CYBERCRIME

LEGAL FOUNDATION AND ENFORCEMENT FUNDAMENTALS

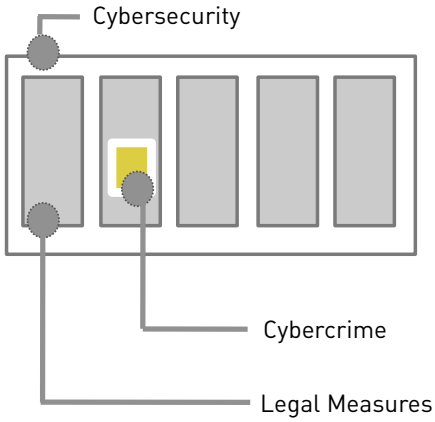
ITU Regional Cybersecurity Forum for Europe and the Commonwealth of Independent States (CIS)
8th October 2008

Dr. Marco Gercke
Lecturer for Criminal Law / Cybercrime, Faculty of Law, Cologne University

LEGAL FOUNDATION

- One element of a Cybersecurity Strategy is the development of a legal framework
- Part of the legal framework is the strengthening of a fight against Cybercrime
- Without the ability to investigate Cybercrime further attacks of the offender can not be prevented
- Legal framework can in this context help to build confidence for users and businesses

CYBERSECURITY / CYBERCRIME



OPEN FOR NON-MEMBERS

- Convention on Cybercrime has become the de-facto legal standards
- Widely supported by key players
- Convention is open for any non member

Art. 37 - Accession to the Convention

After the entry into force of this Convention, the Committee of Ministers of the Council of Europe, after consulting with and obtaining the unanimous consent of the Contracting States to the Convention, may invite any State which is not a member of the Council and which has not participated in its elaboration to accede to this Convention. The decision shall be taken by the majority provided for in Article 20.d. of the Statute of the Council of Europe and by the unanimous vote of the representatives of the Contracting States entitled to sit on the Committee of Ministers.

3 ISSUES

- The international community needs to be involved in the further development of the Convention
- Legal response to new challenges should be discussed
- Training is required

CYBERCRIME GUIDE

- Challenge

RECENT DEVELOPMENT

- Intensive discussion about new investigation instruments
- Remote forensic software tools
- In 2001 reports pointed out that the FBI developed a keystroke logger hat can be remotely installed on the computer system of a suspect
- In 2007 the FBI requested an order to use a software (CIPAV (Computer and Internet Protocol Address Verifier) to identify an offender that used measures to hide his identity while posting threatening messages

CIPAV

Picture removed in print version

ANONYMOUS COMMUNICATION

Example (Public Internet terminal)

