Preface

INTRODUCTION

So many things come in sets of five. The five senses consisting of sight, hearing, touch, smell, and taste; the five elements consisting of water, earth, air, fire and ether; and even the Lorenz cipher machine that uses two sets of five wheels that generate the element obscuring characters—these are but a few examples of independent items that merge together to create a genre of function. Let us now take a look at a number of factors, which on their face value may seem to be totally independent but together create something worth contemplating.

Factor 1

In mid-1960s a group of scientists called the "Rome Club" published a report, which at that time was read and commented on widely around the world. This report was the result of analysis of computer-based models aimed at forecasting the developments of our civilization. The overall conclusions were dim. In the 21st century, human civilization would start facing major difficulties resulting from the depletion of natural resources. The conclusions of the report were discussed and rejected by many at that time. However, without any doubt the Rome Report was the first document trying to address the impact of our civilization on the natural environment.

Factor 2

At the end of the 20th century, the whole world was fascinated with the Y2K computer bug. Due to the limited space used for storing a date in computer records of legacy systems, it was discovered that switching from the year 1999 to 2000 may result in software failures. These failures then may trigger chain reactions due to the fact that computers drive public utility systems (i.e., power supply, water, telecommunications, etc.). As a matter of fact, some people went so far as to hoard food and other supplies to avoid any possible society-wide disturbances that may result. The information technology sector responded with mass action aimed at tracing all possible systems that could generate problems during the switch to a new millennium. As a result, no significant accidents occurred at that time around the world. Interestingly, some mass media outlets clearly were disappointed that nothing had happen.

Factor 3

Telecommunication networks come in many forms; whether they are for the use of businesses, governments, social organizations, and/or individuals, they have great value for improving people's lives. A network is essentially the connecting of two or more entities with the ability to communicate. Utilizing a multitude of telecommunication technologies, such as the Public Switched Telephone Network (PSTN), Public Switched Data Network (PSDN), Cable Television (CATV) network, and orbiting satellite networks (i.e., commercial and military), people from around the globe can communicate and share information virtually in an instant. The real-time services that this infrastructure provides include regular telephone calls, videoconferencing, voice over Internet protocol (VOIP),

and a host of other analog, digital, and multimedia communications. Connecting these networked systems and facilitating their communications are high-speed switches, routers, gateways, and data communication servers. Combined, these technologies and infrastructures comprise the global information infrastructure, which is primarily used for the sharing of information and data. This infrastructure serves communications between communities, businesses, industrial and distribution interests, medical and emergency services, military operations and support functions, as well as air and sea traffic control systems. The global information infrastructure sustains our westernized economic and military superiority as well as facilitating our shared knowledge and culture.

It provides national, international and global connectivity through a vast array of systems. The services overlay that facilitate voice and data transfers support the globalization of western values, business, and cultural transfers by creating a smaller, highly responsive communication space to operate and interact with any interested participants. All of this is facilitated by the massive network of servers known as the Internet, and managed by thousands of organizations and millions of individuals. The global information infrastructure is utilized to improve organizations' and individuals' respective efficiencies, coordination and communication efforts, and share and consolidate critical data for maintaining ongoing efforts. This is why such an infrastructure is so important to our western way of life, and also why it is a viable target for those seeking to assert their influence and agendas on the rest of humanity.

Factor 4

Every year the Computer Security Institute, an organization based in San Francisco, California, produces, in cooperation with the FBI, a report called the CSI/FBI Computer Crime and Security Survey. It is a summary and analysis of answers received from more than 600 individuals from all over the United Stated representing all types of business organizations in terms of size and operation. This survey is known around the world as the most representative source of assessment of the security status of businesses. Some of the key findings from the 2006 survey were:

- Virus attacks continue to be the source of the greatest financial losses.
- Unauthorized access continues to be the second-greatest source of financial loss.
- Financial losses related to laptops (or mobile hardware) and theft of proprietary information (i.e., intellectual property) are third and fourth. These four categories account for more than 74% of financial losses.
- Unauthorized use of computer systems slightly decreased this year, according to respondents.
- The total dollar amount of financial losses resulting from security breaches had a substantial decrease this year, according to respondents. Although a large part of this drop was due to a decrease in the number of respondents able and willing to provide estimates of losses, the average amount of financial losses per respondent also decreased substantially this year.

The overall tone of the survey is optimistic. We, as a society, have put a curb on the rising wave of computer-based crime. The survey's findings confirm that.

Factor 5

The mass media reports everyday on terrorist attacks around the world. These attacks may be launched at any time in any place and country. The method of attack in the overwhelming majority of cases is the same: an individual or a group triggers an explosion at a target. It could be done remotely or in suicidal mode. The common dominator of these tragic events is that the attackers are representing only a small part of society and most of the victims are innocent people who just happen to be in the proximity of the explosion.

The important conclusions that may be drawn from these five factors:

- Lack of symptoms of certain phenomena does not imply that the phenomena do not exist. But if such a phenomenon may eventuate and would be damaging to us, we need to take preventive measures.

