CYBERCRIME

LEGAL FOUNDATION AND ENFORCEMENT FUNDAMENTALS

ITU Regional Cybersecurity Forum for Eastern and Southern Africa
26th July 2008

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

INDEX

TODAY

- Why should you implement legal measures?
- National, regional or International approaches?
- What to take into account?

TOMORROW

- What topics need to be covered?

- Why should you implement legal measures?

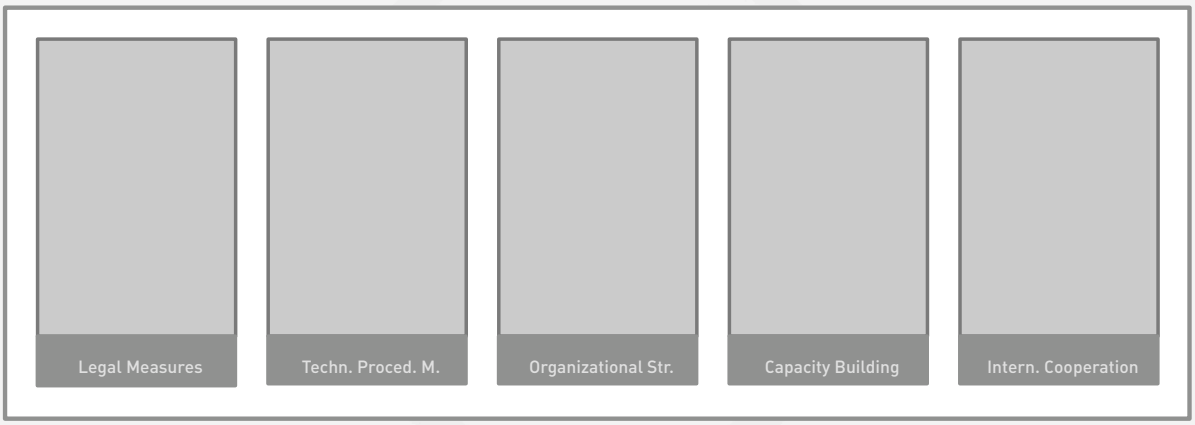
LEGAL FOUNDATION

GLOBAL CYBERSECURITY AGENDA

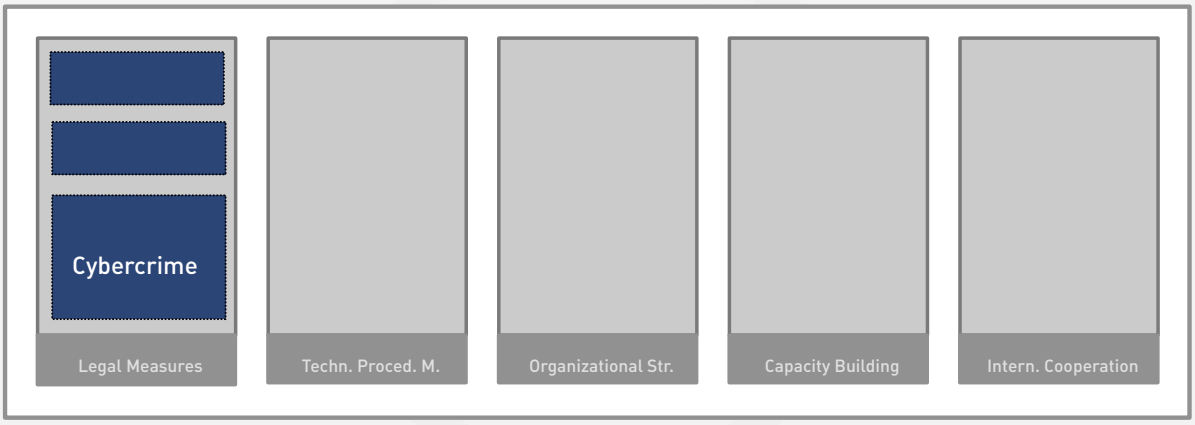
CYBERSECURITY

LEGAL FOUNDATION

5 PILLARS OF THE GCA



LEGAL FOUNDATION



LEGAL FOUNDATION

ITU

Picture removed in print version

ITU & HLEG

- Elaboration of strategies
- Analysing the possibilities and necessity of developing a model Cybercrime legislation

