CYBERCRIME

LEGAL FOUNDATION AND ENFORCEMENT FUNDAMENTALS

ITU Regional Cybersecurity Forum for Asia-Pacific and Seminar on the Economics of Cybersecurity
17th July 2008

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

LEGAL FOUNDATION

CYBERSECURITY / CYBERCRIME

Picture removed in print version

- 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

CYBERCRIME GUIDE

ITU GUIDE

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

Content

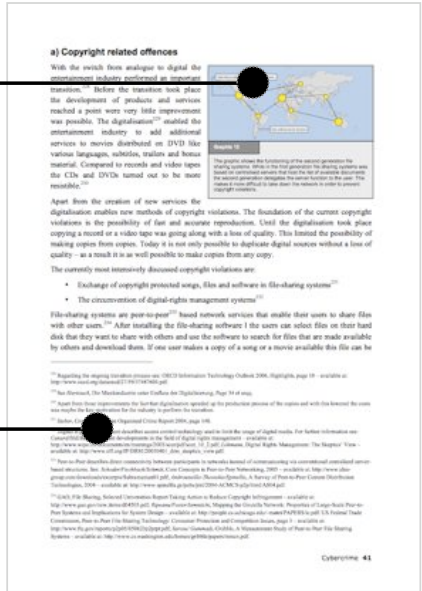
- Phenomenon of Cybercrime
- Challenges of Fighting Cybercrime
- Elements of an Anti-Cybercrime Strategy
- Explanation of legal solutions
  - Substantive Criminal Law
  - Procedural Law
  - International Cooperation

CYBERCRIME GUIDE

ITU GUIDE

Examples and Explanation

References and Sources
(if available from publicly available sources)


a) Copyright related offences

LEGAL CHALLENGE

Desirable:

- Adequate Criminalisation
- Adequate Instruments for Law Enforcement
- Ability for International Cooperation

To be taken into consideration:

