Preface

In today's world, we are becoming more connected by communications and information technologies than ever before. Telecommunication systems and computers have global reach, transmitting voice and data digitally across transnational borders. These systems support economic infrastructures such as the energy and transportation industries, as well as all kinds of commerce and governmental services. This global information infrastructure is the principle foundation for the current integration of economies, cultures, and societies that is taking place throughout the world. It allows for the free flow of thoughts, ideas, and life-changing events that are used in instilling a greater sense of freedom and open democratic processes to people around the world. Never before has there been so much access to so much information that is available in a moments notice. These prolific capabilities have not gone unnoticed by developed countries, nor have they failed to harness their economic benefits as a competitive advantage. They have also not gone unnoticed by Western adversaries.

Information systems technologies are being used to make our lives more efficient. Scales of economies are gained when inefficiencies and redundancies can be reduced through the proper application of information technology. However, such efficiencies have their consequences. Every day we depend more and more on interconnected systems such as telecommunications; electronic banking; global stock markets; international traffic systems; water supply purification and distribution systems; electrical, gas, and nuclear power production and distribution; radio and television; emergency services; and the

list goes on. All of these infrastructures utilize information systems to manage and distribute their services, and are the basis for creating large-scale economic efficiencies in modern societies. By creating and maintaining reliable core infrastructures, a society may then devote its energies towards higher levels of efficient production, further development of innovation, and progressive thought. When this is not the case, significant effort and resources are instead deployed to continual damage control and repair, and as such, further development is greatly diminished. In a paper written for the First Committee on Disarmament and International Security (UNISCA) in December of 2002, Jonas Böttler, from the Delegation of Canada, stated "The more developed a country is, the more it depends on the correct and safe work of all these systems. Any intrusion, manipulation, sabotage, disruption or even destruction on one of these networks or systems will have effects which go far beyond the affection of only the attacked system itself." Therefore, in order for developed societies to maintain their economic superiority, they must secure their underlying infrastructures. When vulnerability does exist, history has shown that competing forces will surely use it to their advantage and their opponent's disadvantage. It is for this reason that this book was written.

People and systems are vulnerable to the methods and processes they employ to get things done. This is because they learn to trust their underlying successes and apply this trust to future applications of their approach. There is a clear link between the elimination of trust and the instillment of fear. It has been proposed that the attacks of September 11th in 2001 (i.e., when the World Trade Towers were destroyed, the Pentagon was damaged, the flight over Pennsylvania was downed, and thousands perished) occurred as a result of asymmetric thinking on the part of the terrorist group al Qaeda. When an opponent is attacked at right angles to their traditional thinking methods, they become vulnerable and unprepared for what is to come. This is known as asymmetric warfare, and is becoming a terrorist's first choice of attack, given the opportunity. The use of jetliners as missiles never occurred to the passengers and civil defense authorities alike until it was too late. It was simply unimaginable, and this notion has played a significant role in traumatizing many who watched these horrific images. The application of the traditional applied in a radically nontraditional manner both seems to be unimaginable and frighteningly real when it happens, especially when it comes to technology. Those with the capability of asymmetric thinking have unforetold power to change and shape the future directly and indirectly through their actions. It is asymmetric thinking applied to technology that has become the countervailing power to the global information infrastructure's ability to enact social, cultural, and economic change.

Historically, power comes in many forms. It may be acquired through position, such as being the head of an organization. Power may be acquired through the application of someone's personality, such as charisma and leadership qualities. But ultimately, power is the ability to take action by employing position, personality, and the control of resources. With respect to terrorists and those combating terrorism, the amount of power through action is dependent on three basic factors. The first of these is knowledge of ones self, including ones abilities and short comings. For without such insights, any action taken may result in limited success, which may not be capable of being sustained. The second is knowledge of one's opponent, which includes their methods, strengths, and weaknesses. Doing battle without first understanding the capabilities of an opponent is reckless at best, and could be fatal at worst. The third is the control and application of resources that can amplify and focus one's abilities to act and/or compensate for one's shortcomings in taking action. Because westernized countries have such economic might, large amounts of resources can be brought to bear as a force amplifier while lessening any shortsightedness, or a lack of inherent aptitudes when confronting adversaries. This author leaves it to the reader to judge the political and military activities of their own respective countries. However, conflict between competing forces and the desire to have power over them is as old as civilization itself. The desire to grow stronger and create a more powerful position to enact change is ever present in an evolving world.

The adversaries that Western nations now face have shown a great aptitude and patience for developing their member's understanding of themselves through education, military, and religious rigors. They have demonstrated a desire to learn about their targets by studying their culture and methods while living amongst them. Many of the hijackers in the September 11th attacks had lived and studied in several Western countries in Europe and North America. In fact, many held advanced degrees in a range of technologies. These terrorists have demonstrated that they can now use our own knowledge and technology against us to create largescale damage using relatively small amounts of resources, and in doing so, turn our own methods and approaches against us. The real question at hand is what can we do to stop them?

