Cybercrime
Research Institute

INTRODUCTION
DEVELOPMENT AND PHENOMENA

ITU, ICB4PAC

02.03.2011, Vanuatu

Prof. Dr. Marco Gercke, Director Cybercrime Research Institute

Cybercrime
Research Institute

GENERAL INTRODUCTION

Cybercrime
Research Institute

CYBERCRIME

- Fighting Cybercrime is a challenge for developed countries as well as developing countries
- The ability to investigate crimes is important to protect Internet users in the country as well as businesses from becoming victim of such offence
- It is in addition necessary to be able to identify and prosecute offenders in the country to avoid international isolation (example: "I love you virus")

Picture removed in print version
Bild zur Druckoptimierung entfernt

ILOVEYOU Virus

Cybercrime
Research Institute

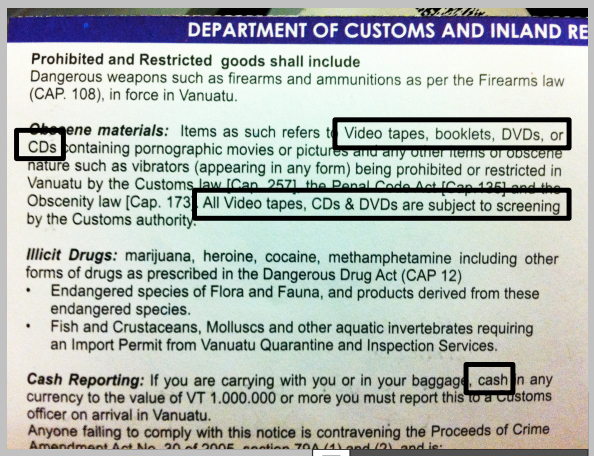
CYBERCRIME

- Tourism plays an important role in the region
- To attract visitors more and more hotels are making use of the Internet to promote service and enable customers to make reservations online. This goes along with the risk that such services are abused (e.g. credit card fraud)
- In addition tourists are nowadays bringing their computer with them. The could commit crimes or become victims while being in the country

Picture removed in print version
Bild zur Druckoptimierung entfernt

Customs Form

CYBERCRIME



DEPARTMENT OF CUSTOMS AND INLAND RE

Prohibited and Restricted goods shall include
Dangerous weapons such as firearms and ammunitions as per the Firearms law (CAP. 108), in force in Vanuatu.

Obscene materials: Items as such refers to Video tapes, booklets, DVDs, or CDs containing pornographic movies or pictures and any other items of obscene nature such as vibrators (appearing in any form) being prohibited or restricted in Vanuatu by the Customs law [Cap. 257], the Penal Code Act [Cap 135] and the Obscenity law [Cap. 173] All Video tapes, CDs & DVDs are subject to screening by the Customs authority.

Illicit Drugs: marijuana, heroine, cocaine, methamphetamine including other forms of drugs as prescribed in the Dangerous Drug Act (CAP 12)

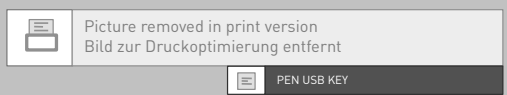
- Endangered species of Flora and Fauna, and products derived from these endangered species.
- Fish and Crustaceans, Molluscs and other aquatic invertebrates requiring an Import Permit from Vanuatu Quarantine and Inspection Services.

Cash Reporting: If you are carrying with you or in your baggage cash in any currency to the value of VT 1.000.000 or more you must report this to a customs officer on arrival in Vanuatu.
Anyone failing to comply with this notice is contravening the Proceeds of Crime Amendment Act No. 30 of 2005, section 70A (1) and (2), and is:

Customs Form

CYBERCRIME

- Today digital information are not necessary stored on CDs or DVDs
- Offenders are more and more frequently using USB keys and other small storage devices
- Identifying storage devices can be difficult as storage technology can be integrated is everyday items like watches or pens



PEN USB KEY

Cybercrime
Research Institute

CYBERCRIME

- Today a lot of devices enable the user to encrypt data
- The use of encryption technology is a key component to protect information and the use of encryption technology is suggested by many Cybersecurity experts
- However, the use of encryption technology can seriously hinder investigations

