Cybercrime
Research Institute

CYBERCRIME

UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES

WSIS FORUM 2009

Geneva, 19th May 2009

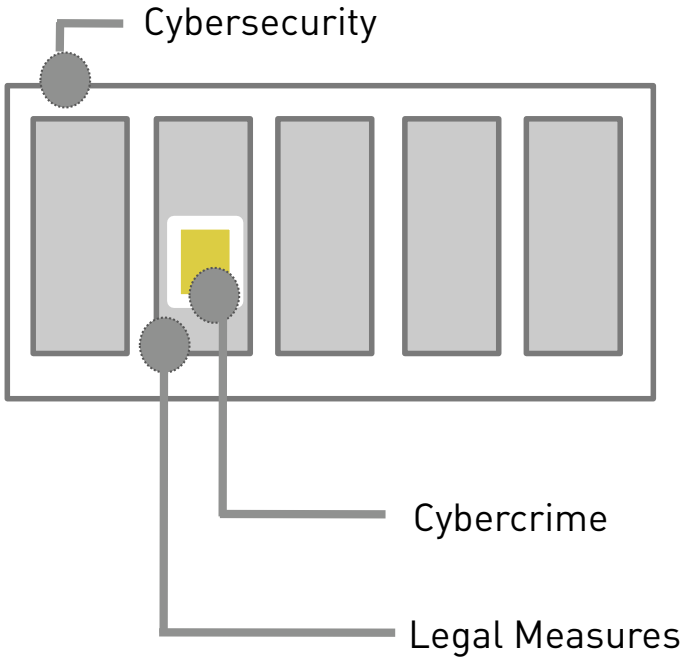
Dr. Marco Gercke

Lecturer for Criminal Law / Cybercrime, Faculty of Law,
Cologne University

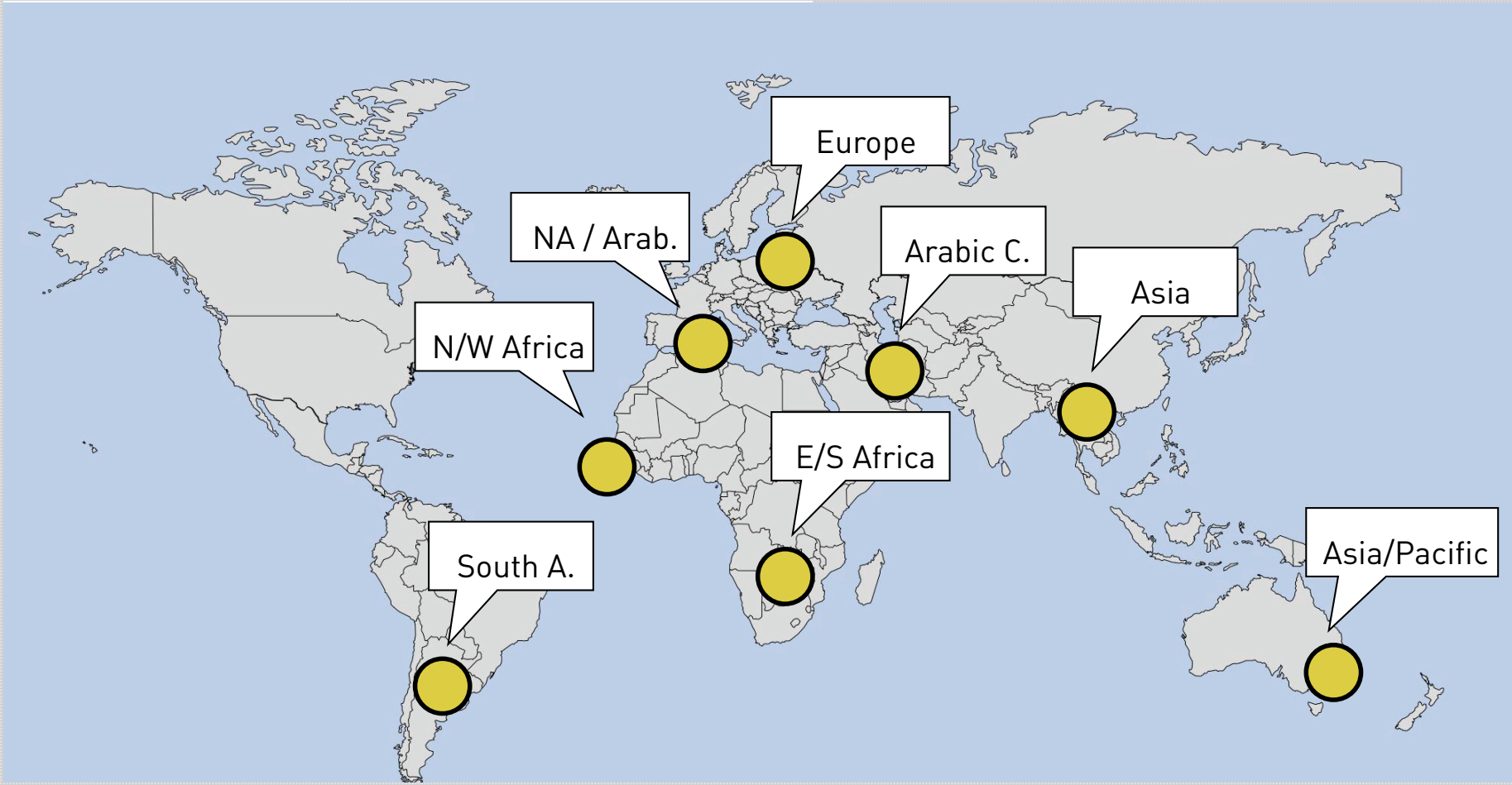
Cybercrime
Research Institute

LEGAL FOUNDATION

- 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



ITU-D REG. FORUM 2007-2009