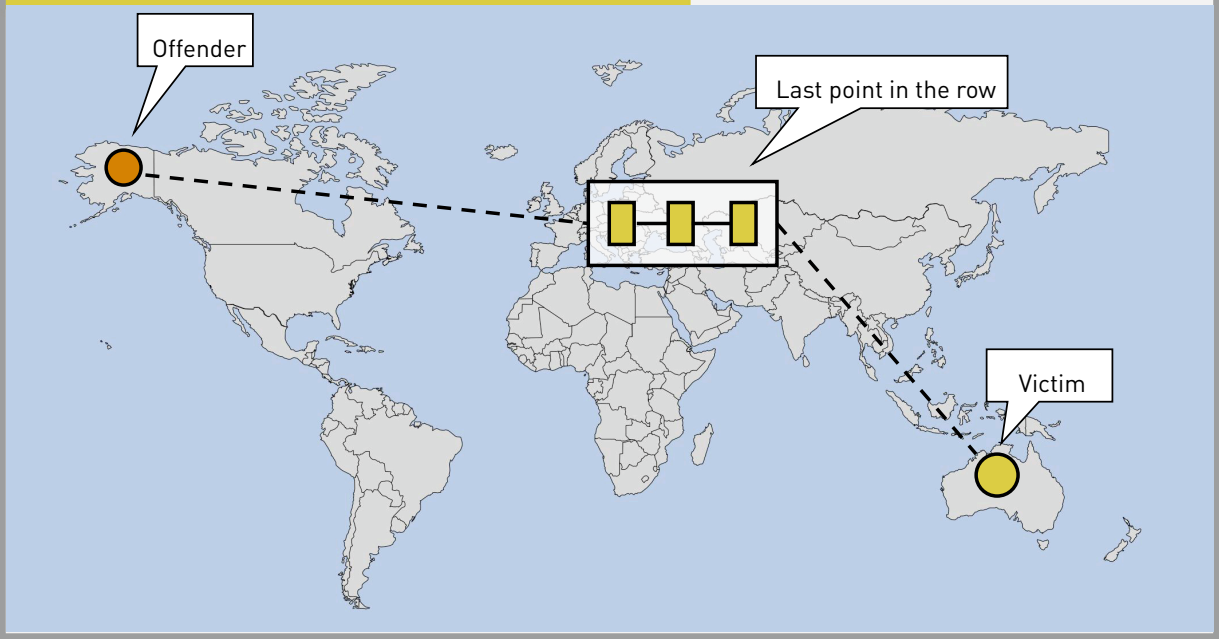
Picture removed in print version

Anonymous communication can be reached by:

- Use of public terminals
- Use of open wireless networks
- Hacked (closed) networks

ANONYMOUS COMMUNICATION

ANONYMOUS COMMUNICATION



ENCRYPTION

PGP

Picture removed in print version

- Encryption is the process of obscuring information to make it unreadable without special knowledge
- Encryption can be used to ensure secrecy
- Encryption can be used to hide the fact that encrypted messages are exchanged
- Encryption used by criminals can lead to difficulties collecting the necessary evidence
- E-Mails, VoIP comminication, files

GLOBAL PHENOMENON

- Availability of encryption technology is a global challenge
- Powerful software tool that enable are available on a large scale in the Internet
- Some of the latest versions of operating systems contain encryption technology

MICROSOFT BITLOCKER

Picture removed in print version

BREAKING A KEY

- Brute Force Attack: Method of defeating a cryptographic scheme by trying a large number of possibilities; for example, exhaustively working through all possible keys n order to decrypt a message
- Gaps in the encryption software
- Dictionary-based attack
- Social Engineering
- Classic search for hints
- Need for legislative approaches?

How long it takes to break a key

Picture removed in print version

SOLUTION

Technical solutions (with legal component)

- Magic Lantern (US)
- Remote Forensic Software (Germany)

Legal solution

- Use of keyloggers
- Various restrictions on import/export and use of encryption technology
- UK: Obligation to disclose password (Sec. 49 of the UK Investigatory Powers Act 2000)

MAGIC LANTERN

Picture removed in print version

3 ISSUES

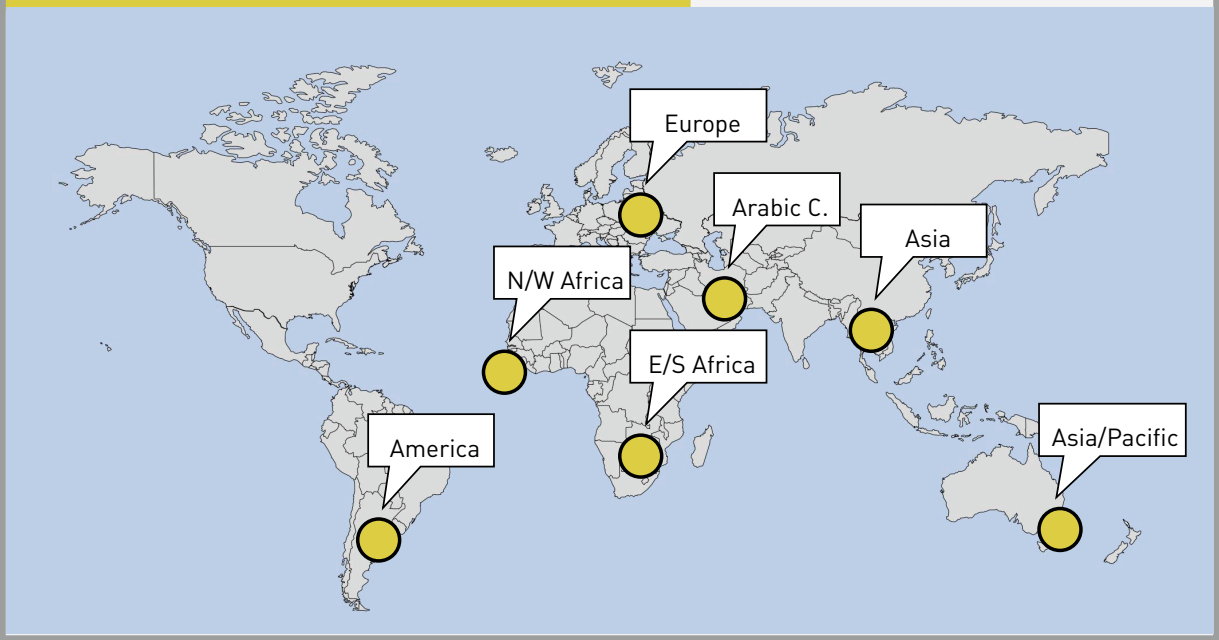
- The international community needs to be involved in the further development of the Convention
- Legal response to new challenges should be discussed
- Training is required

