher order components are Intent and Capability. Intent comprises motive or desire, objectives (purpose) and expectance. Capability comprises technical, knowledge, methods, social factors (such as group and organization), resources and skills (Holliss, 2002). Risk analyses are made at both the strategic and tactical level as to the likelihood and impact of a threat being realized, given intelligence factors derived from Intent and Capability.

When it comes to terrorism, Intent is the key factor in deciding the nature of the threat. Intent of points of view is embedded in the very definitions of terrorism (ASIO Act Amendment Bill, 2002; Hocking, 2003; Wikipedia, 2004). Terrorism is not something defined by its process, or even its agents and their knowledge or resources, but it is violence defined by its purpose. It is a conflict rooted in belief—whether political, religious, economic or social.

The success of terrorism and any model that purports to simulate terrorism should be measured in terms of social outrage. High-impact, high social-outrage events are "successful" terrorist events. The terrorists' motive is not personal gain, but intent to cause social outrage through a