Special Training on Cybercrime 2nd Workshop On Transposition Of SADC Cybersecurity Model Laws In National Laws For Namibia

Windhoek, Namibia – 25 July 2013

Training on Cybercrime and Discussion of the Draft Bill

Presented by: Prof Dr Marco Gercke, ITU Consultant

International Telecommunication Union

Committed to connecting the world

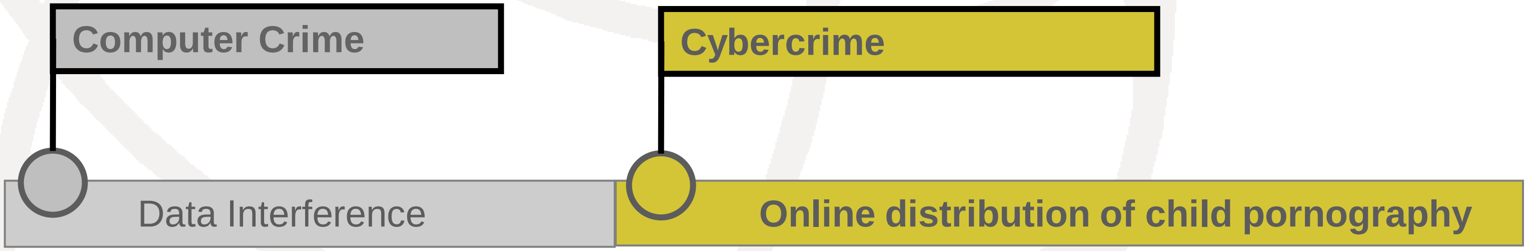
European Commission

Tools

- The presentation and the ITU publication „Understanding Cybercrime“ will be made available after the training

- http://www.itu.int/ITU-D/cyb/cybersecurity/projects/crimeguide.html

CYBERCRIME AND COMPUTER CRIME



Computer Crime

Cybercrime

Data Interference

Online distribution of child pornography

1985

2010

2000

CYBERCRIME AND COMPUTER CRIME

- The term “cybercrime” is narrower than computer-related crimes as it has to involve a computer network

- Computer-related crimes cover even those offences that bear no relation to a network, but only affect stand-alone computer systems

WHAT IS CYBERCRIME ?

DEFINITION

- There are several difficulties with this broad definition

- It would, for example, cover traditional crimes such as murder, if perchance the offender used a keyboard to hit and kill the victim

- Definition developed during the 10th UN Congress is equally challenging

Common Definition

Computer crime is any activity in which computers or networks are a tool, a target or a place of criminal activity

10th UN Crime Congress

Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network

DEVELOPMENT OF COMPUTER SYSTEMS

OVERVIEW

- Ever since the use of computer systems started crimes were discovered
- Over the last 50 years every technical development went along with discovering new types of crime
- Most of the crimes that were first discovered 50 years ago are still relevant
- It is unfortunately not incorrect to say that new crimes were added to the list but almost non removed

196oth

- 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

Picture removed in print version
Bild zur Druckoptimierung entfernt

Source: Wikipedia with ref. to US Gov.

197oth

- 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

Picture removed in print version
Bild zur Druckoptimierung entfernt

Source: Wikipedia with ref. to Ed Uthman

197oth

- 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

198oth

- 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

Picture removed in print version
Bild zur Druckoptimierung entfernt

Source: Wikipedia with ref to B. Bertram

198oth - 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 the file virus “Virdem” followed
- 1990 the first polymorph virus attack “Tequila” was started

Picture removed in print version
Bild zur Druckoptimierung entfernt

Example

198oth- 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

Picture removed in print version
Bild zur Druckoptimierung entfernt

Math Virus

198oth – WALKER VIRUS

- Relatively harmless virus
- Walker virus: Displays occasionally an animation

Picture removed in print version
Bild zur Druckoptimierung entfernt

Walker Virus

198oth - 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

Picture removed in print version
Bild zur Druckoptimierung entfernt

Example

198oth - 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
- Approaches to visualise pornography by using ASCII signs
- Distribution of pornography was at this time focusing on the distribution of text documents

