In our network connected society, intrusion becomes a new form of trespassing, one which quite often leads to significant problems and poses great risks for the individual and for businesses, which are increasingly relying on modern information systems. The main appearances of intrusion, in the Information Society, are those concerning privacy intrusion and intrusion into information systems.

In particular, privacy intrusion is the act of intruding the personal sphere of the individual, which may involve the illicit collection and processing of personal data, the use of intrusive equipment, such as video cameras and key-loggers, but also of more sophisticated technologies, for example RFIDs. In the post 9/11 era, privacy poses as a negotiable good that can be compromised to preserve public security. Thus, surveillance poses as necessary measure in view of the threat of terrorism and organized crime.

Further, intrusion into a computer system can take many forms. We could note attempts at accessing and manipulating of information systems that can compromise the security and trust of such systems, which fall within the realm of e-crime. E-crime is undoubtedly one of the major challenges for the future of law enforcement. As information and communications technology (ICT) becomes more pervasive, the various kinds of electronic crime will be protagonists in all forms of criminal behavior.

The following means may be used for committing the act: electronic communications and transactions, spread of information via the Internet, falsification of physical characteristics and eventually ID theft.

The e-crime types may be categorized into four main groups (see Janczewski and Colaric, 2007):

- **Computer “threats”, ranging from hacking to cracking**: Including viruses, worms, or spyware.
- **Offensive, intrusive or misleading material**: Communicated through a Web page, in e-mails, or over mobile phones.
- **Fraud**: Economic transactions via computer believed to have involved fraud.
- **Identity theft or personal data violation**: The use of credit cards for theft, and the use of confidential personal information.

The rapid growth of ICT over the last few decades has opened up new possibilities for governments and individuals. Governments are increasingly using Wide Area Networks, the Internet, and mobile computing in their daily interactions with citizens and businesses. E-government applications are facilitating interaction with businesses by centralizing information sources into topical gateways, using Web-based
expert tools to help businesses access rules and regulations, and developing applications to allow electronic tax filings. For citizens, transactions, such as renewing licenses and certifications, paying taxes, and applying for benefits, have become less time consuming and easier to carry out.

Apart from government services, ICT has been also utilized in other sectors such as health, commerce, and of course, education. The increased use of ICT has actually been the motivating force for e-commerce.

E-technology allows organizations to deliver more services, more quickly, and directly. As a result, citizens do not interact with the government but also between them as peers promoting the e-commerce models they use (Papazoglou and Ribbers, 2006). These models may be P2P or B2B.

THE TECHNOLOGICAL, SOCIAL AND ECONOMIC POTENTIAL OF INTRUSION

E-crimes are usually committed for personal financial interest, whether they be theft and misuse of ID numbers or other personal information and data, for their benefit in ways that cause damage to the real owners of the data. It can be done through counterfeiting credit cards and using information and credit cards to order goods through the Internet, or cheating others to send personal data to them. These practices are committed through e-mail to mislead receivers that the e-mail is from an office or a reputable organization, such as banks or financial institutions.

Using sophisticated computer hacking techniques, criminals can violate security systems and install programs that may gather enormous quantities of personal financial data. As a consequence, widespread losses are caused to banks, retailers, and consumers.

The new dimension in this socio-economic phenomenon is its global perspective. National legislation protecting our personal data seems ineffective since the Internet has no borders or limitations. In the end, the easy and largely anonymous access, the unique speed, the flow rate of the Internet, as well as its ability to process information over an infinitesimal amount of time, pose new challenges for the protection of our informational privacy, of our virtual goods, of our cyber property, and eventually, of our personality. Indeed, our legitimate use of the Internet leaves behind countless tracks and enables the miscreants to form and misuse our personal profile.

Since the emergence of Web 2.0, the new trend on the Internet invites users not as passive receivers of information, but as creators, or at least as gatherers and redistributors of media rich in content. User-created content is the core means of development for this new era and is expressed through blogs, Wikis, photo collections, music, and even videos online. Small, interconnected tools allow anyone to have his own place on the Web, through which one can demonstrate creative skills in writing, photography, film making and much more. Creating and sharing digital resources is becoming easier (Zeng et al., 2006). In synoptic terms, information has become a primary product of our society. As a result, a shared culture emerges throughout the Internet, based on co-ownership and co-management of collective knowledge – or at least of collective “taste”.