ITU-D

- Providing assistance within the implementation
- Providing information

LEGAL FOUNDATION

ITU

Picture removed in print version

ITU-D

- Providing assistance within the implementation (Self Assessment)
- Providing information (Conferences and Publications)

LEGAL FOUNDATION

- Part of the Self Assessement Toolkit is dealing with Cybercrime legislation
- Toolkit enables the countries to determine the status of the legal foundation

SELF ASSESSEMENT TOOLKIT

Picture removed in print version

CYBERCRIME GUIDE

- Aim: Providing a guide that is focussing on the demands of developing countries
- 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

ITU GUIDE

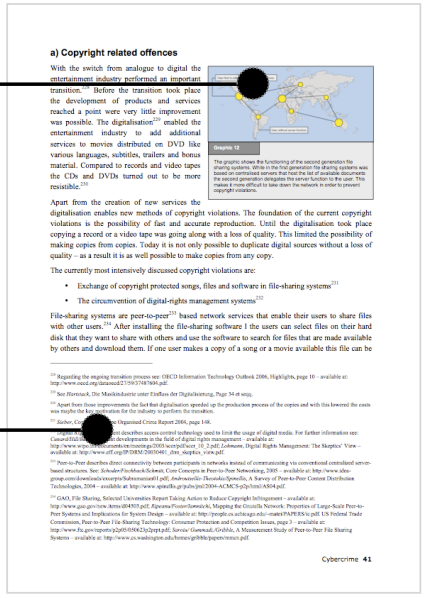
Picture removed in print version

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

[228] Regarding the ongoing transition process see: OECD Information Technology Outlook 2006, Highlights, page 10 – available at: http://www.oecd.org/dataoecd/23/59/37487604.pdf.

[229] See *Hornisch*, Die Musikindustrie unter Einfluss der Digitalisierung, Page 34 et seqq.

[230] Apart from those improvements the fact that digitalisation speeded up the production process of the copies and with this lowered the costs was maybe the key motivation for the industry to perform the transition.

[231] *Sieber*, Cyber Crime – Organised Crime Report 2004, page 148.

[232] [illegible] describes access control technology used to limit the usage of digital media. For farther information see: *Cameron/Frederick*, Recent developments in the field of digital rights management – available at: http://www.w3c.org/2001/03/wsws-popa/paper51/ *Lohmann*, Digital Rights Management: The Skeptics' View – available at: http://www.eff.org/IP/DRM/20030441_drm_skeptics_view.pdf.

[233] Peer-to-Peer describes direct connectivity between participants in networks instead of communicating via conventional centralised server-based structures. See: *Schoder/Fischbach/Schmitt*, Core Concepts in Peer-to-Peer Networking, 2005 – available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, A Survey of Peer-to-Peer Content Distribution Technologies, 2004 – available at: http://www.spinellis.gr/pubs/jnl/2004-ACMCS-p2p/html/ASS04.pdf.

[234] GAO, File Sharing, Selected Universities Report Taking Action to Reduce Copyright Infringement – available at: http://www.gao.gov/new.items/d04544t.pdf; *Ripeanu/Foster/Iamnitchi*, Mapping the Gnutella Network: Properties of Large-Scale Peer-to-Peer Systems and Implications for System Design – available at: http://people.cs.uchicago.edu/~matei/PAPERS/ic.pdf; US Federal Trade Commission, Peer-to-Peer File Sharing Technology: Consumer Protection and Competition Issues, page 3 – available at: http://www.ftc.gov/reports/p2p05/050623p2pprt.pdf; *Saroiu/ Gummadi/Gribble*, A Measurement Study of Peer-to-Peer File Sharing Systems – available at: http://www.cs.washington.edu/homes/gribble/papers/mmcn.pdf.