- Protection of the interest of the user
- No Over-Crimininalisation

CONVENTION ON CYBERCRIME

ITU GUIDE

Picture removed in print version

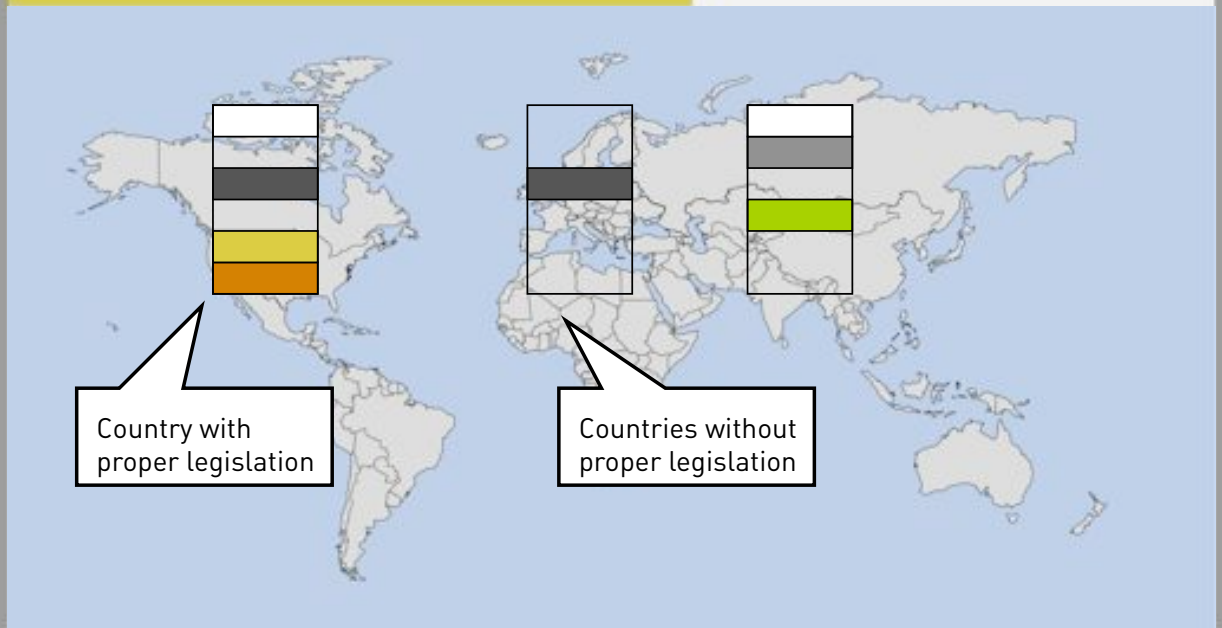
- The Convention on Cybercrime

WHY HARMONISING LAWS

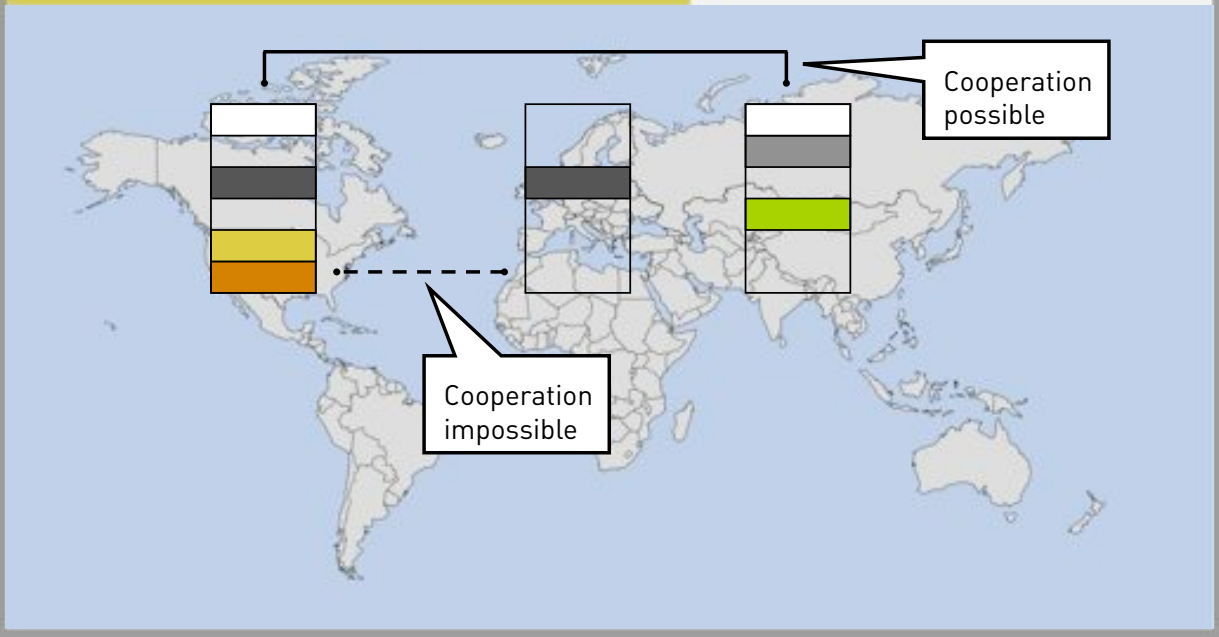
1. Technical aspect: Investigations depend on international cooperation of investigation authorities

2. Legal aspect: Principle of National Sovereignty limits the possibilities of transnational investigations without international cooperation