199oth

- 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
- Went along with several challenges for law enforcement

Picture removed in print version
Bild zur Druckoptimierung entfernt

Source: Wikipedia with ref. to Cailliau

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

Picture removed in print version
Bild zur Druckoptimierung entfernt

Source: Internet World Stats

DIFFERENT CATEGORIES OF CYBERCRIME

Substantive Criminal Law	Illegal Access to a Computer	Illegal Remaining in a Computer	System Interference	Illegal Interception	Illegal Access to Computer Data	Illegal Data Input	Illegal Aquisition of Comp. Data	Illegal Data Interference	Illegal Use of Data	Illegal Devices / Misuse of Devices	Violation of Data Protection Regul.	Computer-related Fraud	Computer-related Forgery	Indecent Material	Pornography	Child Pornography	Solicitation of Children	Dissemination of Racist Material	Identity-related Crime	SPAM	Threat and Harassment	Disclosure of an Investigation	Failure to Provide Assistance	Copyright Violation
HIPSSA / SADC Model Law	✓	✓	✓	✓			✓	✓		✓	✓	✓	✓			✓		✓	✓	✓	✓	✓	✓	
	CIA Offences										Data Protection Violation	Computer-related Offences		Illegal Content								Safeguarding Proced. Law		Copyright Violations

NUMBER OF CRIMES COMMITTED

UNCERTAINTY REGARDING EXTENT

- Lack of reporting leads to uncertainty with regard to the extent of crime
- This is especially relevant with regard to the involvement of organized crime
- Available information from the crime statistics therefore not necessary reflect the real extent of crime

HEIISE NEWS 27.10.2007

The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful
hacker attack," explained Mark Mershon, acting head of the FBI's New York office.

IMPACT OF CYBERCRIME

IMPACT OF CYBERCRIME

- The impact of Cybercrime does not need to be solely financial
- As diverse as the crimes itself is the possible impact
- Ranges from financial loss to a loss of reputation

REPUTATION

- If the offenders abuse the victims ID to commit crimes or open a bank account the damage can go way beyond financial loss
- The reputation of the victim might be damaged
- It could require significant energy to restore the reputation – if this is possible at all

Picture removed in print version
Bild zur Druckoptimierung entfernt

SOCIAL SECURITY NUMBER

REPUTATION

- If the offenders get access to private photos or emails and publish them online it is possible that there are so many copies of those documents available online that they can not be removed anymore

- It is particular difficult to order the removal of content that is stored abroad

Picture removed in print version
Bild zur Druckoptimierung entfernt

EDISION CHEN CASE

REPUTATION OF COMPANIES

- 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

Picture removed in print version
Bild zur Druckoptimierung entfernt

Example

ECONOMIC IMPORTANCE

- Extent of economic damages caused by cybercrime is controversially discussed

- Many companies (esp. small and medium size businesses) do not report attacks and costs

Picture removed in print version
Bild zur Druckoptimierung entfernt

Sources: Computer Economics (2007)

UNCERTAINTY REGARDING EXTENT

- Lack of reporting leads to uncertainty with regard to the extent of crime

- This is especially relevant with regard to the involvement of organized crime

- Available information from the crime statistics therefore not necessary reflect the real extent of crime

Picture removed in print version
Bild zur Druckoptimierung entfernt

HEISE NEWS 27.10.2007

UNCERTAINTY REGARDING EXTENT

- Very often crime is not reported to law enforcement
- As law enforcement is a major information provider for the government a lack of knowledge of law enforcement can have serious consequences on politics and legislation

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE SURVEY PACIFIC ISLAND

DIFFERENT CATEGORIES OF CYBERCRIME

ILLEGAL ACCESS

- Definition
- Accessing (in most cases remotely) a computer, computer system or network without permission.
- Deliberately gaining unauthorised access to an information system