Cybercrime 41

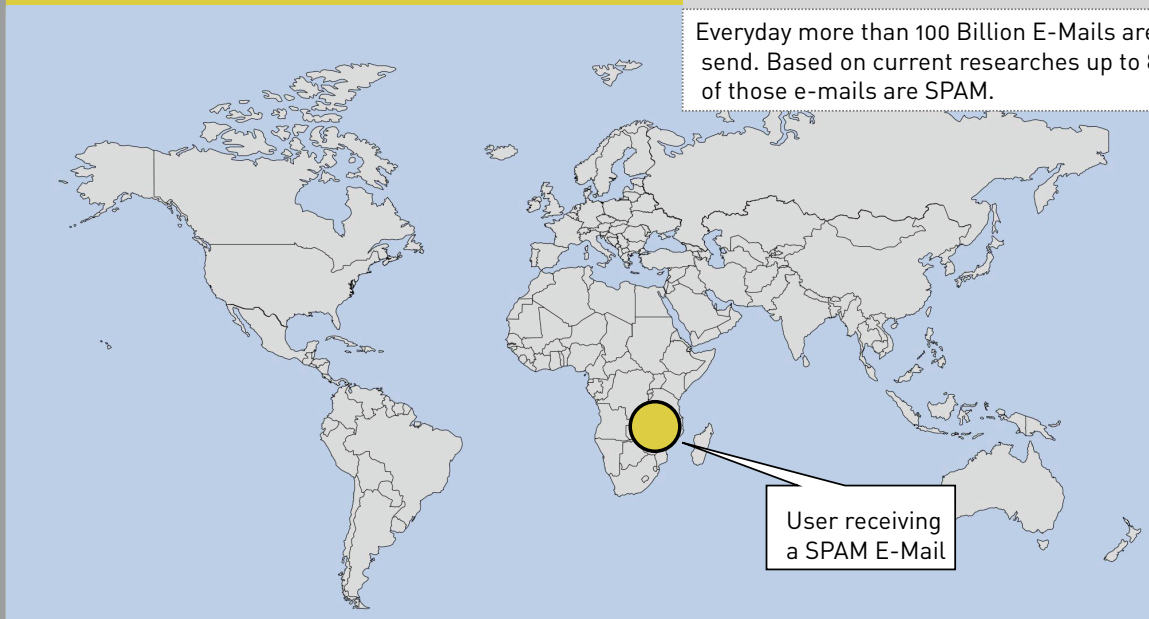
LEGAL MEASURES

- Why are legal measures an important aspect of a Cybersecurity Strategy?

IMPORTANCE OF LEGAL M.

BACKGROUND SPAM

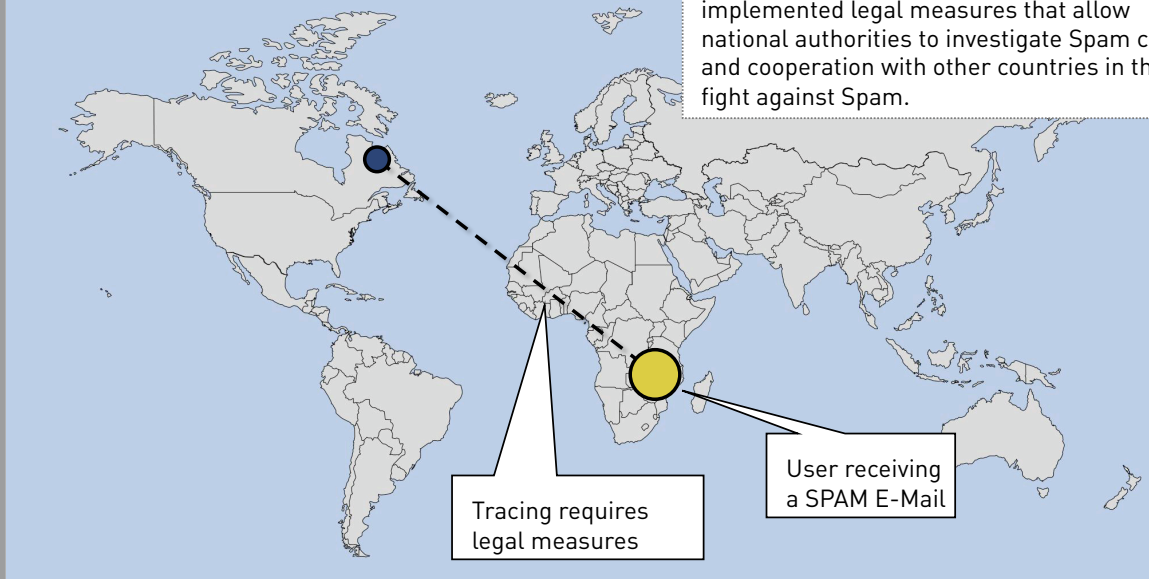
Everyday more than 100 Billion E-Mails are send. Based on current researches up to 85% of those e-mails are SPAM.