CURRENT SITUATION



CURRENT SITUATION

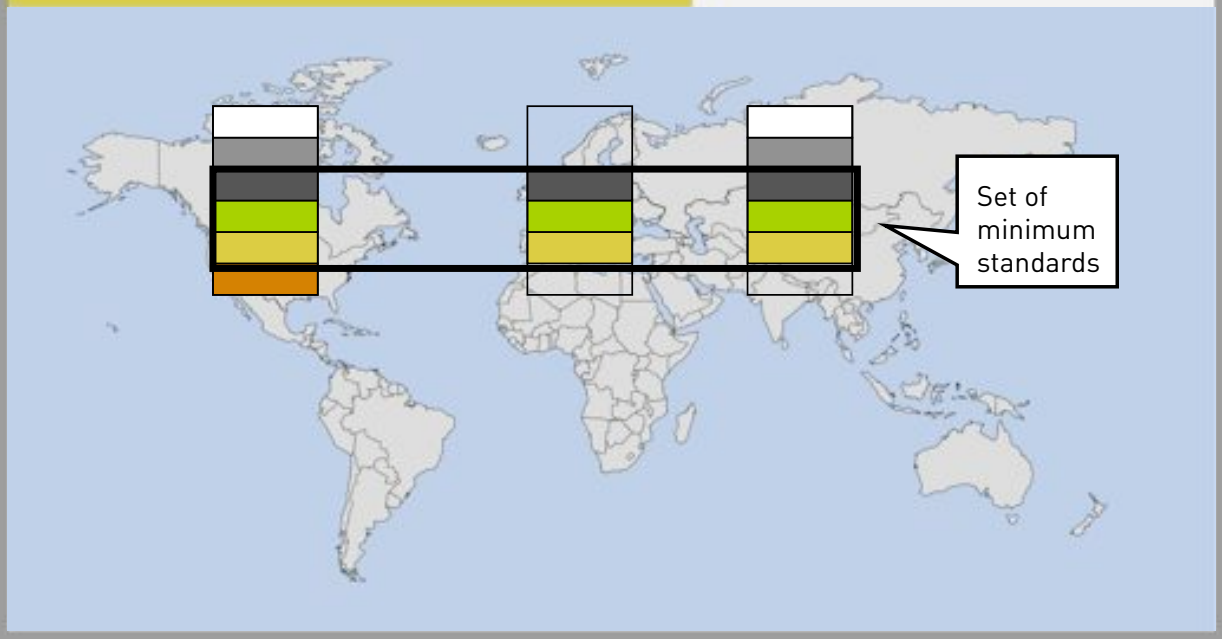


INTERNATIONAL UNIFICATION

- Attempts for improve the Fight against Cybercrime a number of International Organisation such as
  - OECD
  - G8
  - UN
  - European Union
  - Council of Europe (CoE)

- Until now the CoE Convention on Cybercrime is the only international legal framework with a broad approach

AIM OF THE CONVENTION



STRUCTURE

- Section 1: Substantive criminal law
- Section 2: Procedural law
- Section 3: Jurisdiction
- International cooperation

- Additional protocol (xenophobic material)

Not covered:

- Responsibility of Internet Providers

SUBSTANTIVE CRIMINAL LAW

- Art. 1 Definition
- Art. 2 Illegal Access
- Art. 3 Illegal Interception
- Art. 4 Data Interference
- Art. 5 System Interference
- Art. 6 Misuse of Devices
- Art. 7 Computer-related Forgery
- Art. 8 Computer-related Fraud
- Art. 9 Offences related to Child Pornography
- Art. 10 Offences related to Copyright Violations

Art. 2 - Illegal Access

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, the access to the whole or any part of a computer system without right.

SUBSTANTIVE CRIMINAL LAW

- Art. 11 Attempt, aiding, abetting
- Art. 12 Corporate Liability
- Art. 13 Sanction an measures

Art. 11 - Attempt, aiding and abetting

Each Party shall adopt such legislative and other measures as may be necessary to establish as criminal offences under its domestic law, when committed intentionally, aiding or abetting the commission of any of the offences established in accordance with Articles 2 through 10 of the present Convention with intent that such offence be committed.

PROCEDURAL LAW

- Art. 14 Scope
- Art. 15 Conditions, Safeguards
- Art. 16 Expedited Preservation
- Art. 17 Expedited Disclosure
- Art. 18 Production Order
- Art. 19 Search and Seizure
- Art. 20 Real time Collection of Traffic Data
- Art. 21 Real time Interception of Content Data
- Art. 22 Jurisdiction

Art. 16 - Expedited preservation

Each Party shall adopt such legislative and other measures as may be necessary to enable its competent authorities to order or similarly obtain the expeditious preservation of specified computer data, including traffic data, that has been stored by means of a computer system, in particular where there are grounds to believe that the computer data is particularly vulnerable to loss or modification.

INTERNATIONAL COOPERATION

- Art. 23 General principle
- Art. 24 Extradition
- Art. 25 General principle related to mutual assistance
- Art. 26 Spontaneous Information
- Art. 27 Absence of International Agreements
- Art. 28 Confidentiality and limitations of use
- Art. 29 Expedited preservation
- Art. 30 Expedited disclosure
- Art. 31 Access to stored computer data
- Art. 32 Trans-border access to stored computer data

INTERNATIONAL COOPERATION

- Art. 33 Real-time collection of traffic data
- Art. 34 Interception of content data

24/7 NETWORK

- Art. 35 24/7 Network

Art. 35 - 24/7

Each Party shall designate a point of contact available on a twenty-four hour, seven- day-a -week basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence.
[...]