Picture removed in print version
Bild zur Druckoptimierung entfernt

ENCRYPTION

Cybercrime
Research Institute

CYBERCRIME

- Offenders that want to bring illegal material in the country do not necessary have to carry physical storage devices
- Remote storage is very popular
- Various Internet companies such as Microsoft and Google offer large server capacities for the storage of data (such as e-mail, pictures, video) that can be accessed from any place with an Internet connection

Picture removed in print version
Bild zur Druckoptimierung entfernt

Google Storage Space

Cybercrime
Research Institute

LESSON LEARNED

- **Understand the issue**
- **Substantive criminal law** that describes illegal conduct is essential
- Specific **investigation instruments** might be required
- Rules related to the **admissibility of evidence** can be necessary
- **International cooperation** can be required to carry out investigations
- **Training** is very important

Cybercrime
Research Institute

ITU RESOURCES

- ITU published "Understanding Cybercrime: A Guide for Developing Countries"
- 225 pages, available for free download

Cybercrime
Research Institute

ITU RESOURCES

- Available in the following languages: English, French, Spanish, Chinese, Arabic, Russian
- An updated 2nd edition is planed to be released later this year

Cybercrime
Research Institute

ITU RESOURCES

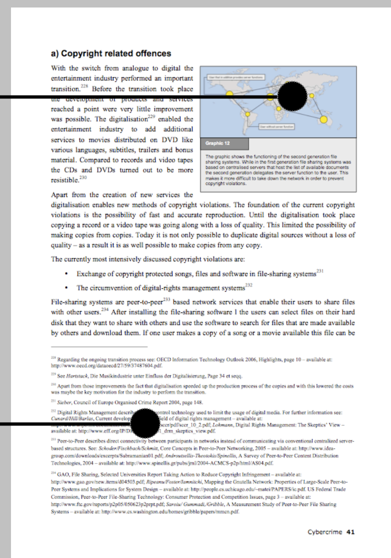
- Guide has become a resource in various training activities around the globe
- Also used in different legislation reform projects (ECOWAS, HIPCAR project)

Cybercrime
Research Institute

CYBERCRIME GUIDE

Examples and Explanation

References and Sources
(if available from publicly available sources)



a) Copyright related offences

With the switch from analogue to digital the entertainment industry performed an important transition.[228] Before the transition took place the development of products and services reached a point were very little improvement was possible. The digitalisation[229] enabled the entertainment industry to add additional services to movies distributed on DVD like various languages, subtitles, trailers and bonus material. Compared to records and video tapes the CDs and DVDs turned out to be more resistible.[230]

Graphic 12

The graphic shows the functioning of the second generation file sharing systems. While in the first generation file sharing systems was based on centralised servers that host the list of available documents the second generation delegates the server function to the user. This makes it more difficult to take down the network in order to prevent copyright violations.

Apart from the creation of new services the digitalisation enables new methods of copyright violations. The foundation of the current copyright violations is the possibility of fast and accurate reproduction. Until the digitalisation took place copying a record or a video tape was going along with a loss of quality. This limited the possibility of making copies from copies. Today it is not only possible to duplicate digital sources without a loss of quality – as a result it is as well possible to make copies from any copy.

The currently most intensively discussed copyright violations are:

- Exchange of copyright protected songs, files and software in file-sharing systems[231]
- The circumvention of digital-rights management systems[232]

File-sharing systems are peer-to-peer[233] based network services that enable their users to share files with other users.[234] After installing the file-sharing software l the users can select files on their hard disk that they want to share with others and use the software to search for files that are made available by others and download them. If one user makes a copy of a song or a movie available this file can be

[228] Regarding the ongoing transition process see: OECD Information Technology Outlook 2006, Highlights, page 10 – available at: http://www.oecd.org/dataoecd/27/59/37487604.pdf.

[229] See *Hartstack*, Die Musikindustrie unter Einfluss der Digitalisierung, Page 34 et seqq.

[230] Apart from those improvements the fact that digitalisation speeded up the production process of the copies and with this lowered the costs was maybe the key motivation for the industry to perform the transition.

[231] *Sieber*, Council of Europe Organised Crime Report 2004, page 148.

