Chapter 7
Concerns About What Will Happen Next:
Should These Things Keep You Awake at Night?

Eduardo Gelbstein
Webster University, Switzerland

ABSTRACT

The rate of innovation and adoption of information technologies continues to accelerate and each development brings with it unknown side effects and unintended consequences. Cybercrime continues to become smarter and the ubiquity of such technologies together with easy worldwide connectivity means that if only one in a million individuals chooses to act with malicious intent there is a population of 6 million potential attackers.

This chapter discusses vulnerabilities that should be considered by decision makers as they could be seen as the soft underbelly of a society that has an irreversible and deep reliance on information technologies.

1. LIKELY FUTURE SECURITY CHALLENGES AND THE POTENTIAL FOR CYBERTERRORISM

I never think of the future, it comes soon enough (Attributed to Albert Einstein)

Prediction is very difficult, particularly about the future (Stated by Niels Bohr – original source uncertain (Mark Twain?))

DOI: 10.4018/978-1-61520-831-9.ch007

The poet Alexander Pope wrote "Hope springs eternal in the human breast". Whilst hope is good, it seems prudent to consider possible scenarios, anticipate trends and keep reviewing them as new information becomes available.

There are many sources of information on terrorism, security and related technologies. In addition, life imitates fiction as there are many works of fiction (and science-fiction) that seem to have given ideas for terrorist attacks or attempts, such as Tom Clancy's *Debt of Honor* (1995) in which

an airliner crashes into the US Congress, Mark Burnell's *The Rhythm Section* (2000) describing a plot to mix liquids and cause simultaneous explosions in several planes during flight and Michael Dobbs *The Edge of Madness* (2009) in which the UK is the subject of cyberattacks by another nation (China).

This chapter discusses the following topics:

- Continuing growth and innovation in the use of IT leading to increased dependency
- Software complexity and quality
- Fragmented data ownership and quality assurance
- Military strength malware, toxic payloads and combined attacks
- Potential consequences of outsourcing and offshoring
- Loss of management skills in IT operations and information security
- Too much information readily available to bad guys
- Executive detachment
- Organisational politics and turf battles
- The special case of public sector IT
- Justifying increased expenditures on information security and related disciplines
- The legal framework surrounding information security

2. GROWTH IN INNOVATION AND USE OF IT, LINKAGES AND DEPENDENCIES

Two basic laws established many years ago continue to apply: Moore's and Metcalfe's.

Gordon Moore, a co-founder of Intel showed, in a paper published in 1965, that the number of transistors that can be placed on an integrated circuit doubles every eighteen months. This has since been re-interpreted into a statement that computing power doubles every two years (known as Moore's Law). The trend is expected to continue for computer chips. (Moore, 1965).

Robert Metcalfe, one of the inventors of Ethernet, a networking technology, stated that "the value of a network grows as the square of the number of its users". This was first mentioned around 1980 (Shapiro & Varian, 1999). Unlike Moore's Law, Metcalfe's can't be quantified, because there are no standard tools for measuring value creating a reliance on *IKIWISI* (I'll Know It When I See It).

This law is mentioned in the paper "Network Centric Warfare" (1998) in which Vice-Admiral Cebrowski states that by 1998 the elements for such warfare model were in place and would have broad impact on military operations.

While in principle Metcalfe's Law has no limit for the size of the network or the number of devices or users connected to it, the authors of the article "Confronting the Limits of Networks" (2002) argue that the usefulness of networks will be limited by four factors:

- **Saturation:** When the network contains most of the valuable material that its members can contribute to it – it would be interesting to gain an insight into how much of the material currently posted on the Internet is actually "valuable" (and to whom) – YouTube and Flickr for example contain a mix of the "good, the bad and the ugly".
- **Cacophony:** When the interaction between members becomes to complex to follow – this is the case in internet forums where discussion threads involve hundreds of replies. The same holds true for a large number of the blogs currently posted – at the limit a blog by every person with access to the internet expressing personal opinions, biases (some of them extreme) and prejudices.
- **Clustering:** When members of a network split into groups that only use part of the network as happens with Special Interest Groups or services that require a subscription fee of which there is a substantial number.