- All the technology that we have created could be used for the benefit of all of us, but also could be used as a tool of attack/destruction against all of us.
- Information technology, and networking in particular, is a marvel of 20th/21st-century civilization. It dramatically changes all aspects of human behavior. Information technology is beneficial for humanity but may also be (and is) used by individuals to pursue their own objectives against the interest of the majority of people.
- These jagged individuals have started creating significant damages to information technology applications and their respective infrastructures. To counter this new discipline, information/computer security emerged. At present, the efforts of security specialists have started to pay off, and the overall percentage of computer-based crime has leveled off.
- Currently, terrorism has become the most widespread form of violence for expressing public discontent. Thus far, terrorism has stayed within its traditional form of violence, but it has already begun to migrate into using computer technology and networks to launch such attacks. As in the case of Y2K, we need to build awareness among information technology professionals and people alike that terrorism based on the use of computers and networks is a real threat.

All of the above has laid the foundation to the discipline called cyber terrorism. So what are the objectives of cyber terrorism, or rather, why do we need to worry about it?

Because of the enormous efficiencies gained over the past 25 years due to the introduction of computers and telecommunications technologies, organizations have a vested interest to maintain and sustain their deployment regardless of any residual issues. The use of these systems and networks means that there now is a major concentration and centralization of information resources. Such a consolidation creates a major vulnerability to a host of attacks and exploitations. Over the past 35 years, electronic economic espionage has resulted in the theft of military and technological developments that have changed the balance of power and continue to threaten the safety and stability of the world. In 2005 alone, more than 93 million people in the United States were subjected to the potential of identity theft as a result of information breaches and poor information security. When viewed globally, organizations of all kinds are obviously doing something terribly wrong with the security of proprietary and personal information. This is why it is so important to re-energize the need to protect these systems and re-examine our underlying organizational processes that may contribute to future breaches. The emergence of cyber terrorism means that a new group of potential attackers on computers and telecommunications technologies may be added to “traditional” cyber criminals.

The use of technology has impacted society as well. Due to automation technologies, organizational processes are becoming similar around the world. Governments are sharing information and aligning legal frameworks to take advantage of these synergies. Businesses are operating in distributed structures internationally to expand global reach, as well as outsourcing services requiring the use of information to less expensive centers around the world. This has created an extended communication structure between functional units, vendors, and suppliers in order to maintain an efficient value chain of products and services. This facilitated the capabilities of attacking targets wherever they may be located.

Individuals now have access to a vast storage of information resources for the creation of new thought, ideas, and innovations. This includes technological as well as political ideas and innovations. Cultures are becoming closer through shared communications, and as a result are changing at faster rates than previously seen in recorded history. While these technologies have inherent benefits to unify disparate groups and nationalities, this is also creating ultra-minorities that may be inclined to engage in extremism in order to control these changes and compete in this unifying environment. The facilitation of the underlying technologies is also being utilized by these groups to form solidarity and global reach for those of similar mindset and means. Thus, the underlying infrastructures are allowing small groups of people to gain their own form of scales of economies. People and organizations are realizing that in order to be able to compete in a globally connected world, they must master the underlying infrastructure that supports this connectivity. Whether this is to gain access to the opportunities that lie ahead from its mastery or it is to undermine and/or destroy these opportunities for others is still an emerging issue we are all facing today and into the future. Therefore, the exploitation of its inherent strengths (i.e., communication and coordination of global activities, and intelligence gathering) and vulnerabilities (i.e., protocol weaknesses and people processes)

can be considered one of the primary sources of attacks today and in the future. This is why we cannot ignore the societal and organizational influences that create the motivations to commit cyber warfare and cyber terrorism in addition to the technological requirements to securing our systems and eliminating any inherent vulnerability.

This book a compilation of selected articles written by people who have answered the call to secure our organizational, national, and international information infrastructures. These authors have decided to come together for this project in order to put forth their thoughts and ideas so that others may benefit from their knowledge and experience. They are dedicated people from around the world who conduct research on information security, and develop and/or deploy a host of information security technologies in their respective fields and industries, and have brought forward a host of key issues that require greater attention and focus by all of us. It is our sincerest hope that the readings provided in our book will create new lines of thought and inspire people around the world to assist in improving the systems and processes we are all now dependent on for our sustained futures.

Following this prologue, there is a chapter *Introduction to Cyber Warfare and Cyber Terrorism* formulating an overview with basic definitions of cyber terrorism and information warfare. Basic recommendations on how to handle such attacks are also presented. The main part of the book follows, containing more detailed discussions of the topics mentioned in the first chapter and other relevant issues. The articles are grouped roughly following the content of the most known security standard ISO 17799, which is entitled "Code of practice for information security management." In each chapter, the reader will find two types of articles: summaries of a given method/technology or a report on a research in the related field. An epilogue is then presented to conclude the content.

The purpose of this book is to give a solid introduction to cyber warfare and cyber terrorism, as we understand it at the beginning of the 21st century. Our book is not a guide to handling issues related to these topics but rather a review of the related problems, issues, and presentations of the newest research in this field. Our main audience is information technology specialists and information security specialists wanting to get a first-hand brief on developments related to the handling of cyber warfare and cyber terrorism attacks.

AC & LJ