TRAINING

Various Organisations provide Cybercrime training

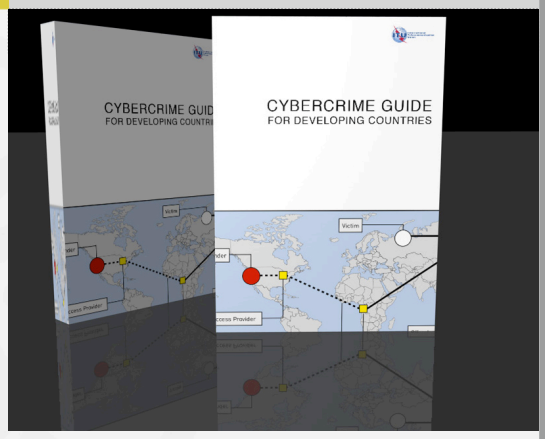
- UN
- ITU
- EU
- CoE
- OSCE
- OECD
- Worldbank
- IMF

ITU-D REG. FORUM 07/08



CYBERCRIME GUIDE

ITU GUIDE



- Aim: Providing a guide that is focussing on the demands of developing
- Including recent developments

Content

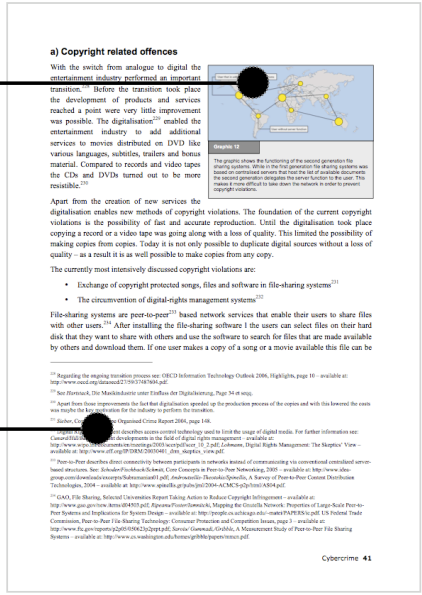
- Phenomenon of Cybercrime
- Challenges of Fighting Cybercrime
- Elements of an Anti-Cybercrime Strategy
- Explanation of legal solutions
  - Substantive Criminal Law
  - Procedural Law
  - International Cooperation

CYBERCRIME GUIDE

ITU 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.[229] Before the transition took place the development of products and services reached a point were very little improvement was possible. The digitalisation[230] 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]

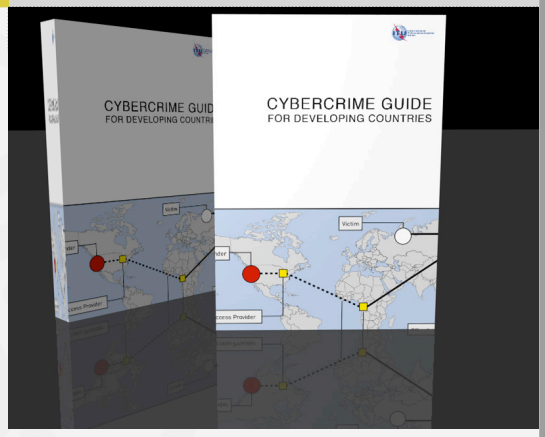
File-sharing systems are peer-to-peer[233] based network services that enable their users to share files with other users.[234] After installing the file-sharing software I the users can select files on their hard disk that they want to share with others and use the software to search for files that 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

Cybercrime 41

CYBERCRIME GUIDE

ITU GUIDE

- Focus of the Guide



CONTACT

THANK YOU FOR YOUR ATTENTION

Dr. Marco Gercke
Niehler Str. 35
D-50733 Cologne

www.cybercrime.de