IMPORTANCE OF LEGAL M.

BACKGROUND LEGAL MEASURES

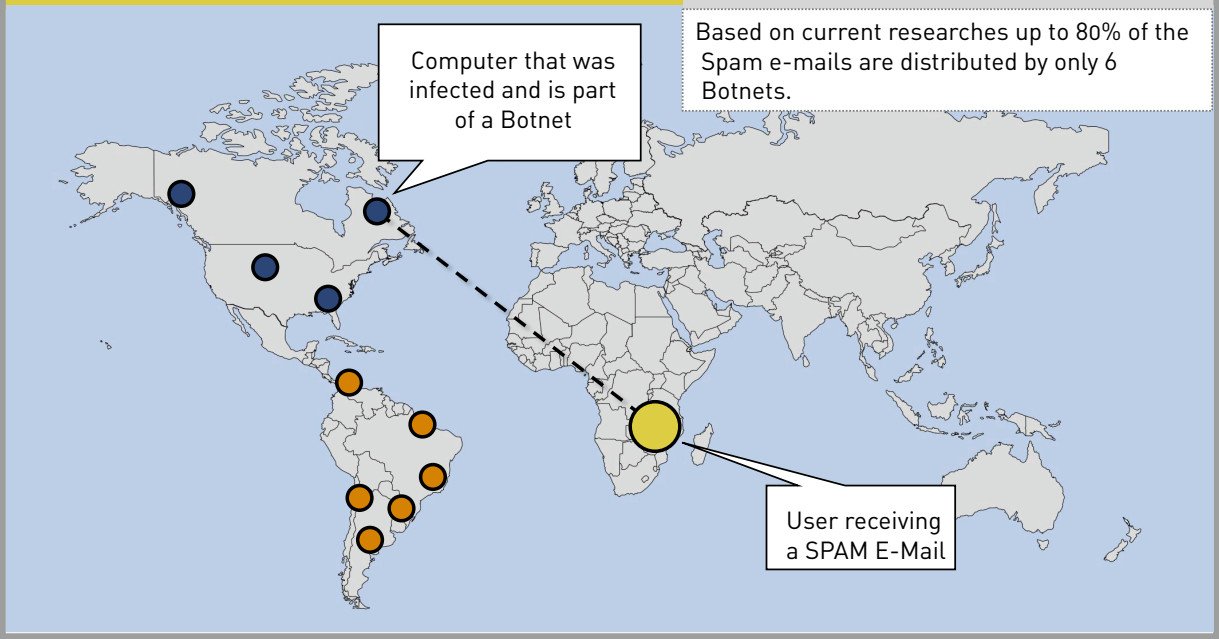
Not all countries in the world have yet implemented legal measures that allow national authorities to investigate Spam cases and cooperation with other countries in the fight against Spam.



IMPORTANCE OF LEGAL M.