- Motivation
- Different motivations
- Financial interest

Picture removed in print version
Bild zur Druckoptimierung entfernt

Hacking Tool

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“
- In 1994, a French hacker contacted the FBI office in Washington, pretending to be an FBI representative who is working at the U.S. embassy in Paris. He persuaded the person in Washington to explain how to connect to the FBI's phone conferencing system. Then he ran up a $250,000 phone bill in seven months.
- Classic scam: Phoning

ILLEGAL REMAINING

- Interesting approach in Art. 4 ECOWAS Cybercrime Directive
- Criminalisation of the fraudulent remaining in a computer system
- Criminalization of illegal remaining in addition to illegal access can be required to address cases where the offender legally accesses a computer system and afterwards illegally remains logged in

ART. 3 ECOWAS CYBERCRIME DIRECTIVE

The act by which a person fraudulently remains or attempts to remain within the whole or part of a computer system.

SYSTEM INTERFERENCE

- Businesses are increasingly depending on the availability of network and communication services

- Example: Switch from tradition high-street shops to e-commerce businesses

- But also businesses that do not offer services online might depend on network technology („Cloud Computing“)

Picture removed in print version
Bild zur Druckoptimierung entfernt

E-COMMERCE WEBSITE

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.

Picture removed in print version
Bild zur Druckoptimierung entfernt

DENIAL OF SERVICE ATTACK

ILLEGAL INTERCEPTION

- The use of network services (and in this context especially Internet services) requires data transfer processes
- During the transmission data is processed and forwarded by different infrastructure provider (e.g. Router)
- Risk that during those transfer processes data can be intercepted

Picture removed in print version
Bild zur Druckoptimierung entfernt

BACKGROUND: DATA TRANSFER

DATA ESPIONAGE

- The term data espionage is used to describe the act of illegally obtaining computer data

- Unlike most other offences there is no wide consensus that the criminalisation of such conduct requires a specific provision

Picture removed in print version
Bild zur Druckoptimierung entfernt

Sony

DATA ESPIONAGE

- Valuable and secret information are often stored without adequate protection
- Lack of self-protection especially with regard to small businesses and private computer users
- Development of protection-plans are often inadequate (eg. change of hard-drive without deleting sensible information in advance)

Picture removed in print version
Bild zur Druckoptimierung entfernt

KEYLOGGER

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

Picture removed in print version
Bild zur Druckoptimierung entfernt

COMPUTER VIRUS

DIGITAL DATA

- Emerging importance of digital information
- Number of digital documents is intensively increasing
- Costs for storing one MB of data was constantly decreasing during the last decades
- Today it is cheaper to store information digitally than to keep physical copies

DATA PROTECTION VIOLATION

- With the current technology it is possible to automatically collect user information, store them and automatically process/analyse them

- This led to an on-going debate about the need for stricter data protection standards

Picture removed in print version
Bild zur Druckoptimierung entfernt

COLLECTION OF DATA

DATA PROTECTION VIOLATION

- Within this debate it is very important to pay attention to the fact that often users are voluntarily disclosing information

- The main difference between todays concerns related to data protection and concerns raised in the past is the fact that not states and private entities are the institutions that significantly collect information

Picture removed in print version
Bild zur Druckoptimierung entfernt

G. ORWELL 1984

DEVELOPMENT

- Fraud remains one of the most popular crimes in general
- This is also relevant as with regard to fraud committed by using means of electronic communication
- Offences involving computer technology are particularly popular as offenders can make use of automation and software tools to mask criminals identities
- The most popular fraud scams include Online Auction Fraud, Advance Fee Fraud, Lottery Scams