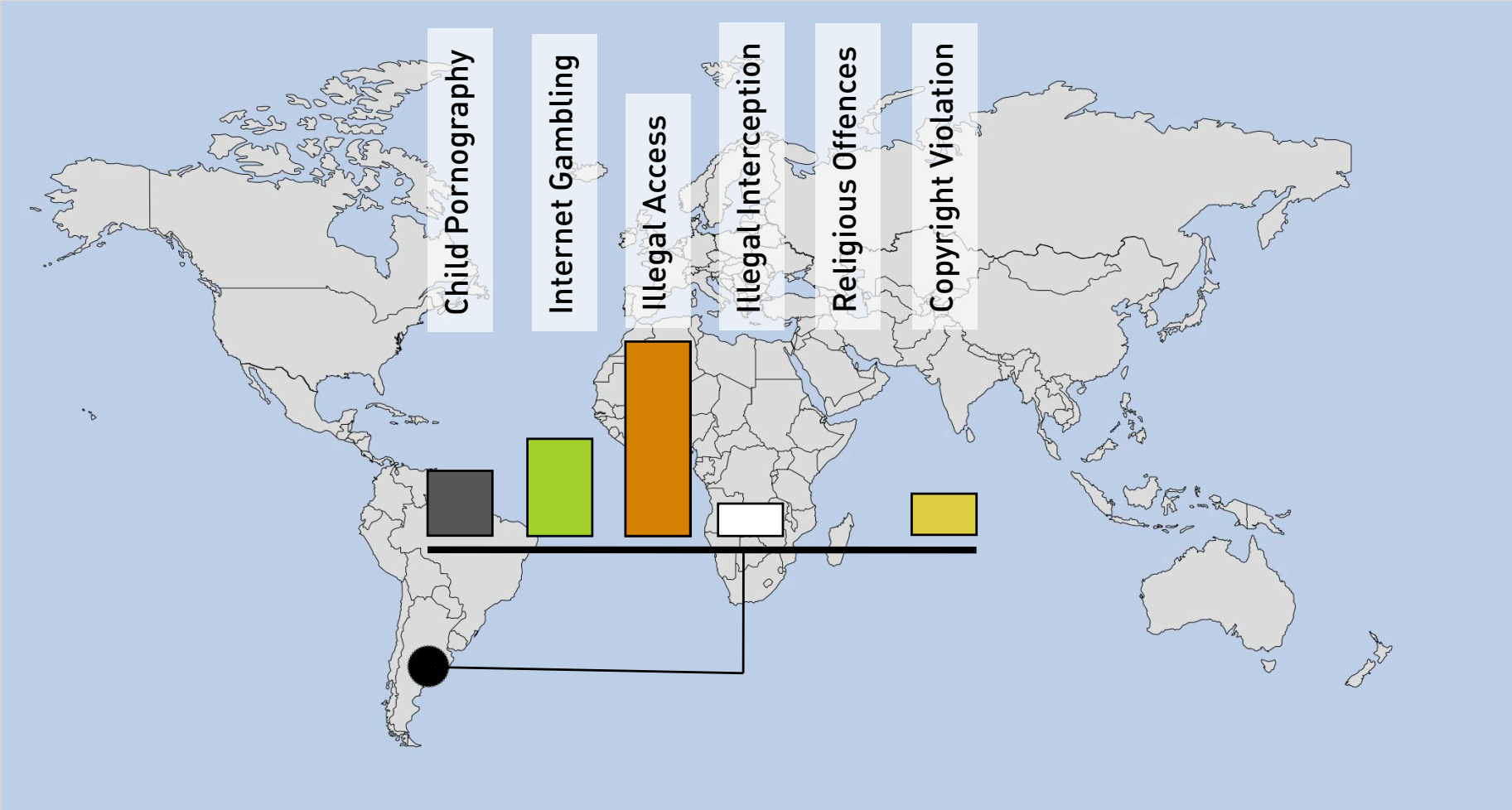


Cybercrime
Research Institute

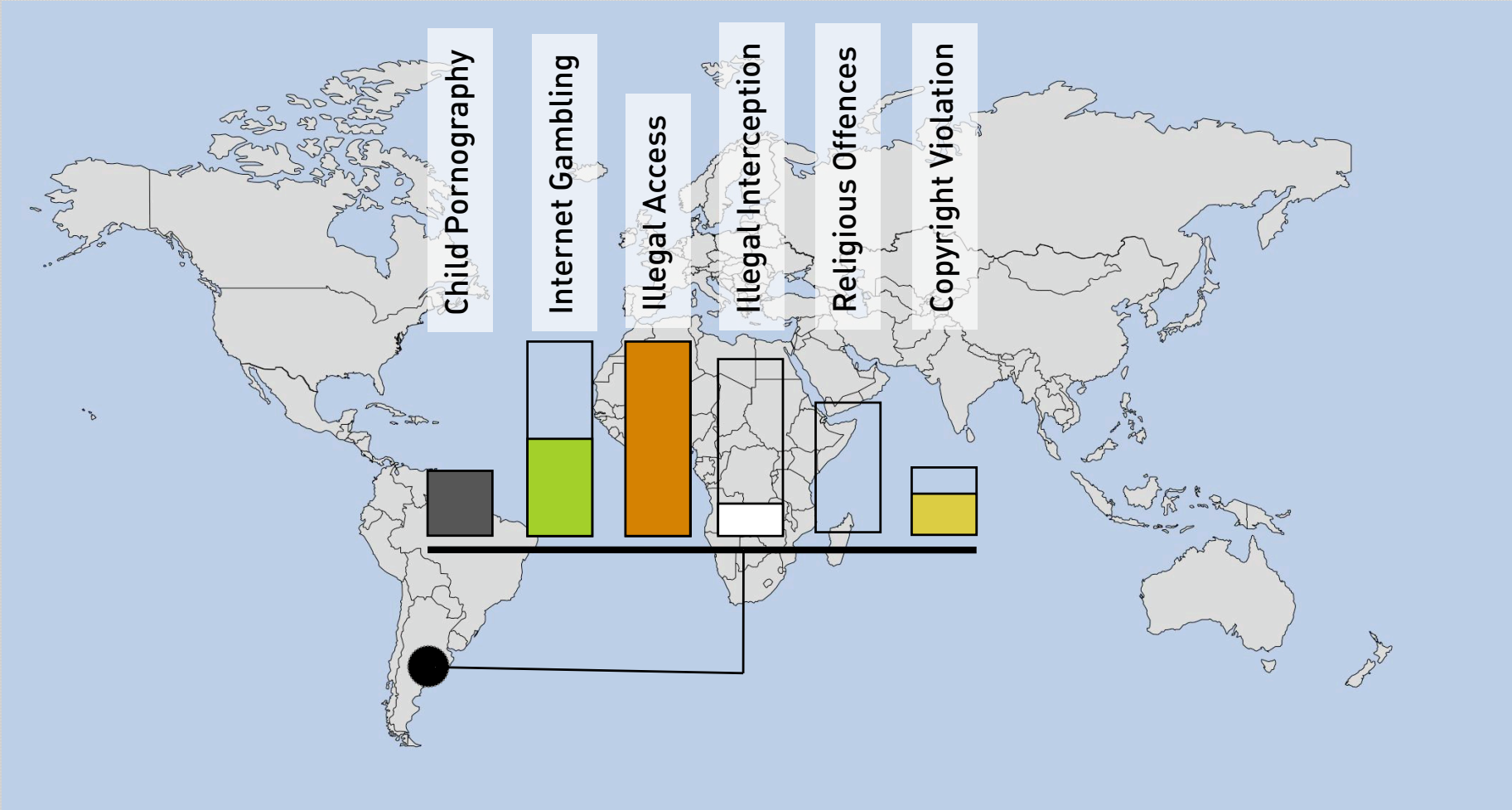
CYBERCRIME GUIDE

- Cybercrime is a global phenomenon
- The regional conferences proved a great interest in the topic
- Threat of developed countries as well as developing countries
- Aim: Providing a guide that is focussing on the demands of developing countries
- The guide does not provide an "out-of-the-box" solutions but aims to support the discussion in the countries

SITUATION

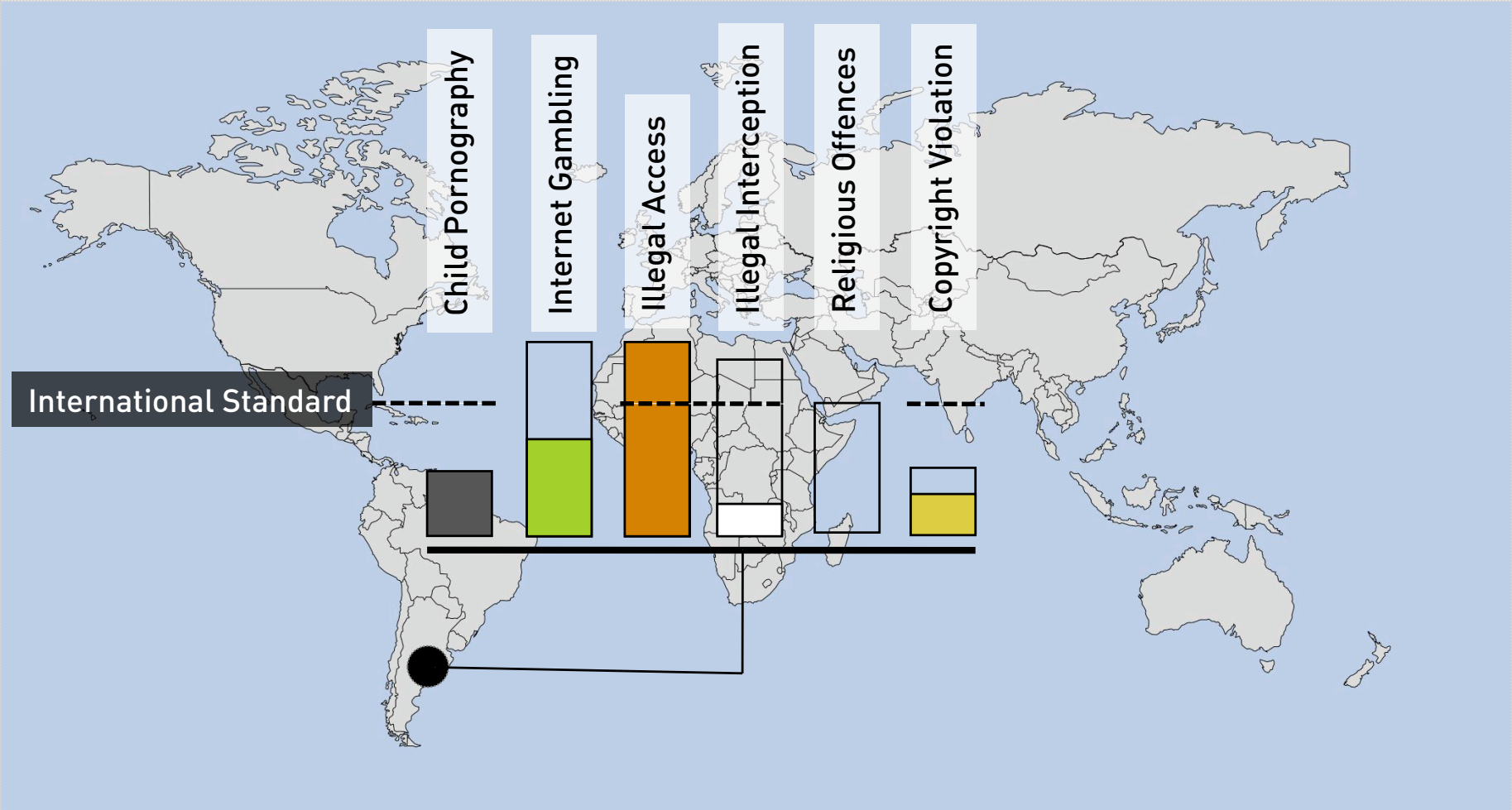

Child Pornography
Internet Gambling
Illegal Access
Illegal Interception
Religious Offences
Copyright Violation

DEMAND

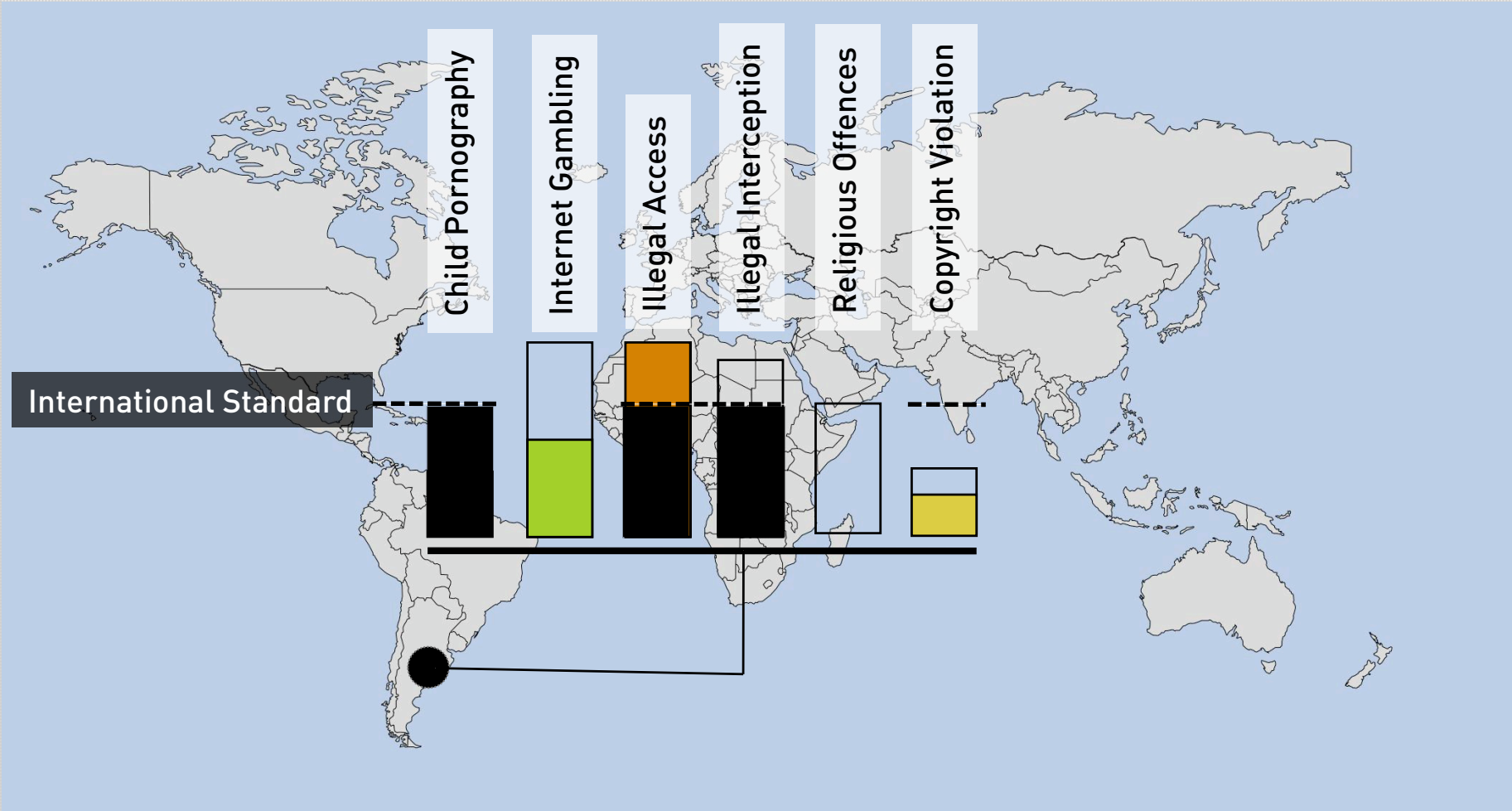

Child Pornography
Internet Gambling
Illegal Access
Illegal Interception
Religious Offences
Copyright Violation

Cybercrime
Research Institute

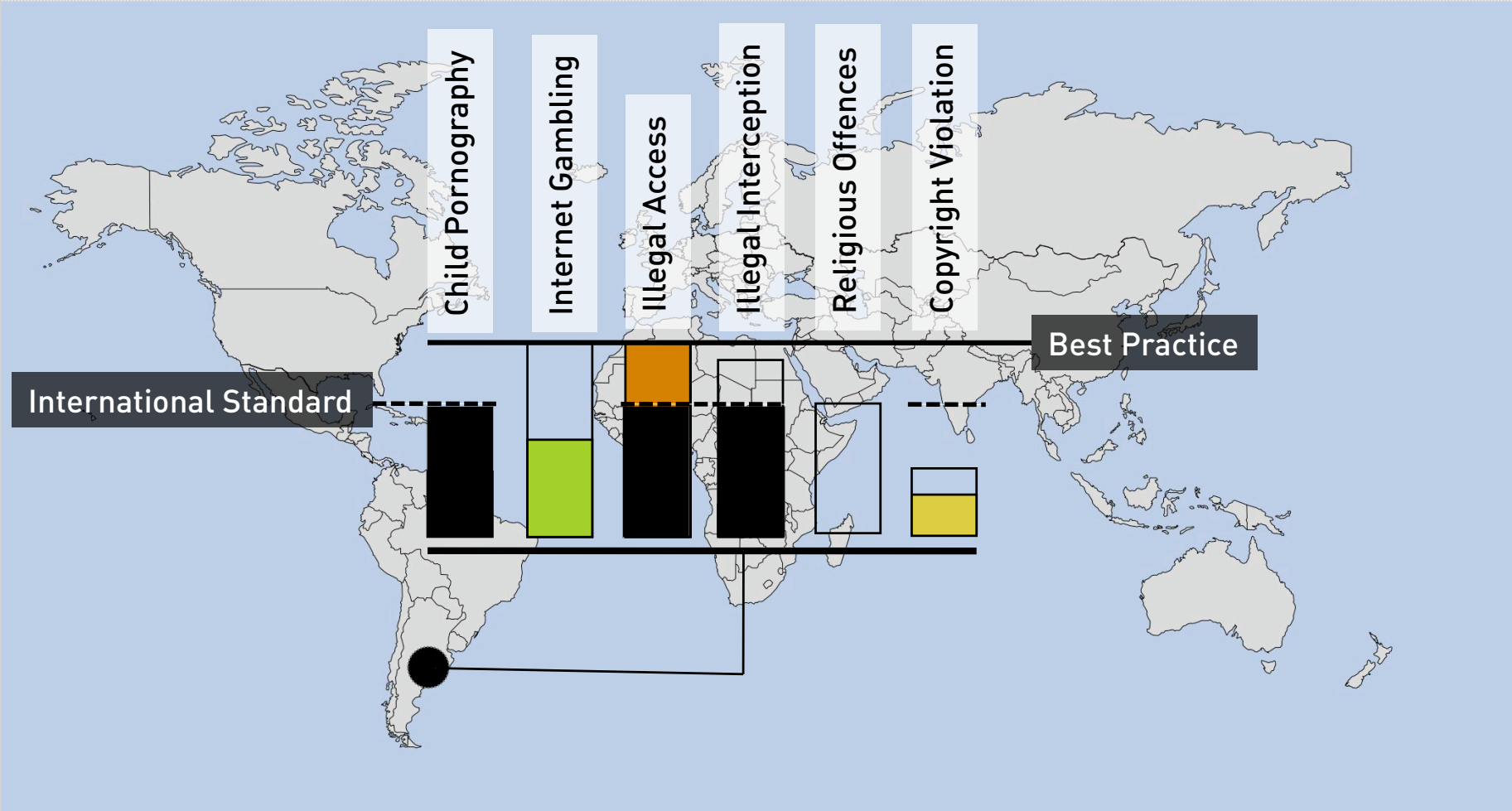
SEARCHING FOR STANDARDS



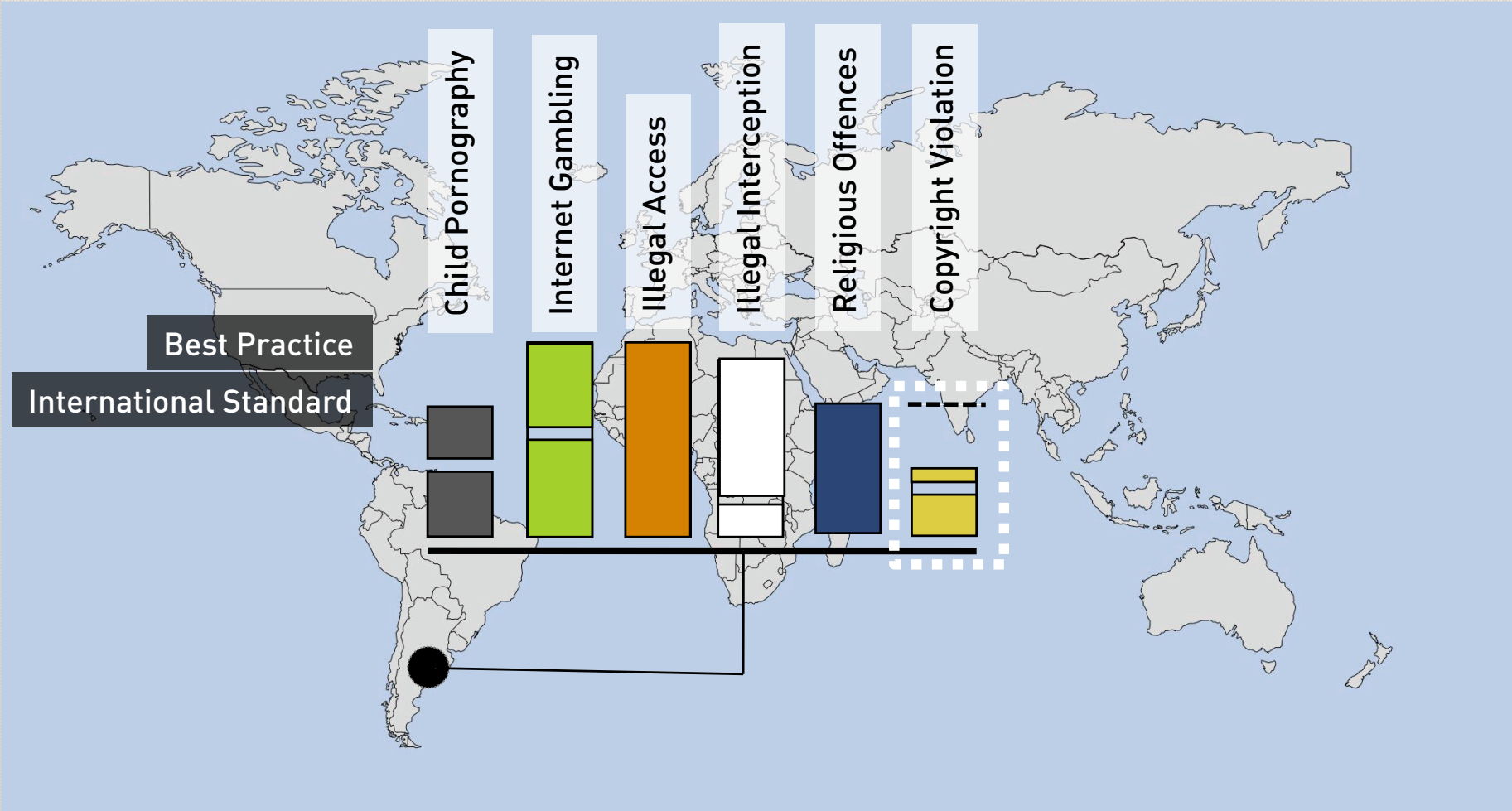
IMPLEMENTING STANDARDS



BEST PRACTICE



INDIVIDUAL APPROACH



Cybercrime
Research Institute

CYBERCRIME GUIDE

- During the the WSIS Forum 2009, HL Panel No. 1 (Accessing Knowledge) the importance of a free access to knowledge was emphasised
- ITU will make the guide available free of charge
- Available on the ITU website now

Cybercrime
Research Institute

CYBERCRIME 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 file sharing systems 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/27/59/37487604.pdf.

[229] See *Hartstack*, 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*, Council of Europe Organised Crime Report 2004, page 148.

[232] Digital Rights Management describ[illegible]ontrol technology used to limit the usage of digital media. For further information see: *Cunard/Hill/Barlas*, Current develop[illegible]ield of digital rights management – available at: [illegible]xcerpt/pdf/wcer_10_2.pdf; *Lohmann*, Digital Rights Management: The Skeptics' View – available at: http://www.eff.org/IP/D[illegible]1_drm_skeptics_view.pdf.

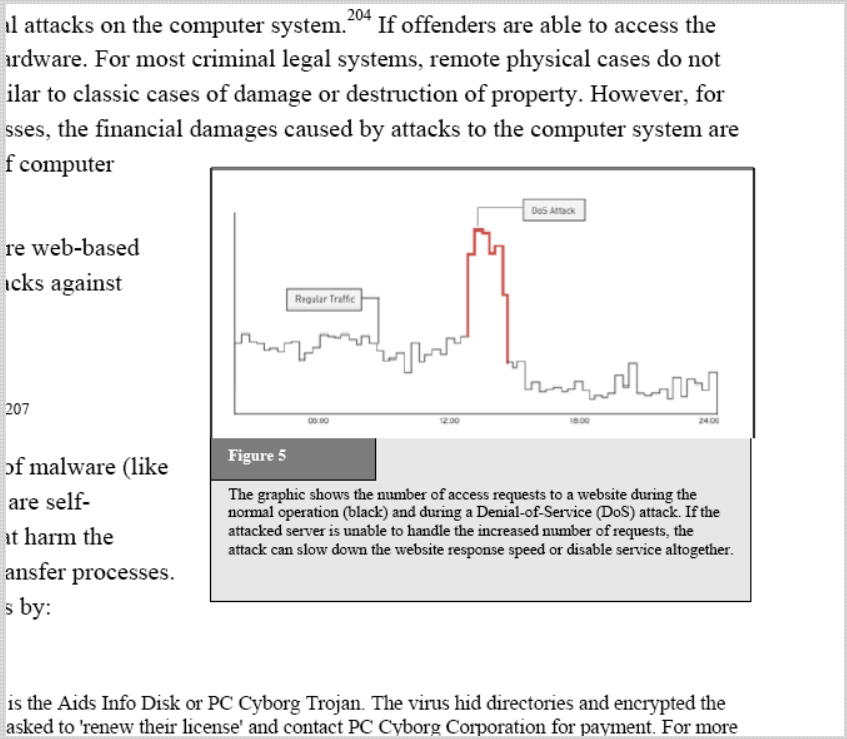
[233] Peer-to-Peer describes direct connectivity between participants in networks instead of communicating via conventional centralized server-based structures. See: *Schoder/Fischbach/Schmitt*, Core Concepts in Peer-to-Peer Networking, 2005 – available at: http://www.idea-group.com/downloads/excerpts/Subramanian01.pdf; *Androutsellis-Theotokis/Spinellis*, A Survey of Peer-to-Peer Content Distribution Technologies, 2004 – available at: http://www.spinellis.gr/pubs/jrnl/2004-ACMCS-p2p/html/AS04.pdf.

[234] GAO, File Sharing, Selected Universities Report Taking Action to Reduce Copyright Infringement – available at: http://www.gao.gov/new.items/d04503.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/p2p05/050623p2prpt.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
Research Institute

PHENOMENA

- Explaining more than 20 different kind of offence linked to the term “Cybercrime”
- Ranging from traditional offences like illegal access or computer-related fraud to complex scams like “phishing” and “cyberlaundering”
- Even topics that go beyond international standards like religious offences or illegal gambling are covered



ıl attacks on the computer system.[204] If offenders are able to access the ırdware. For most criminal legal systems, remote physical cases do not ilar to classic cases of damage or destruction of property. However, for sses, the financial damages caused by attacks to the computer system are f computer

re web-based ıcks against

207

of malware (like are self- ıt harm the ansfer processes. s by:

Figure 5

The graphic shows the number of access requests to a website during the normal operation (black) and during a Denial-of-Service (DoS) attack. If the attacked server is unable to handle the increased number of requests, the attack can slow down the website response speed or disable service altogether.

is the Aids Info Disk or PC Cyborg Trojan. The virus hid directories and encrypted the asked to 'renew their license' and contact PC Cyborg Corporation for payment. For more

Cybercrime
Research Institute

CHALLENGE

- Providing a detailed analysis of the most important challenges related to the fight against Cybercrime
- This includes very recent issues like the emerging use of encryption technology, the use of botnets to commit large scale attacks and the ability to the hide the identity by using anonymous communication services

net user can get access to those instructions.

ines to analyse targets.[598] A training manual was found during investigations up highlighting how useful the Internet is for gathering information on ngines, offenders rmation (e.g., ildings) that help in orted that insurgents istan used satellite

ms of Control

s - from phone ls to the Internet - chnical standards to iscussions about he Internet is no and even astructure.[601] The l by laws and law-makers and law enforcement agencies have started to ing a certain degree of central control.

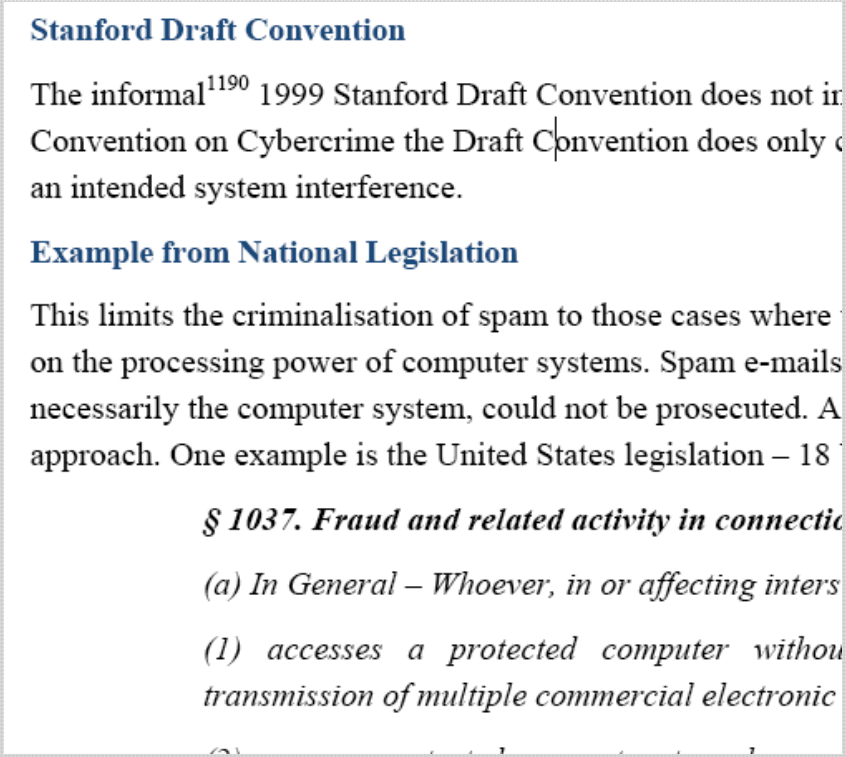
Figure 28

The graphic shows the possibility of circumventing central control mechanisms installed by access providers. If access providers install certain filter technology, user requests will be blocked. This control approach can be circumvented, if the user makes use of anonymous communication servers that encrypt requests. For example in this case, access providers have no access to requests sent to the anonymous communication server and cannot block the websites.

Cybercrime
Research Institute

LEGAL SOLUTIONS

- Guide does not provide an "out-of-the-box" solution
- With regard to nearly 20 offences the guide provides an **overview** and **analysis** about examples for criminal law provisions addressing the phenomenon of Cybercrime
- This includes the outcome of ITU HLEG, Commonwealth Model Law, Budapest Convention on Cybercrime, Stanford Draft Convention and in some cases national approaches



Stanford Draft Convention

The informal[1190] 1999 Stanford Draft Convention does not in
Convention on Cybercrime the Draft Convention does only
an intended system interference.

Example from National Legislation

This limits the criminalisation of spam to those cases where
on the processing power of computer systems. Spam e-mails
necessarily the computer system, could not be prosecuted. A
approach. One example is the United States legislation – 18

§ 1037. Fraud and related activity in connectio

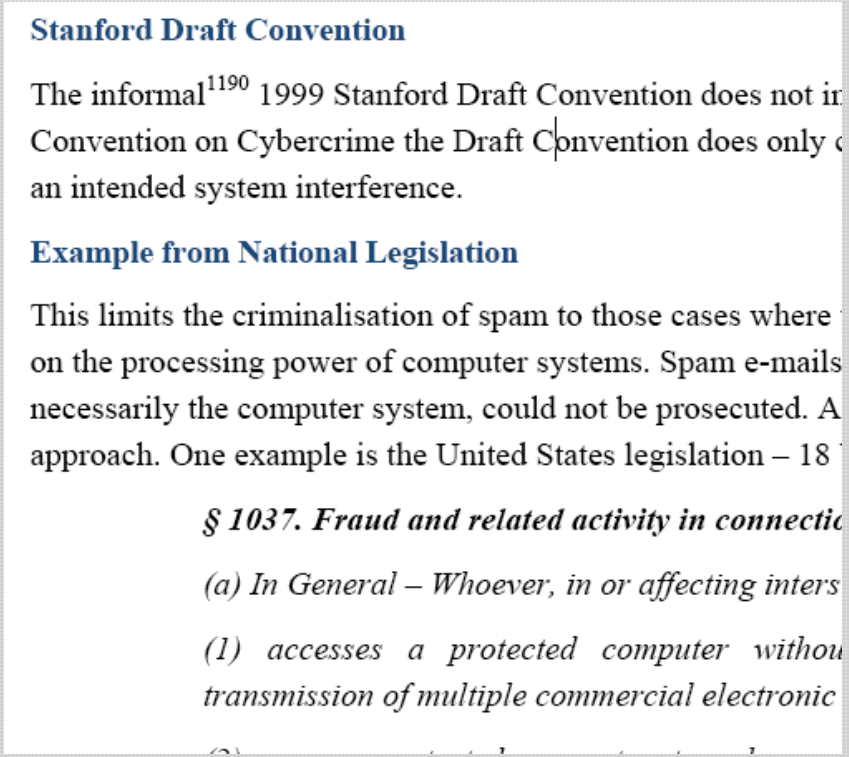
(a) In General – Whoever, in or affecting inters

(1) accesses a protected computer withou
transmission of multiple commercial electronic

Cybercrime
Research Institute

LEGAL SOLUTIONS

- Examples for legal solutions are not limited to substantive criminal law but as well cover procedural law, international cooperation and the liability of Internet Service Providers for offences committed by user of their service



Stanford Draft Convention

The informal[1190] 1999 Stanford Draft Convention does not in
Convention on Cybercrime the Draft Convention does only
an intended system interference.

Example from National Legislation

This limits the criminalisation of spam to those cases where
on the processing power of computer systems. Spam e-mails
necessarily the computer system, could not be prosecuted. A
approach. One example is the United States legislation – 18

§ 1037. Fraud and related activity in connectio

(a) In General – Whoever, in or affecting inters

(1) accesses a protected computer withou
transmission of multiple commercial electronic

Cybercrime
Research Institute

ITU WEBSITE

http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html