SIGNATURES UNTIL 2007

DETAILS ABOUT SIGNATURES

43 States signed the Convention 185 ("Convention on Cybercrime") until March 2006, among them are 4 Non-Members. Details are available unter www.coe.int

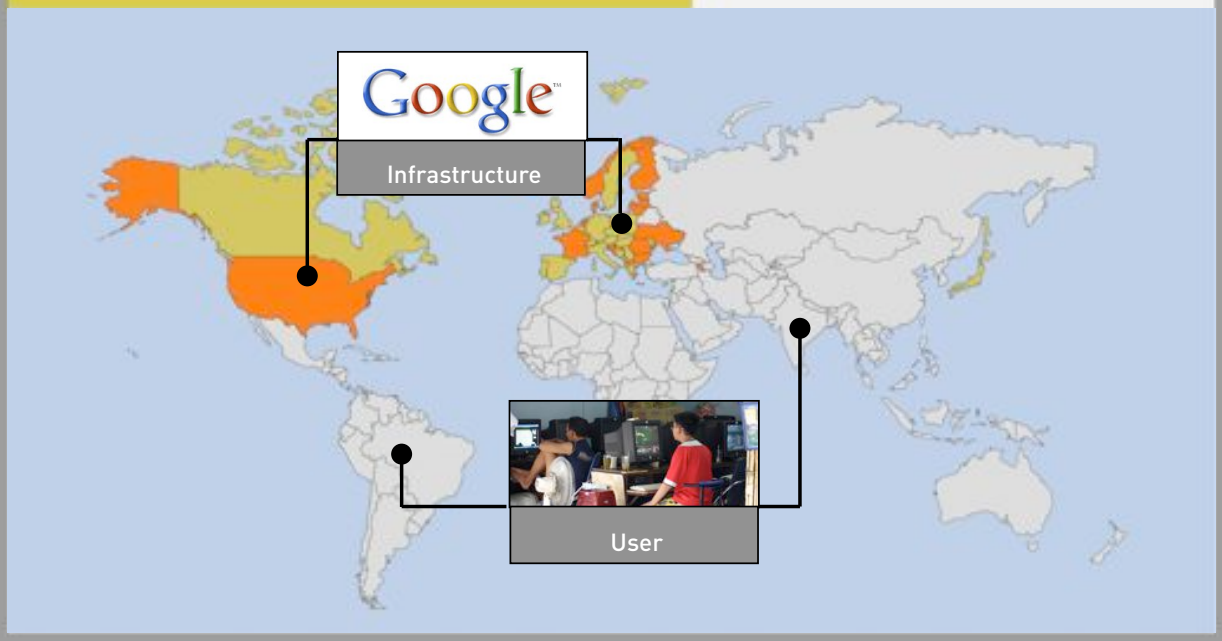
OPEN FOR NON-MEMBERS

- 4 Non-Members were involved in the drafting of the convention and signed the convention
- Convention is open for any non member
- Costa Rica and Mexico were recently invited to access the Convention

