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**

- Aim: Providing a guide that is focusing 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)
**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-Criminalisation

**CONVENTION ON CYBERCRIME**

- 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

Country with proper legislation

Countries without proper legislation
CURRENT SITUATION

Cooperation impossible

Cooperation possible

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

Set of minimum standards

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
<table>
<thead>
<tr>
<th>Art.</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Definition</td>
</tr>
<tr>
<td>2</td>
<td>Illegal Access</td>
</tr>
<tr>
<td>3</td>
<td>Illegal Interception</td>
</tr>
<tr>
<td>4</td>
<td>Data Interference</td>
</tr>
<tr>
<td>5</td>
<td>System Interference</td>
</tr>
<tr>
<td>6</td>
<td>Misuse of Devices</td>
</tr>
<tr>
<td>7</td>
<td>Computer-related Forgery</td>
</tr>
<tr>
<td>8</td>
<td>Computer-related Fraud</td>
</tr>
<tr>
<td>9</td>
<td>Offences related to Child Pornography</td>
</tr>
<tr>
<td>10</td>
<td>Offences related to Copyright Violations</td>
</tr>
<tr>
<td>11</td>
<td>Attempt, aiding, abetting</td>
</tr>
<tr>
<td>12</td>
<td>Corporate Liability</td>
</tr>
<tr>
<td>13</td>
<td>Sanction an measures</td>
</tr>
</tbody>
</table>
### PROCEDURAL LAW

<table>
<thead>
<tr>
<th>Article</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 14</td>
<td>Scope</td>
</tr>
<tr>
<td>Art. 15</td>
<td>Conditions, Safeguards</td>
</tr>
<tr>
<td>Art. 16</td>
<td>Expedited Preservation</td>
</tr>
<tr>
<td>Art. 17</td>
<td>Expedited Disclosure</td>
</tr>
<tr>
<td>Art. 18</td>
<td>Production Order</td>
</tr>
<tr>
<td>Art. 19</td>
<td>Search and Seizure</td>
</tr>
<tr>
<td>Art. 20</td>
<td>Real time Collection of Traffic Data</td>
</tr>
<tr>
<td>Art. 21</td>
<td>Real time Interception of Content Data</td>
</tr>
<tr>
<td>Art. 22</td>
<td>Jurisdiction</td>
</tr>
</tbody>
</table>

**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

<table>
<thead>
<tr>
<th>Article</th>
<th>Topic</th>
</tr>
</thead>
<tbody>
<tr>
<td>Art. 23</td>
<td>General principle</td>
</tr>
<tr>
<td>Art. 24</td>
<td>Extradition</td>
</tr>
<tr>
<td>Art. 25</td>
<td>General principle related to mutual assistance</td>
</tr>
<tr>
<td>Art. 26</td>
<td>Spontaneous Information</td>
</tr>
<tr>
<td>Art. 27</td>
<td>Absence of International Agreements</td>
</tr>
<tr>
<td>Art. 28</td>
<td>Confidentiality and limitations of use</td>
</tr>
<tr>
<td>Art. 29</td>
<td>Expedited preservation</td>
</tr>
<tr>
<td>Art. 30</td>
<td>Expedited disclosure</td>
</tr>
<tr>
<td>Art. 31</td>
<td>Access to stored computer data</td>
</tr>
<tr>
<td>Art. 32</td>
<td>Trans-border access to stored computer data</td>
</tr>
</tbody>
</table>
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.
[...]

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

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.
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

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)

- Technological Development
- Recognised Offences
- Adjustment of the Law

- Networks
- Hacking
- Adjust. Penal Law
LAW ADJUSTMENT

- Technical Development
- Recognised Offences
- Adjustment of the Law

1970:
- PC
- Networks

1980:
- Software Piracy
- Hacking

1990:
- Internet

2000:
- Illegal Contents

Copyright Law, Protection, Responsibility

Recognition of Offences, Adjustment of the Law
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
CURRENT DEVELOPMENT

- Current Development

EXPLOIT AUCTION

- 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

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”
  
  *Source: 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
**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

**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
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)

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
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”
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 planned attacks against an airport in the US.

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?”

- Robots used by Search-engines can lead to 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.
### 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

### 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

---

**LIVE DEMONSTRATION**

Text Encryption
GLOBAL PHENOMENON

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

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?

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)

COMPARING APPROACHES

Key-Logger Disclosure

Ban on Encryption
Possibilities
Cirumvention
Risk
CONTACT

THANK YOU FOR YOUR ATTENTION

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

www.cybercrime.de