CYBERCRIME

THE CHALLENGE OF FIGHTING CYBERCRIME IN DEVELOPING COUNTRIES AND THE ROLE OF NATIONAL, REGIONAL AND INTERNATIONAL CYBERCRIME LEGISLATION

Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection
Buenos Aires, Argentina
18. October 2008

Dr. Marco Gercke

CYBERCRIME GUIDE

ITU GUIDE

Picture removed in print version

- 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

Picture removed in print version

- Phenomenon

CLASSIC IT-CRIMES

HACKING

Picture removed in print version

- Illegal access to a computer system was one of the dominating crimes in the early days of computer crimes
- Incredible technical development since that times
- Hacking attacks are still an important phenomenon - especially with regard to the automation of attacks
- But in addition a number of other offences were discovered

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

Example (http:wslabi.com)

Picture removed in print version

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

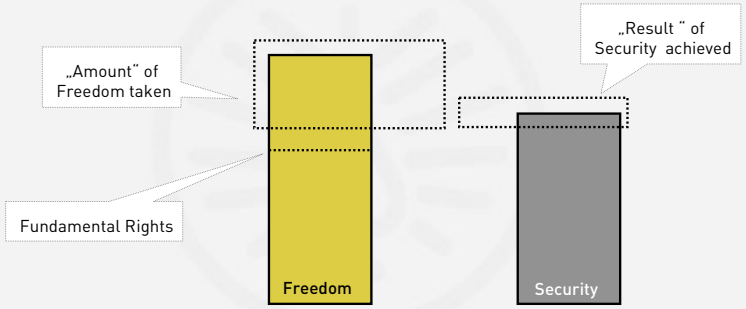
CIPAV

Picture removed in print version

- 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

LEGAL CONCERNS

- Well balanced adjustment



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 (Microsofts CETS)

EXAMPLE CHILD PORNOGRAPHY

Picture removed in print version

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

- 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

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

MICROSOFT BITLOCKER

Picture removed in print version

- 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

BREAKING A KEY

How long it takes to break a key

Picture removed in print version

- 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?

SOLUTION

MAGIC LANTERN

Picture removed in print version

Technical solutions (with legal component)

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

Legal solution

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

STEGANOGRAPHY

Steganography

Picture removed in print version

- Steganography is a technique used to hide information in some other information
- Example: Hiding a message in picture
- Technique can be used to keep the fact that the exchange of encrypted messages is taking place secret

CONCLUSION

INTERNET CAFE HANOI

Picture removed in print version

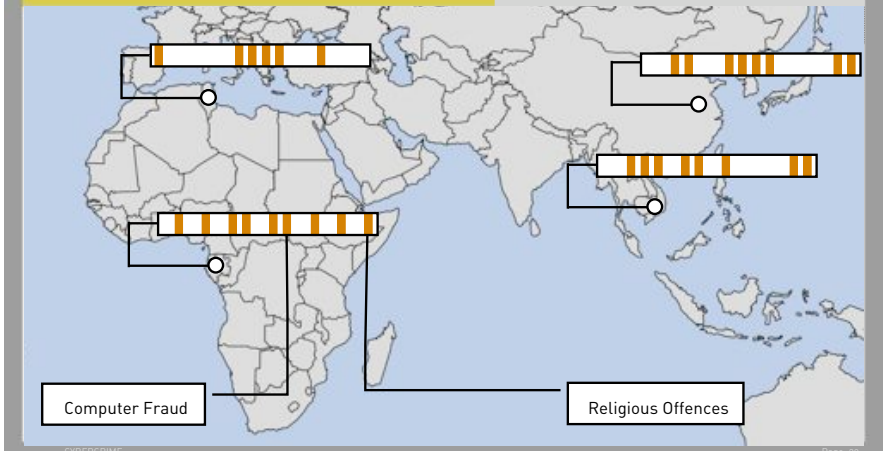
- Developing countries and Industrialised countries are facing similar challenges
- Does this implicate that existing Cybersecurity strategies developed by industrialised countries can simply be copied by the developing countries?

