Chapter 1
The Security Practitioners' Perspective

Eduardo Gelbstein
Webster University, Switzerland

ABSTRACT

This chapter reviews the assumptions on which this section of the book is based, explores the irreversible dependency of society on information and communications technologies, and sets the scene for the asymmetric nature of cyber-attacks, and lists the main the challenges facing security practitioners in the public and private sectors. These are discussed in more detail in subsequent chapters.

1. LESSONS FROM HISTORY

Those who cannot learn from history are doomed to repeat it. (George Santayana)

History is merely a list of surprises. It can only prepare us to be surprised yet again. (Kurt Vonnegut)

History tells us that human societies have been creative –from the invention of writing and numbers, the development of knowledge and science to the construction and deployment of many technologies.

There are many books about the destructive nature of the human species – from impacting the environment and causing other species to become extinct to many forms of war and terrorism throughout the ages.

At least four "species", however, have survived and continue to thrive despite massive efforts to control them if not eradicate them: cockroaches, rats, criminals and terrorists. The latter two have become adept at using various forms of electronic forms of attack.

Will there be a cyber-terrorist attack or even a cyber-war? Will civil society be disrupted? Many people have no doubts. For example, in May 1998, when addressing the U.S. Naval Academy in Annapolis, Maryland, President Bill Clinton said:

DOI: 10.4018/978-1-61520-831-9.ch001

Our security is challenged increasingly by non-traditional threats from adversaries, both old and new, not only hostile regimes, but also international criminals and terrorists who cannot defeat us in traditional theaters of battle, but search instead for new ways of attack by exploring new technologies and the world's increasing openness.

He then added *"...intentional attacks against our critical systems are already under way."* (Transcript, n.d.)

From this statement, not the only one of its kind in the last few years, it would seem that cyberwar has already started but has not yet caused such impact that it becomes instant global news. Other known attacks are discussed in Chapters 3 and 4.

President Clinton's statement also confirms that information security, in all its aspects, is not a technical problem. It is a problem caused by human action, and the only way to manage it is to apply one of the fundamental principles of Physics: a reaction of equal force in the opposite direction which also needs human action.

Attacks to information and communications technologies (ICT) have happened so many times that while they regularly make the news, they no longer come as a surprise.

2. ASSUMPTIONS MADE IN PREPARING THIS PART OF THE BOOK

This part of the book is based on eight assumptions – all of them discussed in this chapter:

1. Few activities in the developed and developing world are not touched by ICT;
2. The dependency on ICT is both strong and irreversible;
3. Information Security has been an issue for many years;
4. Attacks have been happening for many years;
5. Software is not perfect and systems are complex;
6. The seven myths of terrorism;
7. Technical innovation will continue at a rapid pace; and
8. Legislation to deal with the consequences of technical innovation emerges many years later.

Assumption 1: Few Activities Are Not Touched by ICT

The history of humanity is full of examples of tool makers from times before what we now describe as "civilization". These tools have changed the way humanity lives. At various times, cultural waves (Mesopotamia, Persia, China, India, Arabia, Europe, North America) went beyond tool-making to explore and explain how our world works, and Science joined Technology in our tool-making efforts.

Since ancient times, the knowledge and experience acquired in "tool making" was put to good use in all societies. It was also applied to the means through which to defend these societies and also to acquire other territories and societies: weapons. There is nothing that makes electronics and all its products different in this respect.

The virtual world of information encoded into an electromagnetic spectrum started in the mid-1800s: the first demonstration of an operating telegraph took place in 1844. In 2008, we lived with some 4.1 billion cellular telephones plus 1.3 million fixed line telephones worldwide (Measuring the information society, 2009), most of them capable of connecting to another telephone anywhere in the world.

There were also nearly 1.5 billion people with access to the Internet – an amazing growth given that the World Wide Web became a working concept as recently as 1990 and in addition, there is a profusion of other networks using copper wires, optical fibre networks, radio waves, microwaves and satellites that do not use the Internet Protocol.