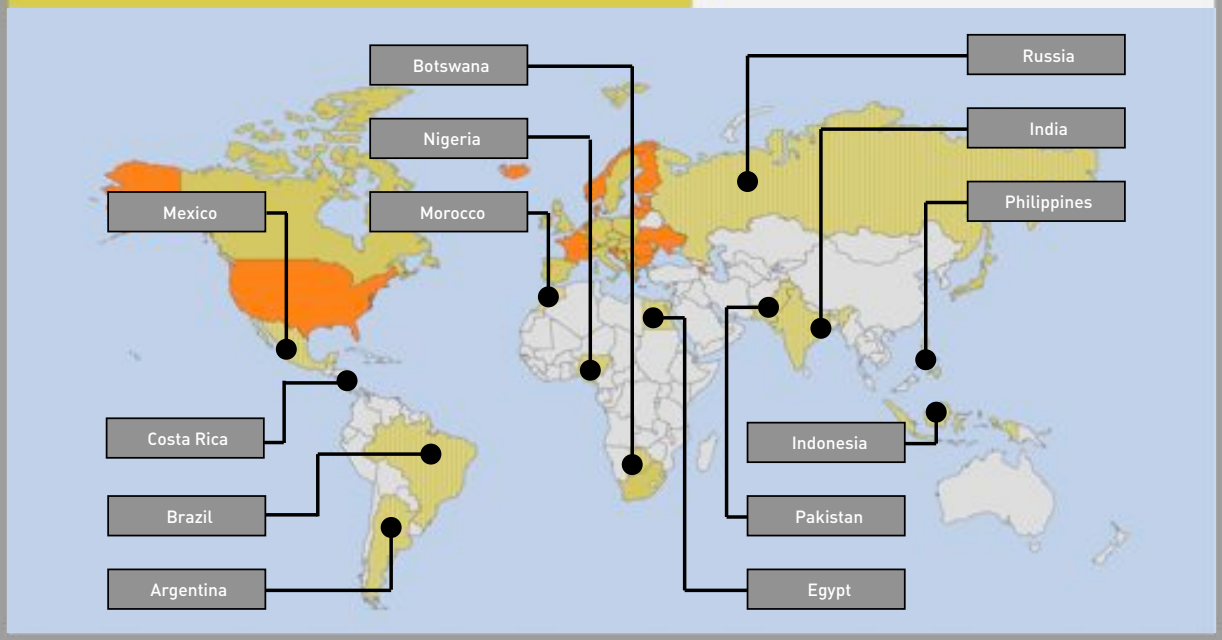
Art. 37 - Accession to the Convention

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.

RATIFICATION



MODEL LAW



WHY SIGNING THE CONVENTION

- An effective fight against Cybercrime requires the implementation of the provisions of the Convention but not the signature of the Convention
- But with the signature of the Convention the states become member of the Cybercrime Committee (T-CY)
- The Committee is the institution that will discuss further amendments to the Convention
- The signature therefore enables the states to participate in this development