BACKGROUND DISTRIBUTION OF SPAM

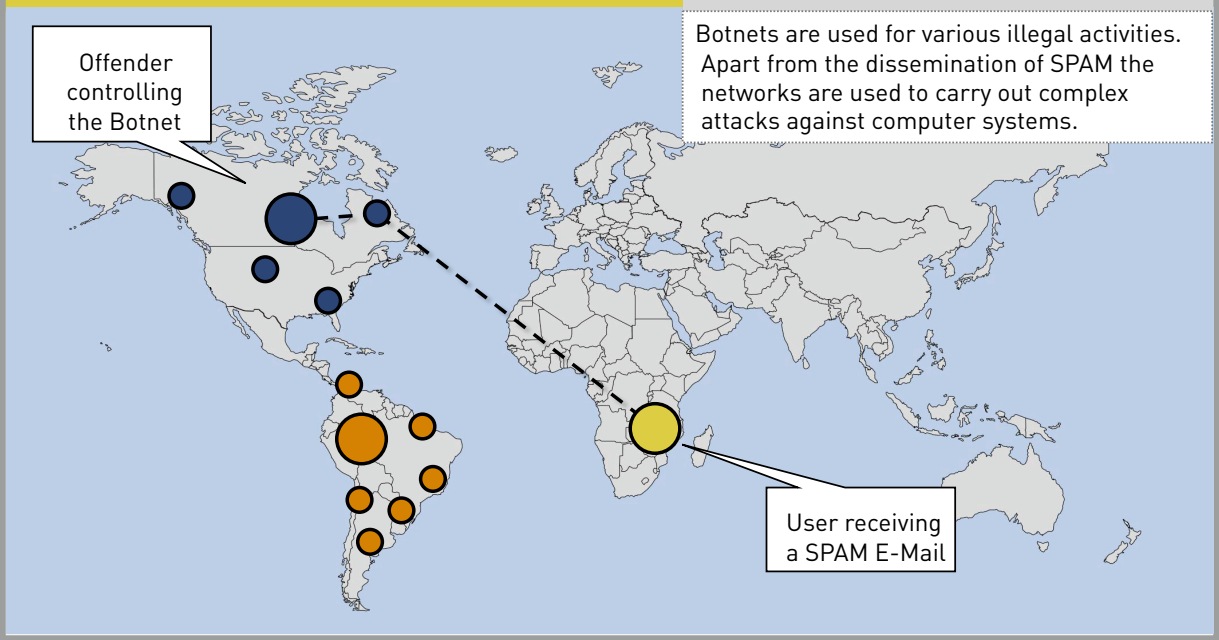
Based on current researches up to 80% of the Spam e-mails are distributed by only 6 Botnets.



IMPORTANCE OF LEGAL M.

BACKGROUND BOTNET

Botnets are used for various illegal activities. Apart from the dissemination of SPAM the networks are used to carry out complex attacks against computer systems.