[232] Digital Rights Management describ[illegible]control technology used to limit the usage of digital media. For further information see: *Cunard/Hill/Barlas*, Current develop[illegible]field of digital rights management – available at: [illegible]sccr/pdf/sccr_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View – available at: http://www.eff.org/IP/D[illegible]_drm_skeptics_view.pdf.

[233] Peer-to-Peer describes direct connectivity between participants in networks instead of communicating via conventional centralized server-based structures. See: *Schoder/Fischbach/Schmitt*, Core Concepts in Peer-to-Peer Networking, 2005 – available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, A Survey of Peer-to-Peer Content Distribution Technologies, 2004 – available at: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

[234] GAO, File Sharing, Selected Universities Report Taking Action to Reduce Copyright Infringement – available at: http://www.gao.gov/new.items/d04503.pdf; *Ripeanu/Foster/Iamnitchi*, Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design – available at: http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf. US Federal Trade Commission, Peer-to-Peer File-Sharing Technology: Consumer Protection and Competition Issues, page 3 – available at: http://www.ftc.gov/reports/p2p05/050623p2prpt.pdf; *Saroiu/ Gummadi,/Gribble*, A Measurement Study of Peer-to-Peer File Sharing Systems – available at: http://www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

Cybercrime **41**

Cybercrime
Research Institute

PHENOMENA

- Explaining more than 20 different kind of offence linked to the term "Cybercrime"
- Ranging from traditional offences like illegal access or computer-related fraud to complex scams like "phishing" and "cyberlaundering"
- Even topics that go beyond international standards like religious offences or illegal gambling are covered

Cybercrime
Research Institute

CHALLENGE

- Providing a detailed analysis of the most important challenges related to the fight against Cybercrime
- This includes very recent issues like the emerging use of encryption technology, the use of botnets to commit large scale attacks and the ability to the hide the identity by using anonymous communication services

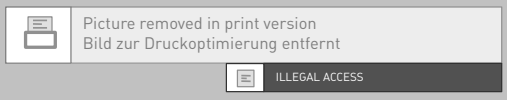
Cybercrime
Research Institute

OFFENCES

Cybercrime
Research Institute

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



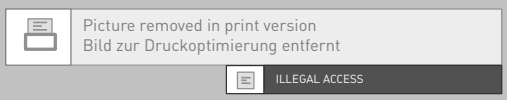
Cybercrime
Research Institute

ILLEGAL ACCESS

Famous victims of hacking attacks:

- NASA (1992)
- CIA (1996)
- US Air Force (1996)
- US Department of Justice (1996)
- Pentagon (1998)
- German Government (2006)

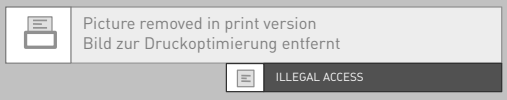
Source:http://en.wikipedia.org/wiki/Timeline_of_hacker_history



Cybercrime
Research Institute

ILLEGAL ACCESS

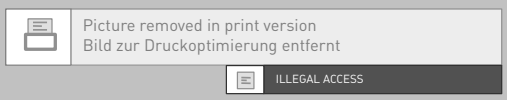
- Motivation of offenders varies significantly (penetration test to identify week points in network technology, demonstration of technical experience, part of a military strategy, political / moral motivation)
- Financial interest (esp. blackmailing) is only one possible motivation
- In some cases the offence was linked to political motivation
- „Sport“ for the next generation of computer criminals



Cybercrime
Research Institute

ILLEGAL ACCESS

- Huge number of attacks is a result of automatic attacks
- Software Tools available that automatically scan IP-address areas for unprotected computers (especially open ports)
- It is possible to scan thousands of computer systems with a single computer
- Average time until a computer is attacked for the first time after being connected to the internet: 30 minutes



Cybercrime
Research Institute

ILLEGAL ACCESS

Modus Operandi

- Access to a computer/network from the inside
- Hacking attack from the outside

Techniques

- Social Engineering
- Use of software devices to break the password protection
- Use or malicious software (spyware, key-logger) to record passwords
- Use of search-engines ("Google")

Cybercrime
Research Institute

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

Cybercrime
Research Institute

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

DATA ESPIONAGE

Cybercrime
Research Institute

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 is inadequate (eg. change of hard-drive without deleting sensible information in advance)