  Technical issues: **Maybe** (capacity)

  Legal issues: **Unlikely** (different system)
- Application of best practices

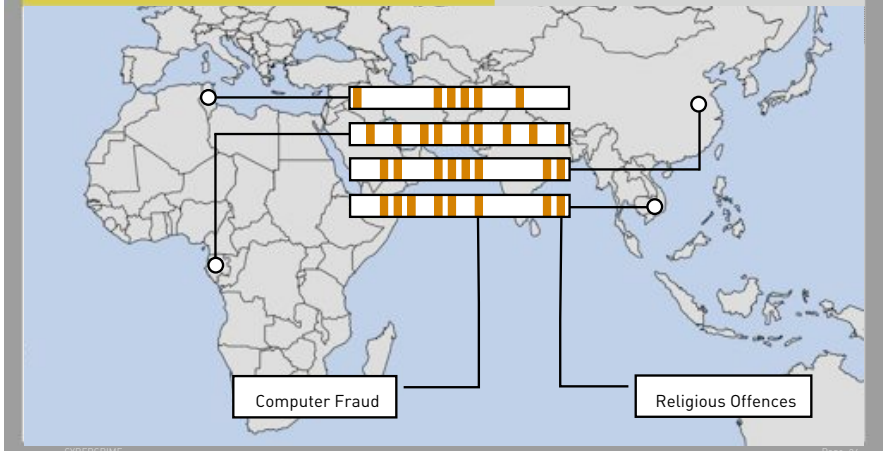
LEGAL SOLUTION

NATIONAL, REGIONAL, INTERNATIONAL



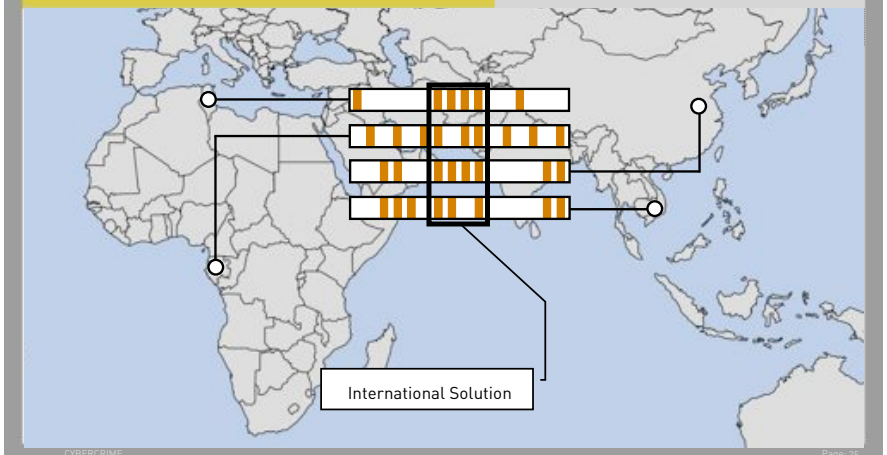
LEGAL SOLUTION

NATIONAL, REGIONAL, INTERNATIONAL



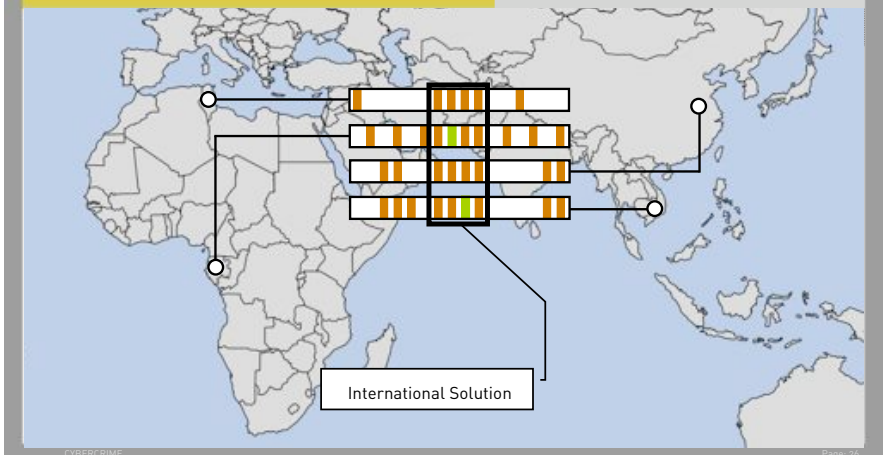
LEGAL SOLUTION

NATIONAL, REGIONAL, INTERNATIONAL



LEGAL SOLUTION

NATIONAL, REGIONAL, INTERNATIONAL



INTERNATIONAL SOLUTION

- Currently the Council of Europe Convention on Cybercrime is the only International Agreement that covers all relevant areas of Cybercrime Legislation (Substantive Criminal Law, Procedural Law, International Cooperation)
- Intention: Harmonisation of selected aspects of Cybercrime legislation
- Open for non-members

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.