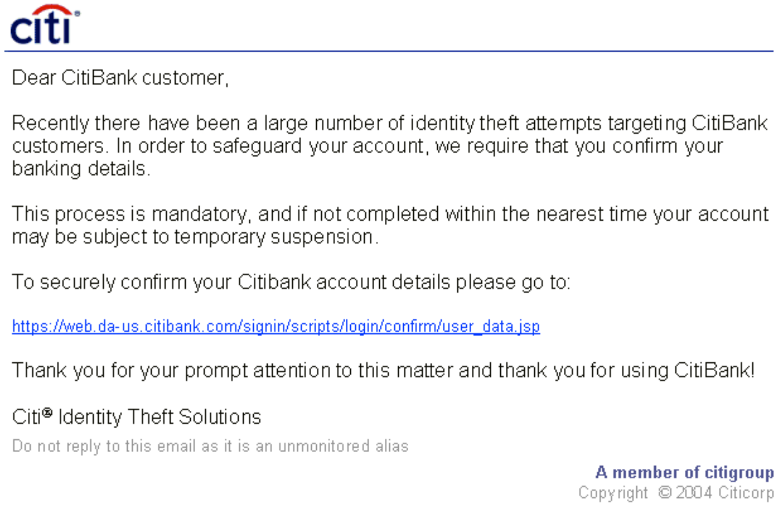
DEVELOPMENT

- As with regard to the legal response it is necessary to differentiate between traditional fraud (manipulation of human beings) committed by using means of electronic communication and computer-related fraud (manipulation of data processing)
- Traditional fraud committed by using means of electronic communication (e.g. auction fraud) is in general covered by traditional criminal law provisions while the prosecution of manipulation of data processing in general require specific legislation

COMPUTER RELATED FORGERY

- Computer-related forgery is today often linked to the phenomenon “phishing”

- Term used to describe act of fraudulently acquiring sensitive information (such as passwords) by masquerading as a trustworthy person or business (e.g. financial institution) in a seemingly official electronic communication



citi

Dear CitiBank customer,

Recently there have been a large number of identity theft attempts targeting CitiBank customers. In order to safeguard your account, we require that you confirm your banking details.

This process is mandatory, and if not completed within the nearest time your account may be subject to temporary suspension.

To securely confirm your Citibank account details please go to:

https://web.da-us.citibank.com/signin/scripts/login/confirm/user_data.jsp

Thank you for your prompt attention to this matter and thank you for using CitiBank!

Citi® Identity Theft Solutions

Do not reply to this email as it is an unmonitored alias

A member of citigroup
Copyright © 2004 Citicorp

EXAMPLE: PHISHING E-MAIL

PORNOGRAPHY

- Various websites with pornographic content
- Commercial and non-commercial
- Link lists available that lead to sexual related content
- No access control that could exclude access of minors
- Making pornographic material accessible without a proper access control is criminalised in some countries

Picture removed in print version
Bild zur Druckoptimierung entfernt

PORNOGRAPHIC WEBSITE

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)
- Today the distribution takes place online

Picture removed in print version
Bild zur Druckoptimierung entfernt

Film Laboratory

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

Picture removed in print version
Bild zur Druckoptimierung entfernt

MOVEMENT IP

DEFAMATION

- Internet can be used to publish false or defamatory information
- Examples: Intimate photos, phone numbers, false information about financial situation

Picture removed in print version
Bild zur Druckoptimierung entfernt

DEFAMATION

- Related problems
- Identification of the offender
- Removing the content

COPYRIGHT VIOLATIONS

- Artwork available:
- Music (esp. but not only copyright protected work)
- Movies (even before they were out in cinema)
- Software (including serial numbers)

SKIMMING

- Seems to become an issue in Namibia
- Not really a computer crime
- But related to computer technology

Picture removed in print version
Bild zur Druckoptimierung entfernt

Skimming

ID-RELATED CRIMES

- Increasing number of reports about Identity theft in the US
- Special risk related to single ID-Systems
- Social Security Number or one-card systems
- Taking over a single ID can enable the offender to abuse the ID

Picture removed in print version
Bild zur Druckoptimierung entfernt

SOCIAL SECURITY NUMBER

ID-RELATED CRIMES

- Users are tending to offering private information in social networks
- Information can be accessed by any Internet user
- Threat of abuse of those information in relation to ID-theft related offences
- Having access to those information can be from great importance for the offender

Picture removed in print version
Bild zur Druckoptimierung entfernt

SOCIAL MEDIA

OPPORTUNITIES

OPPORTUNITIES

- Availability of computer technology improved the ability of law enforcement to carry out investigations

