GERCKE

CYBERCRIME

NATIONAL, REGIONAL AND INTERNATIONAL SOULTIONS IN THE FIGHT AGAINST CYBERCRIME WITH A FOCUS ON THE BUDAPEST CONVENTION ON CYBERCRIME

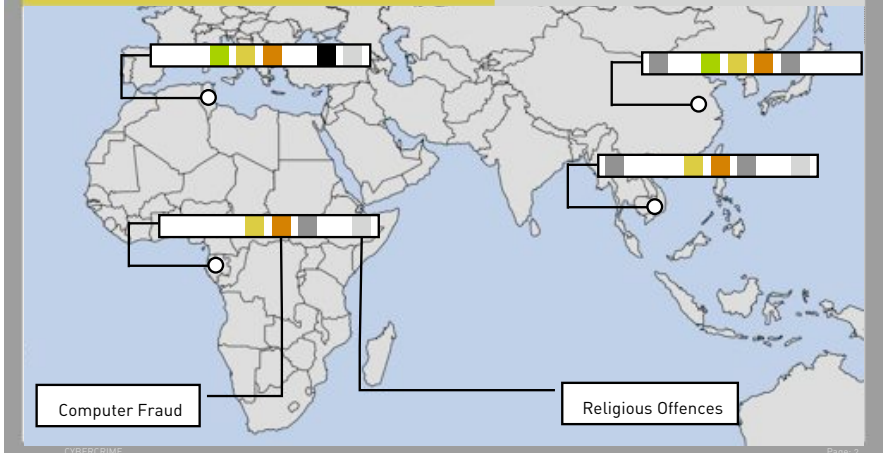
Regional Workshop on Frameworks for Cybersecurity and Critical Information Infrastructure Protection
Cap Verde
28. November 2008

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

GERCKE

LEGAL SOLUTION

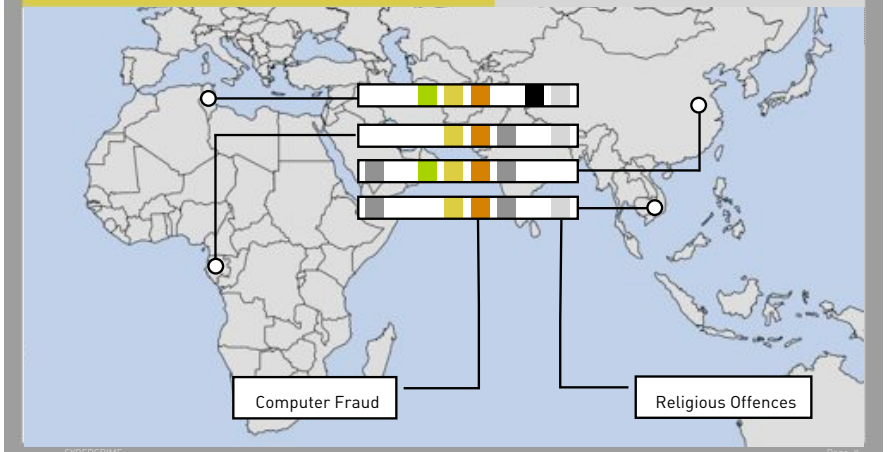
NATIONAL, REGIONAL, INTERNATIONAL



GERCKE

LEGAL SOLUTION

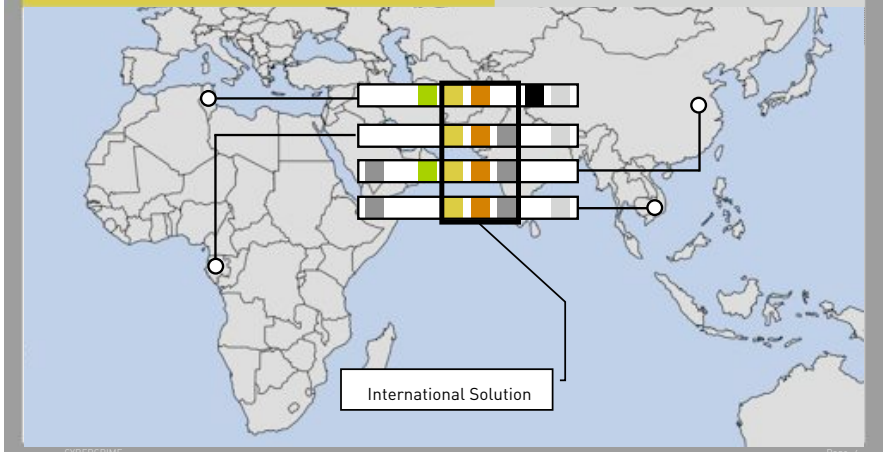
NATIONAL, REGIONAL, INTERNATIONAL



GERCKE

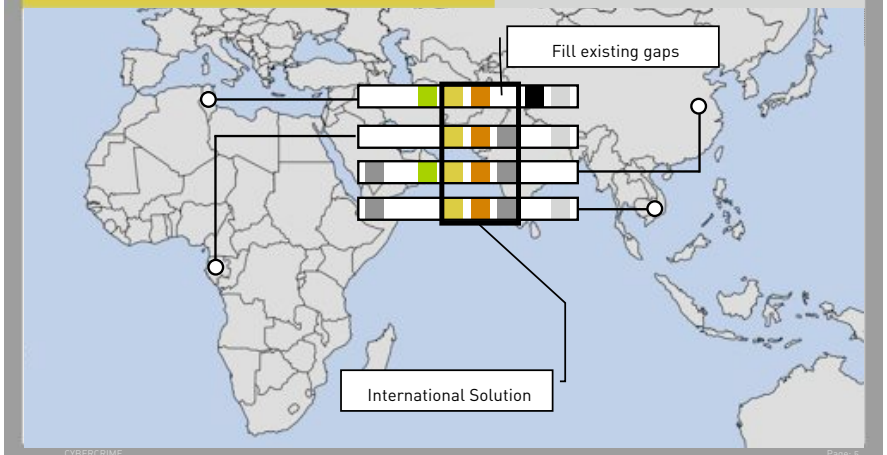
LEGAL SOLUTION

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

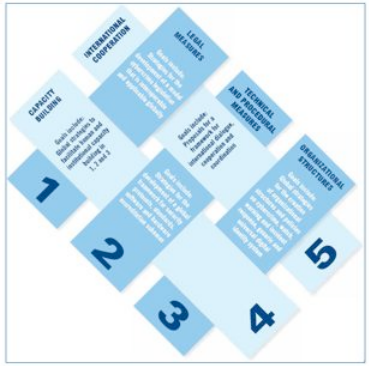
DETAILS ABOUT SIGNATURES

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

ITU HLEG

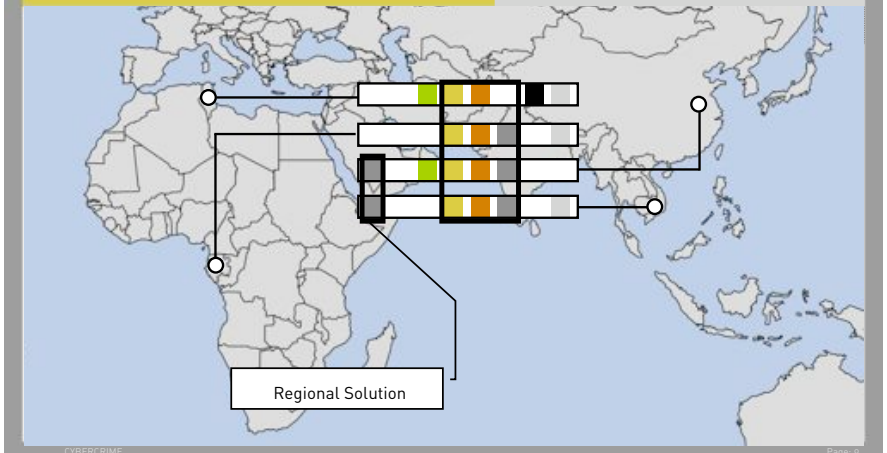
GLOBAL CYBERSECURITY AGENDA

- ITU set up a multi-stakeholder group of experts to further develop the the GCA
- Elaboration of strategies for the development of a model Cybercrime legislation that is globally applicable and interoperable with existing national and regional legislative measures



LEGAL SOLUTION

NATIONAL, REGIONAL, INTERNATIONAL



REGIONAL SOLUTION

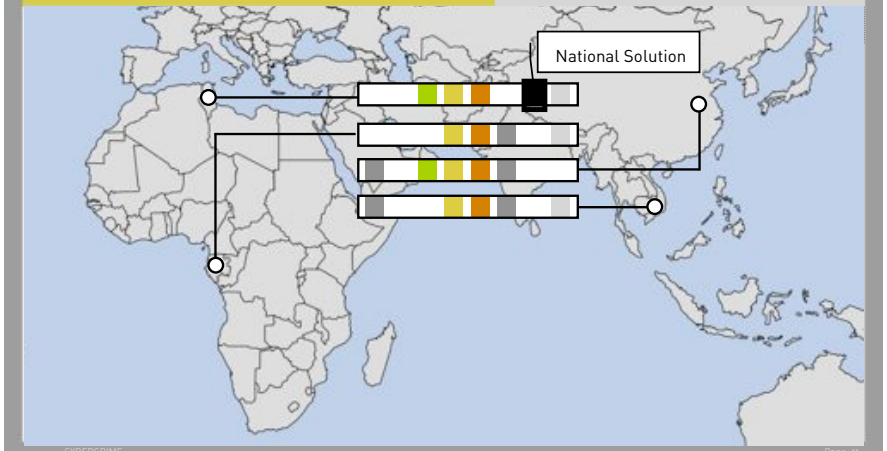
EU COUNTRIES

Picture removed in print version

- 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

BORDER

Picture removed in print version

- 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

CONVENTION ON CYBERCRIME

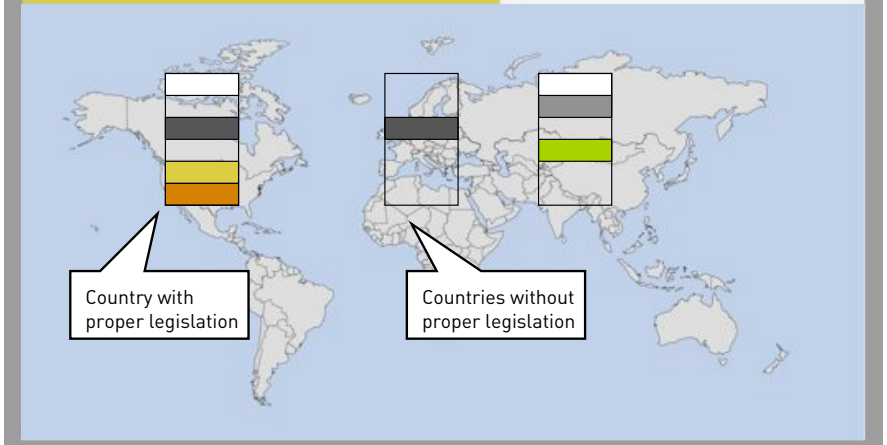
- The need for a harmonisation

NEED FOR HARMONISATION

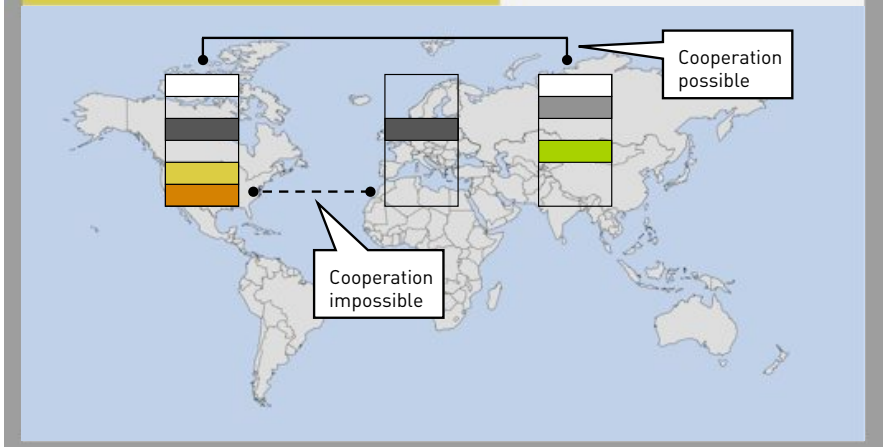
1. Technical aspect: Investigations depend on international cooperation of investigation authorities

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

CURRENT SITUATION



CURRENT SITUATION



REASON FOR THE DIFFICULTIES

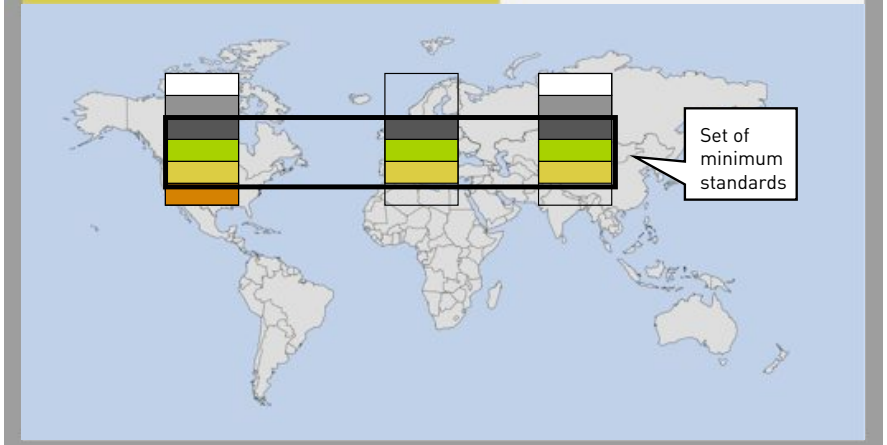
1. **Need of adequate provisions in the national law**
- **Substantive Criminal Law** and **Procedural Law** provisions are in most cases an essential requirement for national investigation (no crime - no investigation)
- **Substantive Criminal Law** and **Procedural Law** provisions are in most cases an essential requirement for international cooperation (dual criminality)

