Chapter III
Criminal Sanctions Against Electronic Intrusion

Irini E. Vassilaki
University of Goettingen, Germany

ABSTRACT

The international dimension of intrusion is discussed in this chapter along with the different legislative approaches adopted by various countries leading to the development of computer specific-legislation concerning electronic intrusion in a rather homogeneous style approach. The integrity of information and computer systems is presented and the misuse of devices, the illegal interception of data transfer and the illegal access to computer systems are bounded so to demonstrate the responsibility of providers or users.

INTRODUCTION

A legal comparative review of the criminal provisions concerning the punishment of the electronic intrusion is a complex operation that is impeded by the following factors:

- Electronic intrusion is - like the most forms of IT-Crime – an **international phenomenon.** In the most of the cases the perpetrators act within the boarders of one country whether the consequences of their activities appear in another one. That means that in a lot of cases is unclear, which is the applicable national criminal law.
- The national criminal systems have **different approaches**. Some countries face the new challenge with the application of the traditional criminal provisions. In the most of the cases these countries amend alternatives that enable the criminalization of the corresponding behaviors. Other countries however, prefer to create specific criminal provisions that cover specific forms of electronic intrusion.

- This form of IT-Crime is direct **depending on technique**. The revision of criminal provisions either as alternatives to existing articles or as new sections generates the following problem: the techniques that are the modus operandi of electronic intrusion change rapidly. However, criminal law has to provide legal certainty. This means that frequent change of the formulation of criminal provisions is neither desirable nor possible. The consequence is that the criminal provisions can either have general terms, which may not cover some of the techniques of electronic intrusion or to include technical terms. Through the last approach, however, the criminal provision will be useless, when the related technical terms become obsolete.

For these reasons, there are no uniform solutions in combating electronic intrusion. The following analysis will concentrate on some of the phenomena of electronic intrusion and will present the main principles that the national legal orders follow in order to criminalize such illegal behavior.

DEVELOPMENT OF COMPUTER SPECIFIC-LEGISLATION CONCERNING ELECTRONIC INTRUSION

Many countries enacted computer specific-legislation at the beginning of the 1980s as a reaction to computer economic crime. The amendments became necessary because new forms of criminality threatened intangible goods (e.g. bank deposits or computer programs) and could not be covered by the traditional criminal provisions. In most of the cases, the national legislator amended existing laws to punish computer specific crime, e.g. computer fraud, and created new provisions to fight the unauthorized access to computer systems.[1]

During the1980s the legislation mainly covered four offences: computer-related fraud, computer sabotage, computer espionage and illegal access to computer. Significant was the amendment of the "hacking" provisions in the national legislation that punished the mere illegal access to computer systems committed via telecommunication systems. Hacking became therefore the "basic offence" of the computer criminal law that protected the "formal sphere of secrecy" against illegal access to computer-stored data and computer communication.

Beginning with the 1990s,"hacking" as form of electronic intrusion increased. Cases such as that of the "German hackers" who, using international data networks, gained access - among others - to the Pentagon in order to sell the collected data to the KGB (Ammann, Lehnhard , Meißner , Stahl, 1989; Hafner, Markoff, 1991; Stoll, 1989) made obvious the dangerousness of such behaviors. During the same period, the press published amazing cases about the exploitation of viruses and worms that made the vulnerability of the computer systems obvious (Hafner, Markoff, 1991; Weihrauch 1988).[2] In the decade of the 1990s, electronic intrusion combined the distribution of illegal contents on the Internet with a broad wave of criminal activities e.g. program piracy, indicating that many perpetrators of such offenses belong to groups of organized crime (International AntiCounterfeiting Coalition, 2003; Union de Fabricants, 2003).[3]

During the decades of 1990 and at the beginning of 2000s, the evaluation of illegal intrusion on computer systems e.g. computer-related crime, became more complicated. This fact is the result of two factors:

- There is **no homogenous pattern** concerning the infringed legal interests. Computer hacking, sabotage or illegal intrusion served different interests such as terrorism, financial gain or Nazi-propaganda. The modus operandi of the perpetrators became more