CYBERCRIME GUIDE

ITU GUIDE

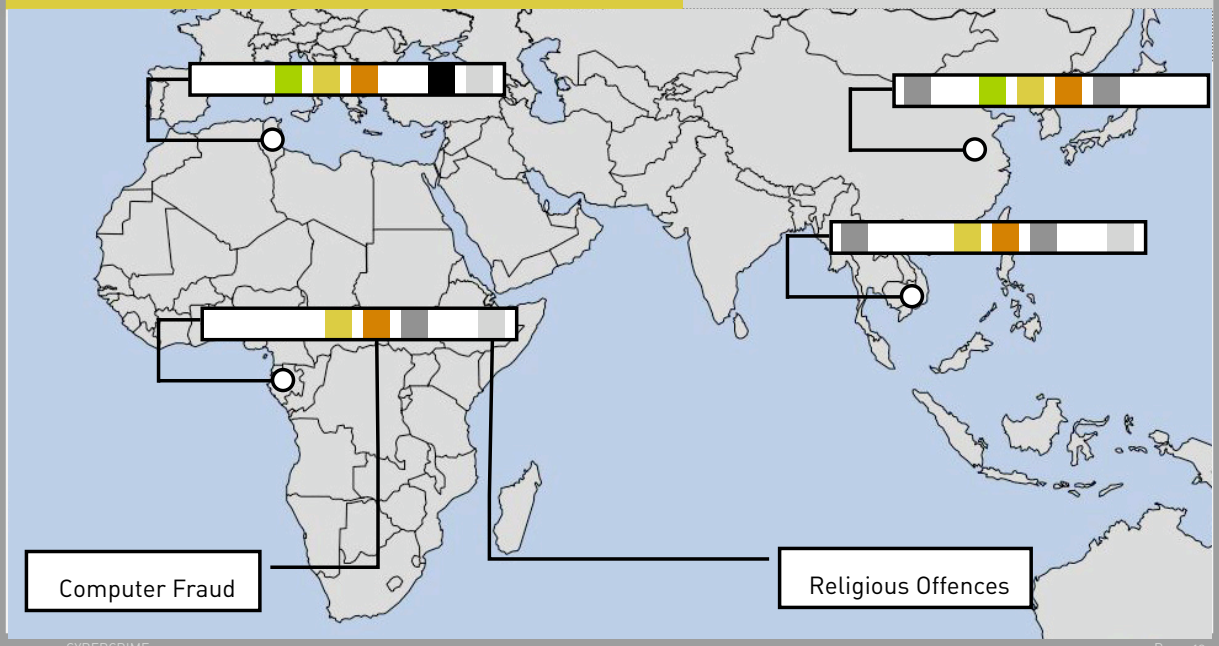
Picture removed in print version

- The guide will provide you with the information about legal instruments that are required for investigations as well as international cooperation
- It includes best practice examples
- Session 4 tomorrow morning will provide an overview

- National, Regional or International approaches?

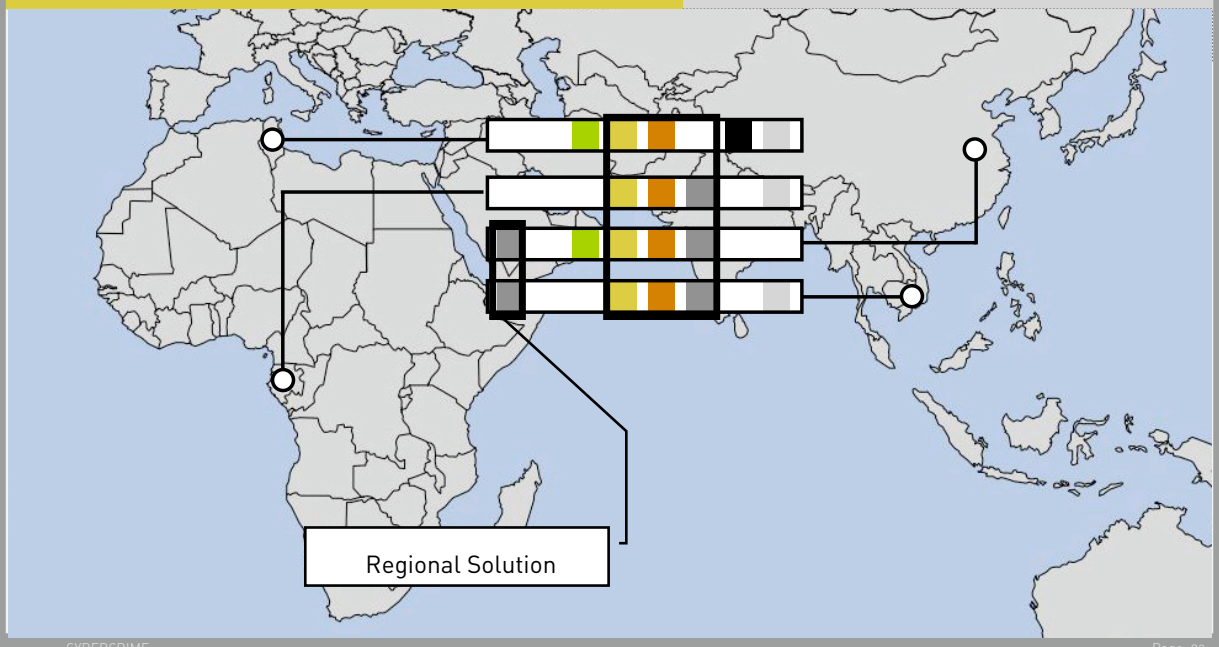
LEGAL SOLUTION

NATIONAL, REGIONAL, INTERNATIONAL



LEGAL SOLUTION

NATIONAL, REGIONAL, INTERNATIONAL



CONTACT

THANK YOU FOR YOUR ATTENTION

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

www.cybercrime.de