Preface

Over the last ten years there have been many books on information security, cybercrime, information warfare, and terrorism using electronic means introducing terms such as “cyber-terrorism”, “economic terrorism” and “economic jihad”. Their authors came from different backgrounds: academia, defense establishments, the legal profession and others, and this is reflected in the focus of these books.

Information and communications technologies continue to evolve rapidly and have a rate of adoption that is faster than all previous technologies in history, (e.g. the telegraph, radio, television).

The current reliance on a relatively small number of standards makes it easier for attackers to concentrate on their weaknesses, as no technology is perfect and these weaknesses (vulnerabilities) can be exploited in many ways. These standards are both de jure, such as the standards that underpin the operation of the Internet, and de facto, as is the case with personal computers using microprocessor technology from a dominant vendor (Intel) and an operating system from another vendor (Microsoft), and the growing adoption of Open Source software with its detailed documentation in the public domain.

The perceived benefits of innovation lead organizations to adopt emerging technologies such as wireless networks, virtualization of servers and other computers and computing clouds which, being new, have as yet unknown weaknesses, side effects and consequences. These will be discovered gradually over time, and until these are fixed, imply an unknown risk to their users.

Legislation advances at a much slower rate, and this has created (not for the first time) an environment where new forms of crime are developed without actually being a “crime” in the legal sense.

Cybercrime has become a major global “business”, and while discussions about the need for an international legal framework began at an OECD meeting in the early 1980s, it was only in 2004 that the Council of Europe Convention on Cybercrime entered into force. Since then it has only been signed and ratified by a modest number of countries worldwide, mostly in Europe, mostly developed rather than developing countries. High technology crime units have been created by law enforcement agencies in a number of countries and have had, so far, limited impact in deterring and prosecuting individuals who are hard to identify and who, working across borders, may not be extraditable.

Cybercrime is a well recognized activity and the technological capabilities of its perpetrators need to be acknowledged as being at least as good (if not better) than those of the individuals and corporate entities they attack. There is every reason to believe that these technological capabilities could be given or sold to other attackers ranging from small groups of activists to terrorist groups and Nation States which do not have this expertise.

It is also a fact that there have been attacks on private and public sector networks and computer systems. Many of these attacks did not have financial gain as their intent and instead were motivated to access confidential information and/or cause significant disruption for political or religious or other
reasons. These attackers have learned how to exploit technologies to gain anonymity – it is easier to suspect a party, such as a nation state – to be the sponsor and executor of such attacks than to collect evidence that will stand up to scrutiny in a court or by decision makers or military or national security/intelligence agencies – and this will be explored in the various case studies included in this book.

There are several objectives in producing this book. One is to combine the perspectives of various disciplines in an interdisciplinary, global discussion about evolving issues on cyber and information security for which no one has all the answers. The second is to identify within the fields of law, policy and information security current initiatives to address the challenges in confronting these issues. A third is to look prospectively at how to address gaps in law, policy and information security that we know currently exist (taking into account new technology and economic aspects that might shape the direction or paths in addressing these gaps).

This approach allows several basic questions to be explored, as follows:

- **WHAT** is the specific nature of the problem, covering the irreversible dependency of societies and business on technology and communications.
- **WHO** are the parties that have an interest in disrupting technology infrastructures and computer systems, considering both insiders and outsiders to an organization.
- **HOW** do such attacks take place and **HOW** can an organization prepare its defenses to limit the impact of attacks (considered to be inevitable).
- **WHEN** and **WHERE** have such attacks occurred - as illustrated by several case studies of attacks that have already occurred and been widely reported in the worldwide media.
- **WHY** – whenever this can be accurately established.

Over the nearly twenty years since the Internet has become available outside academic and military circles, we seem to have come full circle. What started as a method for scientific communication (Kaffner, 1998) that was then developed for use in the military domain, gradually became open access/open source for netizens throughout the world. Businesses in the first wave adopted it for e-commerce, and later for sharing their data within and outside the organization, managing supply chains, etc.

The public has adopted it for information search and access, creating content through personal websites and blogs, as well as communication with individuals via email and later social networking, communication with governments via e-government sites and links. A major side effect of the rapid adoption of personal computers and global networking was the emergence of a new breed of technically knowledgeable people around the world who understand the vulnerabilities of these environments and have the capabilities to exploit them for whatever reason.

Governments use the Internet for their own functions, ranging from connecting elements of their critical information infrastructures -- such as transportation, water, electricity and energy, and emergency and medical services to communicating within their departments and outside to citizens and the private sector in the provision of online services for forms, tax declarations, access to databases of medical records, electoral registers and more. Additionally, the police, legal institutions, CERTs, and national security agencies likewise use it to monitor, investigate, and address the breaches and security issues raised in this book.

Legislators are called upon to draft and adopt appropriate legislation; however, such legislation emerges many years after technologies have become widely established, which creates many opportunities for their exploitation with impunity. At times capacity for legislative drafting is limited or the legislation
drafted is inadequate for the new paradigm, resources are inadequate or non-existent to meet require-
ments mandated by legislation, or the legislation does not easily enable investigations or prosecution,
which may involve anonymity and necessitates cross-border collaboration when there are no official
channels for such collaboration.

This book presents the full panoply of issues, few answers, and a starting point for more work lasting
well into the future.

The Editors

Pauline C. Reich
Waseda University, Japan

Eduardo Gelbstein
Webster University, Switzerland

REFERENCES