Chapter II
Knowledge Management, Terrorism, and Cyber Terrorism

Gil Ariely
Interdisciplinary Center Herzliya, Israel

ABSTRACT

This chapter applies the conceptual framework of knowledge management (and vehicles familiar from that discipline) to analyze various aspects of knowledge as a resource for terrorist-organizations, and for confronting them, in the post-modern era. Terrorism is a societal phenomenon, closely integrated with changes in our knowledge society. Terrorist organizations became knowledge-centric, networked organizations, with a post-modern approach to organizational paradigms. Cyberspace is habitat for knowledge and information, and terrorists are knowledge-workers proficient in it. Cyber terrorism is the convergence of cyberspace and terrorism, and is closely entwined with "nonvirtual" terrorist activities and global terrorism. IT allows terrorists similar societal power-shift - from large organizations to small groups and individuals. The chapter reviews the changing nature of terrorism towards postmodern terrorism and towards "learning terrorist organizations" implementing knowledge, cyber terrorism and cyberplanning. Since it takes a network to beat a network, the chapter discusses knowledge and knowledge management (KM) in counterterrorism. Through 'NetWar,' conducted also in cyberspace (not necessarily aimed at the IT systems it uses as a platform—but rather at human lives), implementing familiar vehicles from the KM toolkit such as social network analysis (SNA), to KM in intelligence and KM in low intensity conflicts. Knowledge management proves salient both for terrorism and for countering it in a knowledge society.

INTRODUCTION

Terrorist organizations are going through fundamental changes that other organizations went through in the postindustrial age, as Mcluhan (1960) and Toffler (1970) predicted. Many of these changes are derived from implementation and management of knowledge and innovation, towards devastating action and effective knowledge centric networks. This understanding is the key to confront them, since terrorism is a soci-

etal phenomenon, and as such is closely integrated with changes in our knowledge society. Terrorists themselves are *knowledge-workers*, with the skills and abilities to leverage technology and information technology (IT) towards their goals.

Thus, *cyber terrorism* goes beyond the phenomenon of implementing IT to interfere with other IT systems (harmful as it may be) that is widely covered in other chapters in this book. Cyber terrorism is the convergence of cyberspace and terrorism, and is closely entwined with "nonvirtual" terrorist activities and global terrorism. Cyberspace and IT allows the terrorists the same advantages that the postindustrial (or postmodern) information era allows any knowledge-worker, and any global (or "virtual") organization. The societal power-shift from large organizations to small groups and individuals gives the terrorist the ability to maximize their ability to communicate, collect intelligence, learn, plan, and inflict terror through a network of operatives and cells. It expands the concept of cyber terrorism: cyberspace as an infrastructure to support terrorism that is nonrelated to IT.

BACKGROUND

Knowledge is acknowledged as a resource by terrorists in manifest. Stewart (1997, p. ix) in his seminal book on intellectual capital, refers to "Knowledge as a thermonuclear weapon." Undeniably it has become so for terrorists in the information age. As the events of September 11, 2001 have proven, more efficient than any bomb is the knowledge which incorporates skills (such as flight) and competences, original and creative thinking, some understanding of engineering, learning, and integration of many context insights (Ariely, 2003), such as effect on communication and economy (Hoffman, 2003a). The smartest bomb that fighting forces ever invented, is the human one—the only bomb that adapts to a changing situation (in addition to being "preprogrammed"), charging a psychological price too.

And it is Stewart (2001) who mentioned Al-Qaida's networked organizational structures and knowledge-based operations, vs. the difficulties of hierarchies in the large organizations confronting it. Knowledge and information are intangibles, for which IT and the cyber arena are natural habitat. Smuggling tangibles (like a bomb) is more difficult than sending instructions over the Web or posting a lesson online.

THE CHANGING NATURE OF TERRORISM

Postmodern Terrorism

Insight into this new nature of terrorism shows it is no longer an agent of change through "proxies" and secondary mediums (such as public opinion or decision makers), but rather a devastating instrument able to cause direct change, effecting 1,000s and even whole populations.

The most sophisticated weapons (WMDs) are implemented (through highly technical knowledge) vs. the most sophisticated usage of the most primitive weapons (Ganor, 2001b). Suicide bombers become precision weapons (WMDs), through knowledge and innovation.

The Economic Jihad

Furthermore, new forms and dimensions of global terrorism implement *economic knowledge* both for internal conduct and for economic effect in the globalization era.

Research work in the last few years analyzing Al-Qaida documents (Fighel & Kehati, 2002), shows understanding of economic knowledge implemented explicitly towards an "economic Jihad." The Al-Qaida author confirms:

that the attack against the Twin Towers (September 2001) and against the French oil tanker (October 2002) are part of the economic Jihad. These attacks are meant to signal to the West under US leadership, that this type of Jihad, if it continues, will bring upon the West an economic holocaust. (Fighel & Kehati, 2002)