Picture removed in print version
Bild zur Druckoptimierung entfernt

DATA ESPIONAGE

Cybercrime
Research Institute

DATA ESPIONAGE

- Apart from hardware tools there are a number of software-based keylogger solutions
- Unlike the hardware solutions most software based keylogger tools can be detected by anti-spyware tools

Picture removed in print version
Bild zur Druckoptimierung entfernt

DATA ESPIONAGE

Cybercrime
Research Institute

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

Cybercrime
Research Institute

ILLEGAL INTERCEPTION

- Popularity of network based service increased the threats
- Availability of high-speed Internet connections and server infrastructure today enables the development of storage concepts that are not anymore based on local but decentralised storage
- „cloud computing“ and „cloud storage“

Picture removed in print version
Bild zur Druckoptimierung entfernt

EXAMPLE: AMAZON CLOUD COMPUTING

Cybercrime
Research Institute

ILLEGAL INTERCEPTION

- Another reason for increasing threats is the popularity of wireless Internet devices
- Wireless technology (WLAN / WIFI) is a popular technology to make services available in a local area

Picture removed in print version
Bild zur Druckoptimierung entfernt

WIRELESS LAN

Cybercrime
Research Institute

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

Cybercrime
Research Institute

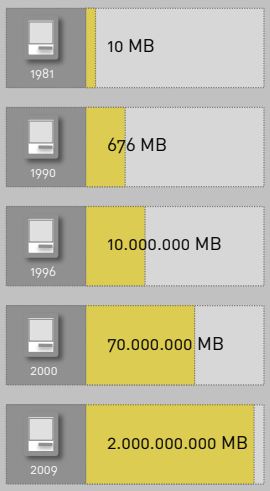
DIGITAL DATA

- 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

Cybercrime
Research Institute

BACKGROUND

- Development of large storage media supports the increasing importance digital information



Cybercrime
Research Institute

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

Cybercrime
Research Institute

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.

Cybercrime
Research Institute

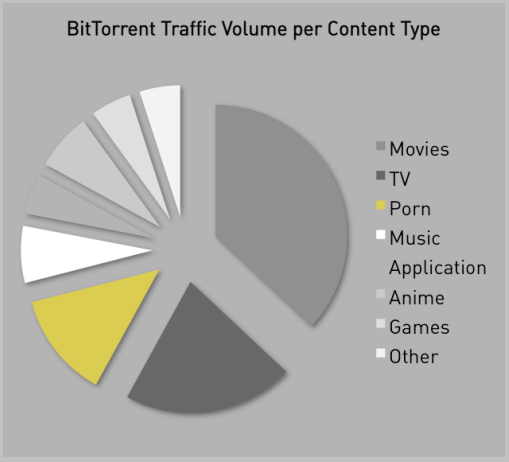
PORNOGRAPHY

- 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

Cybercrime
Research Institute

PORNOGRAPHY

- Thousands of pornographic movies and pictures are available for free download in **Filesharing-Systems**
- Current researches highlight, that pornographic material is among the most popular contents distributed via Filesharing-Systems



Cybercrime
Research Institute

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)

Picture removed in print version
Bild zur Druckoptimierung entfernt

Film Laboratory

Cybercrime
Research Institute

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

Picture removed in print version
Bild zur Druckoptimierung entfernt

Video Camera

Cybercrime
Research Institute

CHILD PORNOGRAPHY

- Today child pornography is available online
- Global phenomenon
- Influences the way how child pornography is distributed. Today it is possible to host files anywhere in the world and make it available for any user
- Means of distribution are classic services like WWW and email but also less popular services like filesharing

Picture removed in print version
Bild zur Druckoptimierung entfernt

SOURCE: Steel, Child Ab & Neg. 09, 563

Cybercrime
Research Institute

ONLINE GAMES

- Hugh interest in Online Games
- Secondlife has several million users
- Companies like Microsoft and Nissan are present
- Includes a virtual currency (L$ - Linden Dollar)
- First US$ Millionaire "Anshe Chung" who earned 270.000.000 L$ by developing and selling "real estate"
  (FTD 28.11.2006)

Cybercrime
Research Institute

ONLINE GAMES

- Increasing number of links between the virtual world and the real world
- L$ as well as SL-objects are offered on Ebay
- First cases of "virtual theft"