AN OVERVIEW OF CYBERCRIME OFFENCES

Asia-Pacific Regional Workshop on Fighting Cybercrime
21. – 23.09.2011, Seoul
Prof. Dr. Marco Gercke, Director Cybercrime Research Institute

CATEGORIES OF OFFENCES

It is possible to divide between four different categories of offences:

• Offences against the Confidentiality, Integrity and Availability of Data and Computer Systems

• Content-related Offences

• Copyright and Trademark Offences

• Computer-related Offences

In addition there are so called “combined offences”
OFFENCES

- Illegal access to or remaining in a computer system
- Illegal data acquisition
- Disclosure of secret information
- Illegal data interception
- Illegal data manipulation
- Illegal system interference
- Computer-related fraud
- Computer-related forgery
- SPAM
- Defamation
- Harassment through ICT
- Pornography, indecent material and child pornography

ILLEGAL DATA ACQUISITION

- Valuable and secret information are often stored without adequate protection
- Lack of self-protection especially with regard to small businesses and private computer users
- Increasing number of cases
- Very often not criminalized because older regional and international legal frameworks do not contain such provision
IDENTITY THEFT

- Risks related to the illegal acquisition of data increases with regard to large data bases
- Information that can be obtained by copying such databases can not only be used for criminal purposes but also be sold

WIKILEAKS

- Information are not only illegally obtained but nowadays often published
- Controversial discussion about the advantages and disadvantages of whistle-blower platforms
- Approaches of major governments to remove the website from the web in 2010 failed
- Often the criminalization of publishing information is limited to state secrets
MISLEADING INFORMATION

- Information that are listed in search engines can influence consumers and business partners in their decisions.

- A posting that an e-commerce company is involved in fraudulent activities can for example negatively influence the operator of an online store.

- Offenders are setting up websites, manipulate search engines and charge companies to remove the posting.

CHILD PORNOGRAPHY

- Instead of offering files with illegal content for download operators of illegal websites today enable streaming video.

- This enables them to charge per view (pay-per-view) and limit the ability of users to share the content free of charge.

- Depending on the technology no data is saved on the users side. Therefore it is difficult to prosecute this as "possession".
THE BAD NEWS

- None of the above listed offences is covered by the "old" regional approaches such as the Budapest Convention on Cybercrime (2001) or the Commonwealth Model Law (2002).

- However, more recent approaches, such as the ICB4PAC Structure for Cybercrime Legislation that was developed by 15 Pacific Countries or the HIPCAR Model Legislative Text on Cybercrime, that was developed by 15 Caribbean Countries contain those offences.
OPPORTUNITIES

• Availability of computer technology improved the ability of law enforcement to carry out investigations
• DNA sequence analysis and fingerprint databases are examples for an emerging use of information technology in traditional criminal investigation

AUTOMATE

• Software tools are available to automate investigations
• Significant reduction of time for an investigation
• One example is the Software PERKEO that detects child pornography pictures on the basis of hash values
OPPORTUNITIES

- Case example 1: Within an investigation of a murder case law enforcement was unable to identify a murder based on search engine history. They were able to use search engine logs on the suspects computer to identify places he was interested in.

- Case example 2: Investigator were able to discover that the suspect was searching for specific terms such as “undetectable poisons,” “fatal digoxin levels,” “instant poisons,” “toxic insulin levels,” “how to purchase guns illegally,” “how to find chloroform,” “fatal insulin doses,” “poisoning deaths,” “where to purchase guns illegally,” “gun laws in PA,” “how to purchase guns in PA,”
More information about the topics mentioned within this presentation are available in the ITU publication *Understanding Cybercrime, 2nd Edition*, 2011.

The publication can be downloaded free of charge: