Cybercrime Offences

Asia Pacific Regional Mock Court Exercise on Fighting Cybercrime
18-19 Sept 2012, Jakarta, Indonesia

Prof. Dr. Marco Gercke
COMPUTER CRIME

- Computer crime is not a new phenomena
- The topic is discussed for half a century already
- However, it remains a current topic as the technology is changing at a high speed
- In addition legal response to the phenomena has made it to the top of the agenda of the international community
DEVELOPMENT OF COMPUTER SYSTEMS
1960th

- Introduction of transistor based computer systems lead to an increasing use of computers
- Offences at this time were focusing on the physical damage of computer systems and data
- Example: Student riot cause a fire that destroyed computer systems at a university in Canada
1970th

- Further increase in the use of computer systems and data
- Estimated 100,000 mainframe computer operated in the US only
- Physical damage of computer systems remained a relevant offence
- But new forms of crime were also discovered
1970th

• Illegal use of computer systems (that could lead to great financial losses)

• Manipulation of computer data (without and physical interference with the storage devices)

• Computer-related fraud (as more and more businesses and financial institutions switched to computer operations)

• Application of existing legislation to this new methods and targets went along with difficulties
1980th

- Increasing use of personal computers
- Lead to an increase in the potential number of targets
- First cases of software piracy
- In addition malicious software was more frequently produced and distributed
1980th - HISTORY OF VIRUSES

• 1982 the “Elk Cloner” virus was created (by Rich Skrenta). Designed for Apple OS
• 1986 “Brain Virus” was identified. Virus was designed for MS-DOS
• 1986 the file virus “Virdem” followed
• 1990 the first polymorph virus attack “Tequila” was started
1980th- MATH VIRUS

• "Math virus" stopped the computer after 30 steps and displays a simple addition or subtraction questions

• Execution of the program is denied unless the correct answer is given by the user
1980th – WALKER VIRUS

- Relatively harmless virus
- Walker virus: Displays occasionally an animation
1980\textsuperscript{th} - VIRUS

- At this time the speed of the distribution was limited due to the distribution by physical data storage media exchange.

- This left time for prevention measures. However, anti-virus software also needed to be physically distributed at this time.
1980th - PORNOGRAPHY

- The possibility to electronically distribute pornography was at this time limited
- Computer systems at this time were text-based and the resolution of screens were limited
- Distribution of pornography was at this time focusing on the distribution of text documents
• Introduction of the graphical user interface WWW (World Wide Web) in the 1990th lead to an increasing popularity of the network
• It became easier to use the services offered
• In addition it enabled the spreading of pictures, audio and video
• In addition the Internet eased transnational communication
TODAY

• More than 2 billion Internet user
• More Internet users in developing countries than in developed countries
• Globalization of services (with some services having several hundred million users)
• Increasing number of data
• Increasing reliance on computer services
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
# Substantive Criminal Law

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>COMESA Model Bill (2011)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>HIPCAR Cybercrime Model Law (2010)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>CoE Cybercrime Convention (2001)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>ICB4PAC Cybercrime Model law (2011)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Different EU instruments</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>Draft African Union Convention (2011)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>HIPCAR Cybercrime Model Law (2010)</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
<tr>
<td>HIPSAA Draft Model Cybercrime</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
<td>✔</td>
</tr>
</tbody>
</table>
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”
Illegal Data Acquision

- 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
- 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
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.
ILLEGAL ACCESS

- Accessing (in most cases remotely) a computer, computer system or network without permission.
- Deliberately gaining unauthorised access to an information system
- Phenomenon also called “hacking”
- Origin of the term “hacking” was positive development of new functions
ILLEGAL ACCESS

• Social Engineering
• Social engineering is the term used to describe the utilization of human behaviour to breach security without the participant (or victim) even realizing that they have been manipulated.
• „Human Approach“
ILLEGAL INTERCEPTION

- Many Internet users that set up wireless access devices are not aware that the related signals are available in a radius of up to 100 meter

- Offenders can make use of the internet connection from the distance to commit crimes
DATA INTERFERENCE

• The term data interference is used to describe a negative interaction with regard to computer data
• Example: Computer virus that deletes information on a hard drive
• A computer virus is a malicious software that is able to replicate itself and infect a computer without the permission of the user in order to carry out operations
• Primary target: Computer data
BACKGROUND

• Development of large storage media supports the increasing importance digital information
SYSTEM INTERFERENCE

• Example: Denial-of-Service Attacks
• Definition: attempt to make a computer resource unavailable to its intended users
• Distributed DoS attack: DDoS attack occurs when multiple compromised systems flood the bandwidth of a targeted system.
CHILD PORNOGRAPHY

- In the past child pornography was traded offline
- The production in general required the involvement of service provider (film laboratories)
- Similar situation with regard to the distribution that required the involvement of a limited number of service providers (postal services)
CHILD PORNOGRAPHY

• Availability of Video Cameras changed the situation dramatically.

• With a video camera the offender did not need to rely on service provider to produce child pornography

• Decreased the possibility to identify the offender within the production / duplication process

• Limited means of distribution remain a strong possibility for investigation
• Extent of an involvement of organized crime is uncertain
• An example for quotations without verifiable reference was discovered by the Wall Street Journal in 2006.
• While investigating a quotation that “child pornography is a multibillion business – 20 billion USD a year” - a journalist discovered that two main documents containing information about revenues from 3 billion to 20 billion – a publication from NCMEC and one from the Council of Europe - did quote non-existing sources.
SPEED OF DATA TRANSFER

- Data transfer speed enables quick move of data

- Offenders can make use of the speed of data transfer processes to hinder the removal of information