Chapter 7.17
Security Implications for Management from the Onset of Information Terrorism

Ken Webb
Webb Knowledge Services, Australia

ABSTRACT

This chapter results from a qualitative research study finding that a heightened risk for management has emerged from a new security environment that is increasingly spawning asymmetric forms of Information Warfare. In particular, there is evidence that after recent terrorist events there has been a lift in security across the world and identification of terrorists now able to conduct Information Warfare. Also concerning is that, over the years, there have been many interpretations of what constitutes this threat. Therefore, after extensively reviewing literature mainly on Information Warfare and Terrorism, this chapter defines for readers what the threat of Information Terrorism is and the new dynamic security environment that it has created. Security implications for management have subsequently evolved, as they are now required to think about the philosophical considerations emerging from this increasing threat, and these are outlined and form the basis for future thinking.

INTRODUCTION

The objective of this chapter, so appropriate guidance for future thinking occurs, is to inform readers about Information Terrorism and the adjudged security implications for management from its onset. This occurs by:

1. Defining the Information Terrorism threat;
2. Describing the new security environment and the sub-environments forming it; and
3. Providing a high-level discussion from an information security perspective of the emergent philosophical considerations for management generally.

DOI: 10.4018/978-1-60566-326-5.ch005

This is needed because a new set of security dynamics that influence the decision-making process faces society today. For example, at the strategic level, gone is the 20th Century security paradigm that helped form geographically based continental strategy. The traditional international system that links sovereignty to Westphalian-style territorial nation states is under pressure from the new age of globalisation and the 'information revolution' (Evans, 2003).

Some argue that the major strategic change required now is a transition away from a dominant state-centric structure towards that marked by a greater number of non-, sub- and trans-state actors. This influence has devolved down to all levels of society (Hall, 2003).

More specifically, Colarik (2006) confirms that being in this information-dependent age has increased the frequency and potential magnitude of Information Warfare. This is because parties that normally rely upon physical violence, irrespective of their disposition, are now more able to conduct information operations in a myriad of forms. The relative unknown knowledge of this aspect and current perpetrators, alongwith the complexity of information and communications in the global environment, provides a real problem for management.

Also worth considering is that many forms of critical infrastructure assets for society are now information dependent and non-physical. They are invisible to the untrained observer, or difficult to define or harness. Complicating this is that, due to their diversity and complexity, stakeholders throughout the world have not universally accepted a standard definition of critical information infrastructures, let alone standardising the protection of them. This has contributed to government authorities and academia making many attempts to define critical information infrastructures and introducing such issues as technology leadership, quality of service, network centric operations, privacy and other emerging considerations (Barker *et al*, 2006).

Furthermore, Barker *et al* (2006) explain that to date there are no consistent approaches to the forms of reporting and/or evaluation of critical information infrastructures. It means different things to different people, and this perspective issue is part of the described problem.

These observations imply that Information Warfare is now intangible by nature. It impedes the general ability for traditional parties to understand and manage it, as contemporary forces of influence not necessarily contingent on traditional thinking now exist. This means that a clearer understanding for management of the implications from this onset of Information Warfare and the conduct of it by terrorist groups, thus Information Terrorism, is required. Managers dealing with this need to now take a much more expansive and philosophical approach, as there is a range of new environments reflecting these dynamics that are contributing to a new security atmosphere.

Worth considering as part of the managerial approach for dealing with the new security environment, as it applies to Information Terrorism, are three relevant and deep philosophical considerations that congruously interrelate and influence each other. These, as explained later in the chapter, are:

- Change in the direction of thinking,
- Culture, and
- Group dynamics.

They have emerged from the changed Information Warfare environment and form the basis of the implications for management.

BACKGROUND

During the years 2003 to 2007, a doctoral research project conducted by the Author, which used Australia as the case study, investigated how to enhance national security from terrorist groups conducting Information Warfare. This project