- DNA sequence analysis and finger print databases are examples for an emerging use of information technology in traditional criminal investigation

Picture removed in print version
Bild zur Druckoptimierung entfernt

FINGERPRINT DATABASE

OPPORTUNITIES

- In 2013 news reports indicated that the US Postal Service photographs 160.000.000 letters every year

- Such measure allows investigations that have not been possible before

- The news reports indicate that the measures have been used in criminal investigations already

Picture removed in print version
Bild zur Druckoptimierung entfernt

RT NEWS

OPPORTUNITIES

- In 2013 the Guardian reported about a UK based program (Tempora), operated by HCHQ that monitors international data communication passing through the UK in real time

- Additional reports that the UK stores both content data and traffic data (meta data) for several days

Picture removed in print version
Bild zur Druckoptimierung entfernt

GUARDIAN

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

Picture removed in print version
Bild zur Druckoptimierung entfernt

PERKEO

AUTOMATE

- Automation techniques can also be used to identify copyright violations

- One example is file-sharing monitoring where software tools can automatically detect copies of copyright-protected art-work made available

- Another example is the automatic scanning of scientific work (like PhD)

Picture removed in print version
Bild zur Druckoptimierung entfernt

GUTTENPLAG

AUTOMATE

- With regard to file-sharing systems investigators can automate the process of detecting users that make available copyright protected material
- Ten-thousands of reports submitted to a single prosecution department within one year underlines the effectiveness of such investigation method
- However, the following process (especially the court proceedings) require significantly more time

Picture removed in print version
Bild zur Druckoptimierung entfernt

FILESHARING

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.

Picture removed in print version
Bild zur Druckoptimierung entfernt

Informationliberation.com

OPPORTUNITIES

- 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,”

Picture removed in print version
Bild zur Druckoptimierung entfernt

PCWORLD

DEVICES PROCESSING DATA

- Devices do often store information that are valuable for traditional investigation
- The user do not necessary have knowledge about such operation
- One example is the iPhone that stored the geo-location of the user and thereby enabled the reconstruction of movements/travel

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE: AMAZON CLOUD COMPUTING

DEVICES PROCESSING DATA

- In addition to “general” meta data the photos might include GPS data that shows where the photo was taken

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXIF

DEVICES PROCESSING DATA

- Criminals taking photos and placing them online might leave traces that can be used by law enforcement officers to identify them
- In addition to the “photo” graphic files might contain meta data
- Several camera models include the serial number of the camera in the meta data of each file

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXIF

EXAMPLE SUBSTITUTION

- Another example for substitution of traditional evidence is e-mail communication
- In the past correspondence was basically done via letter
- This enabled courts to analyse evidence presented (Graphology)

Picture removed in print version
Bild zur Druckoptimierung entfernt

HANDWRITING

EXAMPLE SUBSTITUTION

- The introduction of typewriter already changed the ability of courts to verify that a document was not altered

- But it was possible to analyse various factors within court proceedings (e.g. ink used)

- Unless use advanced technology (such as digital signatures) are used it is rather easy to manipulate e-mails

EXAMPLE SUBSTITUTION

- Emerging use of e-mails has changed the abilities to verify evidence again
- Unless use advanced technology (such as digital signatures) are used it is rather easy to manipulate e-mails

E-MAIL FORENSICS

- More and more correspondence is done electronically
- Uses of Internet-services such as e-mail leave various traces
- Information contained in an e-mail go way beyond sender, recipient, subject and content
- Header information can help law enforcement to identify the sender of threatening mails

ALTERATION

- As valuable e-mails can be for an investigation as important it is to keep in mind that e-mails are only text documents
- Open to alteration
- Courts in some jurisdictions are therefore restrictive when it comes to the admissibility of electronic mails

BACKGROUND

- Emerging relevance of digital evidence influences the procedures in court

- Influence is not limited to the fact that courts need to deal with digital evidence

- Even the design of courtrooms is influenced

BACKGROUND

- Courtrooms designed today are equipped with technology that allows the court to handle digital evidence adequately

- As the technology is constantly developing this is an on-going process