LEGAL CHALLENGE

ITU GUIDE

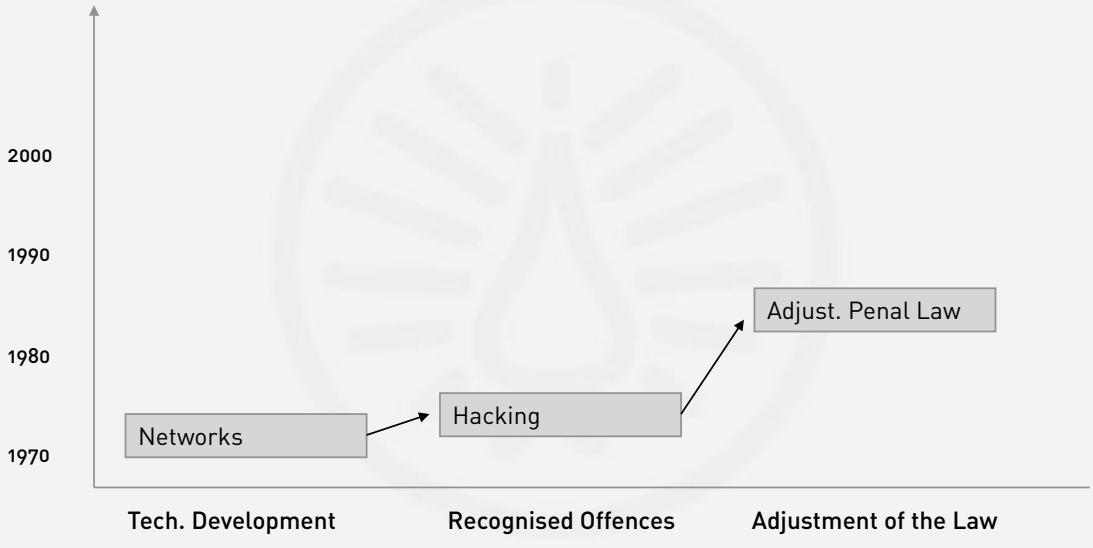
Picture removed in print version

The Challenge of Fighting Cybercrime

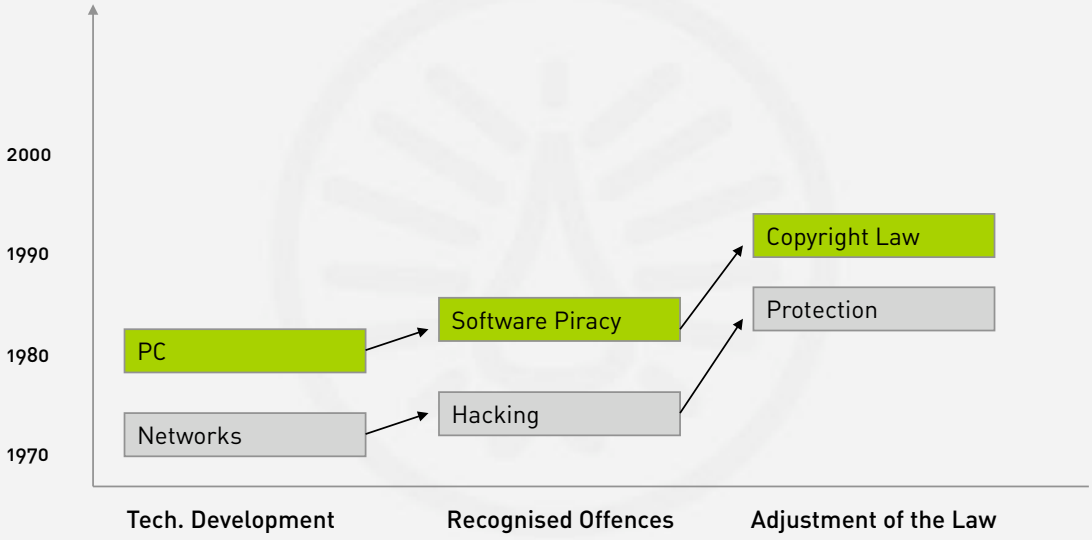
OFFENCES NOT COVERED

- The challenges related to the fight against Cybercrime are not limited to the development of an adequate legislation
- Set up of specialised units, providing equipment and regular training
- One of the main challenges related to legal aspects is to keep the law updated

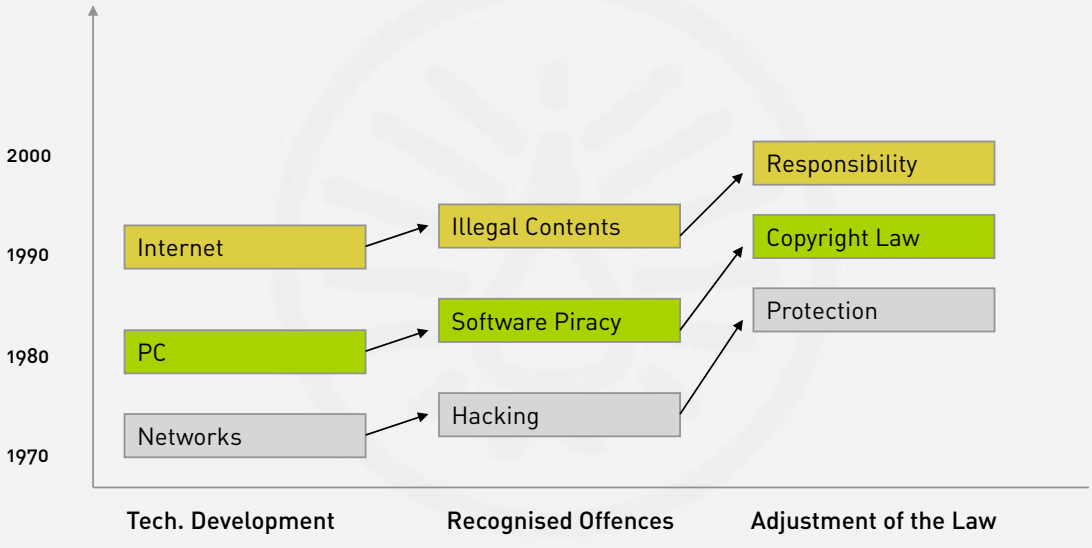
LAW ADJUSTMENT (GERMANY)