An international culture of dealing online has been established. The creative and productive incorporation of new technologies across all frames and levels of our socio-economic environment constitutes indeed a promising frontier; however, up to now, it has not avoided multitudinous abuse.
REGULATING THE BATTLEFIELD: THE LEGAL LIMITATIONS

Legal regulations of privacy seem necessary in order to protect informational privacy. As new risks for privacy are emerging with new technologies, specific provisions need to be addressed, in order to tackle with the new realities. However, law should not impose solutions that hinder innovative technologies, but rather reconcile the right to privacy with the rights of others and technological progress.

Furthermore, securing computers, networks and mobile devices against the increasing complexity or malware and cyber threats requires commitment, vigilance and uncompromising reliability. Technical measures ensuring the highest levels of permanent ICT security apply a defensive mechanism aiming to mitigate the risks from online threats and phishing attacks, which are constantly increasing in both volume and complexity. However, the attacks of a determined offender and available opportunities to act illegally (in other words, the presence of a suitable target), and the absence of a capable guardian or someone who might prevent the crime from being committed are phenomena seen in daily transactions with an alarming frequency. Although motivations for acting illegally may well have remained fairly constant over time, developments in computing and communications technologies have created many new opportunities for people to act illegally. At the same time, the computer security industry has increased its capacity as “electronic capable guardians”.

Nevertheless, the globalization of the scene has given the opportunity to the world wide on-line community (estimated around the 1/5th of this planet’s population) to participate in cross-border transactions. There, the intentional commission of an act usually deemed socially harmful or dangerous is not always specifically defined or clearly excluded. This vulnerable situation where many things are not allowed but yet not specifically prohibited or punished, fuels, unfortunately, the boost of electronic criminality in its global perspective.

Crimes are classified by most legal systems for purposes such as determining which court has authority to deal with the case and what law to apply. In international law terms this is projected primarily as a jurisdictional issue. In addition, social changes often result in the adoption of new criminal laws and the obsolescence of older ones. The on-line community, at the same sense, explores prevailing theories of criminal activity, the conduct of all stages of criminal proceedings, and the various theories and practices for punishing electronic crime in its global manifestations.

The motivation, the formation and the impact of electronic crime on the social, economic and judicial sectors are presented in this book as a network of well connected factors. These factors that influence the roadmap to a homogenized confrontation of electronic crime are seen in Figure 1 (Politis et al, 2008).

ORGANIZATION OF THE BOOK

This book is organized in 19 chapters clustered in 3 sections. A brief description of each of the 19 chapters can be found in the detailed table of contents.

Section I, titled “The Social and Economic Dynamic for Electronic Crime” is comprised of eight chapters. In this section, background information is given about the factors that encourage and promote electronic crime.

Section II, titled “Electronic Intrusion: Technologies, Strategies and Methodologies” describes spearhead technologies that form the main context of the electronic crime literature. In this section, a more technical language is used to promote understanding of the scientific bias for illegal transactions.
The legal texts of this section address the implications of electronic crime for commercial, contract and criminal law, with concerns for the homogeneity of law enforcement in cross border situations and other jurisdictional matters.

Section III is titled “The Forensic Challenges for Intrusion.” Forensic engineering generally is defined as the investigation of questions, events and conditions having possible legal ramifications through the application of engineering principles and methodologies. Since litigation necessitates the use of expert testimony often involving highly technical issues, the expert is responsible for explaining highly technical subject matters in an understandable and sincere manner. Facts must be separated from speculation and the likely from the unlikely.

Comprising four highly technical chapters, it provides in-depth analysis of four distinct domains that are actively present in our everyday on-line habitat:

- Secure multimedia distribution
- Unsolicited electronic communication
- Electronic signature based authentication using public key infrastructures
- Security in e-banking transactions

**REFERENCES**


**ENDNOTE**

1 P2P stands for Peer to Peer, and collectively means any form of communication between two or more usual on-line users, in a globalized environment, in contradistinction to the centralized client-server transaction model. B2B signals the conceptual model for Business to Business communique, as an enhancement of the previous model for everyday e-Business transactions.