It has been said that information is power. Information is one of the West's greatest strengths. We rely on it as a primary foundation for supporting our open, democratic processes. The dissemination of information provides citizens of democratic countries with the ability to stay informed about their government's activities (good and bad), and to make decisions on a collective basis for their own respective well-being and sustained futures. Accurate and

timely information provides a distinct competitive advantage in all aspects of living and governance. Information is, in fact, a commodity unto itself, as it is regularly packaged, traded, and sold around the globe, affecting monetary and commercial markets. As previously mentioned, the use of technologies that facilitate the sharing of information, societies, and economies are becoming closer, more familiar, and increasingly integrated, as their exposure to each other occurs more and more each day. As such, the global information infrastructure is both a tool for furthering Western ideals and ideologies, and is a facilitator and target for those forces seeking to diminish its influence and progress. Therefore, our reliance on the mechanisms, systems, and basic infrastructures that support the use of information is both subject to being used for violence, as well as being a target of violence. Everyday technologies used by hundreds of millions of people are now a new tool in the arsenal of terrorists, and this form of terrorism is known as cyber terrorism.

In the 1980s, it has been reported that the term cyber terrorism was defined by Barry Collin to represent the convergence of cyberspace and terrorism. Since that time, the term has continued to change in definition, and has had its scope expanded to the point where it has become a wholly subjective term that has lost its true focus (i.e., where true terror and cyberspace converge). Other prominent authors and governmental actors have offered their definitions, but most have lost the core connection to terrorism itself, and have instead disconnected the electronic world from the physical world. In fact, the term "terrorism" has been hijacked by self-interests seeking an expansion of their respective controls and power base by turning this term into a form of *fearism*. This book seeks to establish cyber terrorism as it is applied to the global information infrastructure and its use by terrorists for the creation of violence and not just fear. It has become commonplace to label an aggressive, nonviolent act as a form of terrorism, just as it has become commonplace for a major computer disruption to be labeled as an act of cyber terrorism. Such approaches diminish our ability to enact effective security measures and instill mature responses when such true terrorism occurs. With over 20 years of definitions, discussions, and debates over what cyber terrorism is and what we should do about it, it is now here and affects us all. It is now time to create a real awareness of the threat of cyber terrorism so we can mobilize and focus our efforts in creating a safer world dependent on using information technology.

The notion that terrorists are ignorant and unskilled needs to change. With the proliferation of the Internet, global reach by terrorists to potential target intelligence, and its dissemination amongst their members and affiliated groups is

now possible in near real time. This usage with the acquisition of additional skills affords them the opportunity to master the underlying technologies and infrastructures that may ultimately be used to cripple our own information infrastructure and facilitate future physical attacks against us. Accessing critical information remotely is but the tip of the iceberg. Because we rely on these systems to control utilities, govern financial institutions, utilize medical databases for healthcare, and logistical support for military operations, terrorists can institute widespread chaos as well as precision targeting through a host of technology-driven attack methods. These new technologically skilled terrorists are providing the information and communication support for terrorist operations. As their skills continue to increase (and they will), cyber terrorists will commence assaults on high-value targets through the interception of confidential communications, the modification of critical data resulting in physical harm, and the denial of resources in times of crisis used in conjunction with physical attacks.

This emerging domain will affect everyone as we are forced to change how we utilize surveillance techniques and apply personal countersurveillance techniques to everyday activities. Because terrorist groups such as al Qaeda have demonstrated that they are capable of thinking outside our mental boxes, the weapon of choice by the majority of governments and individuals must be good intelligence (i.e., information) on terrorist activities in order to prevent future attacks and preparing ourselves for any resulting consequences of such attacks. Privacy issues and the rights of individuals to self-govern their information will emerge as a result of poor intelligence and counterintelligence measures. In fact, if governments and organizations misapply these technologies, they may actually cause sympathy for those labeled as terrorists. It is this author's sincerest belief that if left unchecked, cyber terrorism will become the principle motivator for creating a culture of security in the Information Age. This book was written to help create an awareness of the problem, and its primary contributions to the domain of cyber terrorism consist of:

- The role of information technology in terrorism (Chapter I),
- Identifies the various forms of traditional terrorism taking place in today's world as a foundation for its broad usage of cyberspace (Chapter II),
- Outlines and identifies a simple progression from hacker, cracker, cyber criminal to cyber terrorist (Chapter III),
- Offers a focused definition of cyber terrorism that is strongly attached to terrorism (Chapter III),

- Identifies the foundational components of the global information infrastructure and many of its core security services, mechanisms, and protocols (Chapter IV),
- Pinpoints many of the current modes of electronic attack and corresponding vulnerabilities (Chapter V),
- Puts forward a host of attack scenarios for key economic sectors and individuals (Chapter VI), and
- Proposes simple, preventative ideas designed to resolve many of the core issues to securing the global information infrastructure from cyber terrorists and cyber criminals alike (Chapter VII).

In short, it is the usage of technology, and in particular the global information infrastructure, by which terrorists communicate, coordinate, and facilitate their initiatives, that this book addresses. It is a *brief*, designed to provide an overview of terrorist activities, and their evolving use of information technologies. This book also provides the needed simplified details of our dependence on information systems to begin a common dialog between all stakeholders for creating rational initiatives. Finally, this book aims to propose ideas that address many of the larger issues governing the protection of data and information, rather than detailed solutions to any particular security area.