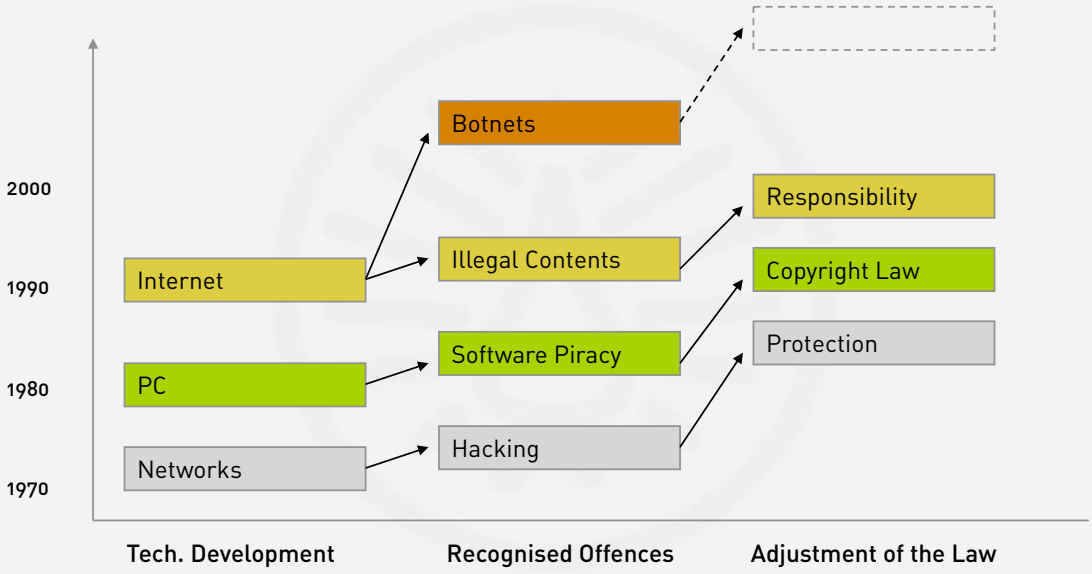
LAW ADJUSTMENT



LAW ADJUSTMENT



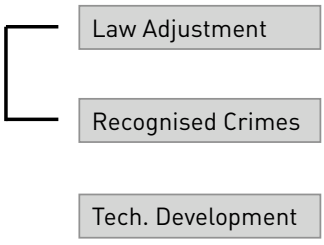
LAW ADJUSTMENT



LAW ADJUSTMENT

- To cut down the time between the recognition of crimes and the adjustment of law is the main challenge
- Challenge especially for the Continental European law systems that are not based on case law
- Advantage for the more flexible Anglo -American-System

Challenge



CURRENT DEVELOPMENT

ITU GUIDE

Picture removed in print version

- Current Development

EXPLOIT AUCTION

Example (http:wslabi.com)

Picture removed in print version

- Information about system vulnerabilities are published on websites
- In addition these information are offered for sale by some businesses
- Information can be used to increase security as well as to commit computer-related offences

RECENT DEVELOPMENT

- New scams related to online-games
- Closer relations between virtual worlds and the real world (exchange of virtual currencies)
- Highly sophisticated phishing-scams

ONLINE GAMES (SECONDLIFE.COM)

Picture removed in print version

RECENT DEVELOPMENT

- Current analysis proof that up to a quarter of all computer connected to the internet could be used by criminals as they belong to "botnets"

  Souce: BBC report "Criminals 'may overwhelm the web"

- Some analysis go even beyond that number
- Botnets can for example be used to send out Spam or carry out a DoS attack
- Use of Botnets makes the identification of the offender difficult

Botnets (www.shadowserver.org)

Picture removed in print version

RECENT DEVELOPMENT

- Increasing activities of terrorist organisations
- Not concentrating on attacks against critical infrastructure - information, recruitment, communication, ...
- Continuing improvement of methods protecting communication from lawful interception
- Integration of the Internet in terrorist financing activities

CYBERTERRORISM

Picture removed in print version

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

CYBERCRIME GUIDE

ITU GUIDE

Picture removed in print version

- Challenge

CHALLENGES

- Dependence of the society on information technology
- Availability and power of devices that can be used to commit a crime
- Availability of Information
- Languages
- Missing control instruments
- International dimension
- Speed of information exchange
- Speed of the technological development, power and vulnerability of devices
- Anonymous communication
- Encryption

POSSIBILITIES

- There are no doubts that the ongoing improvement of information technology enables the law enforcement agencies to carry out investigations that were not possible previously
- Automated search for key-words / hash-values
- Great chance for public private partnership (Microsoft's CETS)

EXAMPLE CHILD PORNOGRAPHY

Picture removed in print version

AUTOMATE

- Computer and Networks enable offenders to automate attacks
- Within minutes millions of spam mails can be send out without generating high costs - sending out one million regular letters would be very expensive and take days
- Special software products enable automatic attacks against computer systems

Example (Hackerwatch.org)

Picture removed in print version

AVAILABILITY OF DEVICES

- Internet connected devices as **tool** and **target**
- The number of people who have access to the internet is still growing fast
- New ways of access to networks are implemented (UMTS, WLAN,)
- Capacity of Computers has increased (great potential)
- Number of operations controlled by the use of networks increased

Examples

Misuse of open WLAN-Access Point to hide identity; Terrorists communication via VoIP using encryption technology;

AVAILABILITY OF INFORMATION

- Secret Information are available in the Internet
- Available especially through search engines
- "Google hacking"

EXAMPLE

Picture removed in print version

AVAILABILITY OF INFORMATION

- Services like Google Earth were reported to be used in several attacks - among them attacks against British troops in Afghanistan and the planed attacks against an airport in the US

