Chapter I
The Socioeconomic Background of Electronic Crime

Maria Karyda
University of the Aegean, Greece

ABSTRACT

This chapter discusses current and emerging forms of network and computer-related illegality (electronic crime), its background, the motives driving individuals to such actions as well as strategies and techniques for controlling it. The chapter places emphasis on current and future trends and highlights the open issues that need to be addressed to tackle this phenomenon.

INTRODUCTION

The presence of Information and Communication Technologies (ICTs) in modern societies is pervasive and affects all aspects of the economic, social, political and private life of individuals. Commerce, financial functions (including banking, stock exchanges), air traffic control, communications, electric power management and energy distribution, communications, transportation, healthcare services, education and other critical activities are largely dependent on ICTs. Companies use information technology and networks for effective organization, in order to implement their business processes and to improve communication with business partners and consumers. In the United Kingdom, for instance, nearly all companies use the Internet; 97% of companies have an Internet connection, 81% have a Web site, with 89% of these being externally hosted. Moreover, their dependence on information and communication technologies is considered very high, since only one out of six small-sized UK companies could operate without use of information technology (DTI, 2006).

Governments and public authorities depend more and more on technology to improve the quality of public services provided to their citizens, to cut down on exceeding costs while achieving value for money for services provided, to improve the efficiency and effectiveness of public organizations, to reduce "red tape" and to

align and better coordinate public administration, while individuals use technology in a wide range of their everyday lives for their professional (e.g. teleworking, collaborating, designing and manufacturing) and personal (e.g. education, entertainment, communication) lives.

Electronic crime (e-crime), or computer crime, or cyber crime refers to criminal activities where a computer or network is the source, tool, target, or place of a crime and is generally defined as a criminal activity involving an information technology infrastructure. Electronic crimes differ from traditional crimes, as we know them, mainly with regard to the location of the offender in relation to the scene of the crime: individuals now can commit an illegal act hundreds of miles away from their location, for instance hackers penetrating the computer system of a company in another country. Moreover, detection of electronic crime is often more difficult, since nothing may by physically missing as, for example, in cases of information theft or unauthorized access to computers and networks. E-crime affects all types of organizations (public, private etc.), as well as individuals, governments and public authorities with a wide range of consequences.

Generally, individuals' concerns about the security of information and communication infrastructures and the possibility to fall victims of some type of electronic crime are found to be very high. It is estimated, for example, that as high as 70% to 80% of European and US citizens have strong concerns over the privacy and security of their personal data. These concerns have a negative impact on the development of e-business and especially on client-oriented business functions (Business-to-Consumer). For instance, in a recent survey conducted for the European Commission about two thirds of the 11.832 individuals who participated, reported that they have been prevented from buying online or using on-line banking services because of security and privacy related concerns (Rand Europe, 2003). The same survey identified that a lack of trust and confidence in electronic services is a significant barrier to the development of e-Government. Businesses share, to some extent, the same concerns, since the protection of a company's information infrastructure is crucial for building customers' trust and for its overall operation and good reputation in general.

There are several aspects of electronic crime that remain underspecified; this chapter aims to provide an analysis of different aspects of electronic crimes and identify critical issues which are now rising as well as those that will evolve in the future. The first issue analyzed refers to the impact information and communication technologies have on crime. Then, the nature and different types of electronic crime are explored, by studying the different definitions, approaches and classifications found in the literature, in order to better understand and tackle it. Furthermore, the sources of electronic crime and different motives and characteristics of offenders are identified. We also discuss the impact electronic crime has on businesses and individuals and identify current and future trends. Finally, the chapter elaborates on the different approaches for controlling e-crimes.

INFORMATION AND COMMUNICATION TECHNOLOGIES AND CRIME

The Impact of ICTs: Old Crimes in New Bottles?

From the criminology point of view (Theoharidou et al, 2005) electronic crime can be understood as a matter of opportunities, based on the assumption that 'crime follows opportunity'. It is also widely acknowledged that the variety and volume of opportunities provided by information and communication technologies for electronic crime are proliferating. However, crimes usually need motivated offenders and a lack of adequate