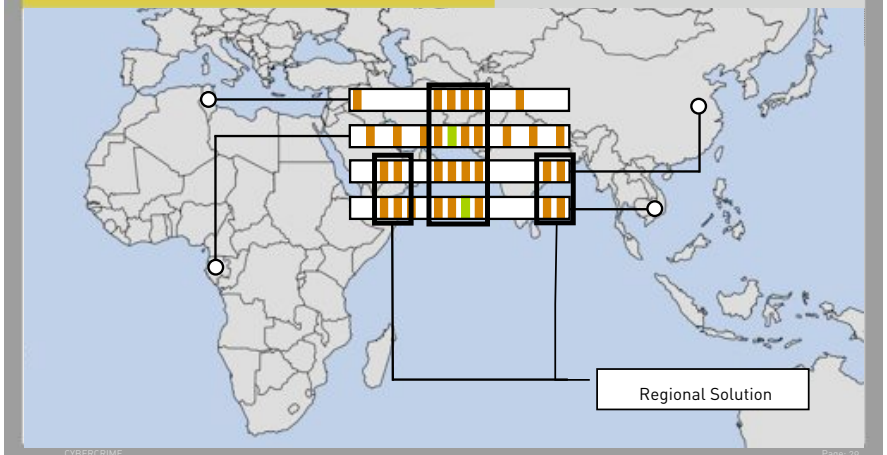
SIGNATURES UNTIL 2007

DETAILS ABOUT SIGNATURES

43 States signed the Convention 185 ("Convention on Cybercrime") until October 2007, among them are 4 Non-Members. Details are available unter www.coe.int

LEGAL SOLUTION

NATIONAL, REGIONAL, INTERNATIONAL

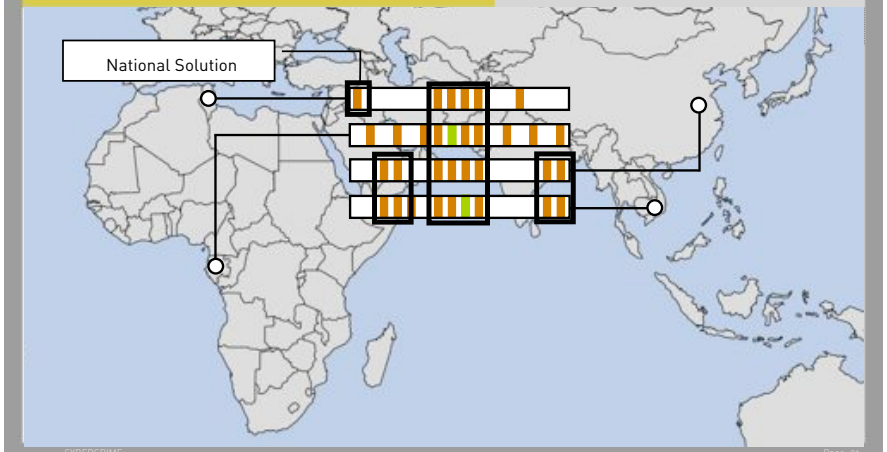


REGIONAL SOLUTION

- A number of regional initiatives
- Examples for current developments are the European Union, Gulf Cooperation Council (GCC)
- Advantage: Often comparable legal systems
- Regional agreements can supplement international agreements

LEGAL SOLUTION

NATIONAL, REGIONAL, INTERNATIONAL



REGIONAL & NATIONAL

EU COUNTRIES

Picture removed in print version

Can regional an national solutions work?

- One argument against regional and national solutions is the fact that the internet does not know any boarders and boundaries and therefore international solutions are necessary
- International dimension requires harmonisation to effectively fight Cybercrime
- It does not necessary exclude additional regional and national approaches

REGIONAL & NATIONAL

- Geo-tracking enables to keep geographic borders in times of the Internet
- It enables to exclude users with certain IP addresses from services
- The fact that the possibility to circumvent virtual or real border exists does not mean that there are no borders

BORDER

Picture removed in print version

THANK YOU FOR YOUR ATTENTION

gercke@cybercrime.de