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

Notice

French and Arabic translation of the Convention and it's Explanation are available at

www.coe.int - Treaty Office - Convention 185

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.
[...]

NATURE (LEGAL)

- International Agreement
- Needs to be ratified an implemented to come into effect
- Binding only on a political level
- Various spaces for interpretation and restrictions

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

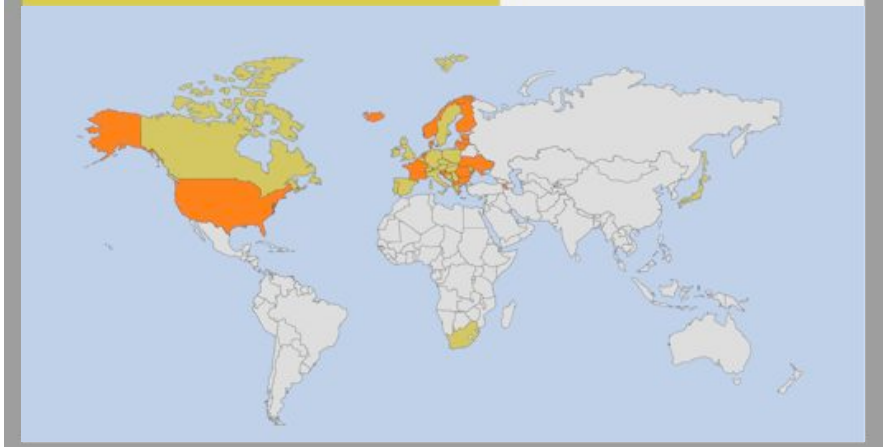
OPEN FOR NON-MEMBERS

- 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

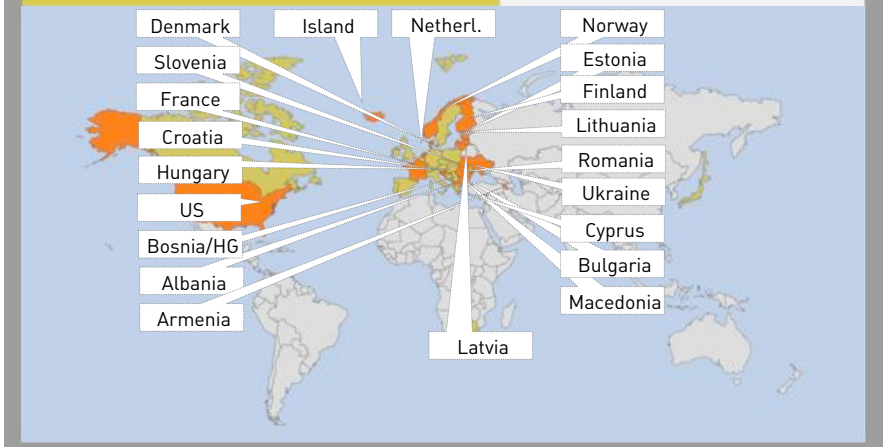
Art. 37 - Accession to the Convention

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



RATIFICATION



RATIFICATION

2002	2003	2004	2005	2006	2007
				Norway	
				Netherl.	
				Armenia	
		Macedonia		US	
		Slovenia	Cyprus	France	Finland
Croatia	Hungary	Romania	Denmark	Ukraine	Latvia
Albania	Estonia	Lithuania	Bulgaria	Bosnia/HG	Island

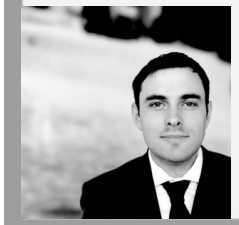
COUNCIL OF EUROPE

- Council of Europe is not on only providing the framework
- Assistance with regard to the evaluation of the status of the current legislation
- Training / Workshops
- Assistance within the implementation process

- Signatory states participate in the Cybercrime Committee that further develops the Convention

CONTACT

THANK YOU FOR YOUR ATTENTION



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

www.cybercrime.de