**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
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
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
Anonymous communication can be reached by:

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

Offender

Last point in the row

Victim

ENCRYPTION

- 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 communication, 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

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 in order to decrypt a message

- Gaps in the encryption software

- Dictionary-based attack

- Social Engineering

- Classic search for hints

- Need for legislative approaches?
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)

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
Various Organisations provide Cybercrime training

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

ITU-D REG. FORUM 07/08

- Europe
- Arabic C.
- Asia
- N/W Africa
- E/S Africa
- America
- Asia/Pacific
CYBERCRIME 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

Examples and Explanation

References and Sources (if available from publicly available sources)
• Focus of the Guide

**CONTACT**

THANK YOU FOR YOUR ATTENTION

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

www.cybercrime.de