Telegraph.co.uk (13.01.2007)

Terrorists attacking British bases in Basra are using aerial footage displayed by the Google Earth internet tool to pinpoint their attacks, say Army intelligence sources.Documents seized during raids on the homes of insurgents last week uncovered print-outs from photographs taken from Google.The satellite photographs show in detail the buildings inside the bases and vulnerable areas such as tented accommodation, lavatory blocks and where lightly armoured Land Rovers are parked.Written on the back of one set of photographs taken of the Shatt al Arab Hotel, headquarters for the 1,000 men of the Staffordshire Regiment battle group, officers found the camp's precise longitude and latitude. "This is evidence as far as we are concerned for planning terrorist attacks," said an intelligence officer with the Royal Green Jackets battle group. "Who would otherwise have Google Earth imagery of one of our bases?

AVAILABILITY OF INFORMATION

- Robots used by Search-engines can lead the disclose of secret information
- Handbooks on how to build explosives and construct chemical and even nuclear devices are available
- Internet sources have been used by the offenders in a number of recent attacks

TERRORIST HANDBOOK

Picture removed in print version

AVAILABILITY OF INFORMATION

- Information regarding the construction of weapons were available long time before the Internet was developed
- Ragnar's Action Encyclopaedia of Practical Knowledge and Proven Techniques
- Approaches to criminalise the publication of information that can be used to

RAGNAR'S ENCYCLOPEDIA

Picture removed in print version

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 comminication, files

PGP

Picture removed in print version

LIVE DEMONSTRATION

Text Encryption

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

LIVE DEMONSTRATION

How long does it take to break a key?

SOLUTION

Technical solutions (with legal component)

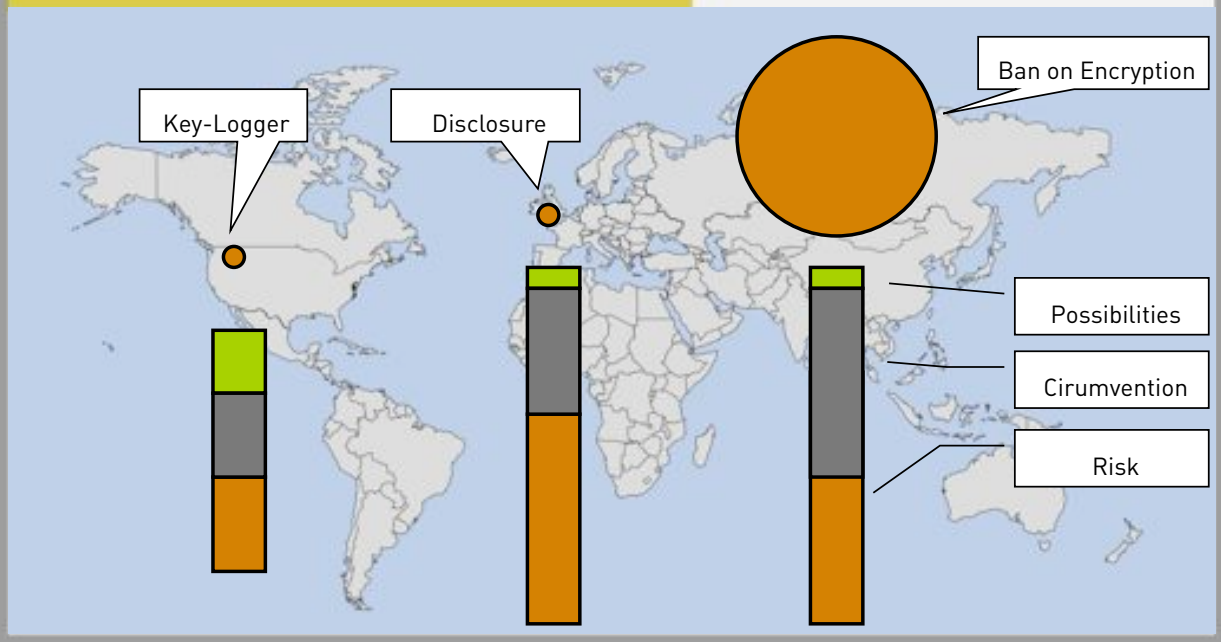
- Magic Lantern (US)
- Remote Forensic Software (Germany)

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

COMPARING APPROACHES



CONTACT

THANK YOU FOR YOUR ATTENTION

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

www.cybercrime.de