

CYBERCRIME

UNDERSTANDING CYBERCRIME: A GUIDE FOR DEVELOPING COUNTRIES

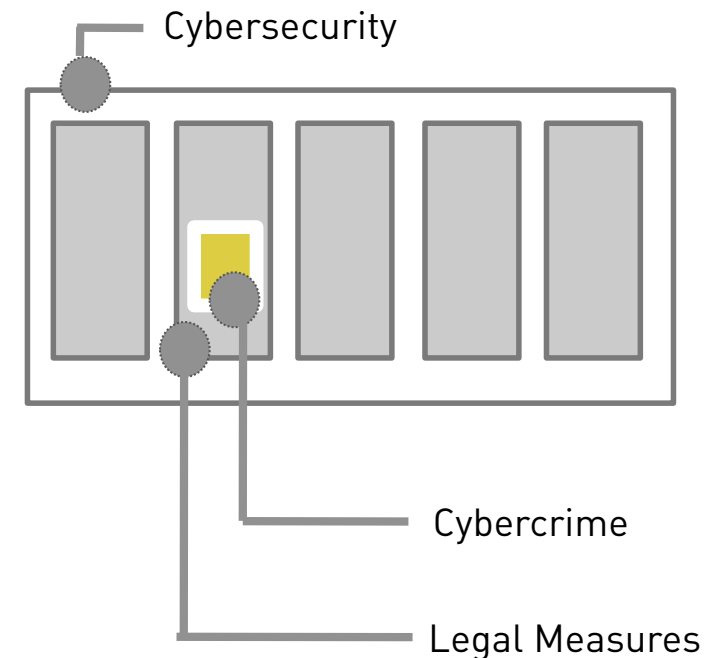
ITU CYBER SECURITY FORUM
Tunis, 05th June 2009

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

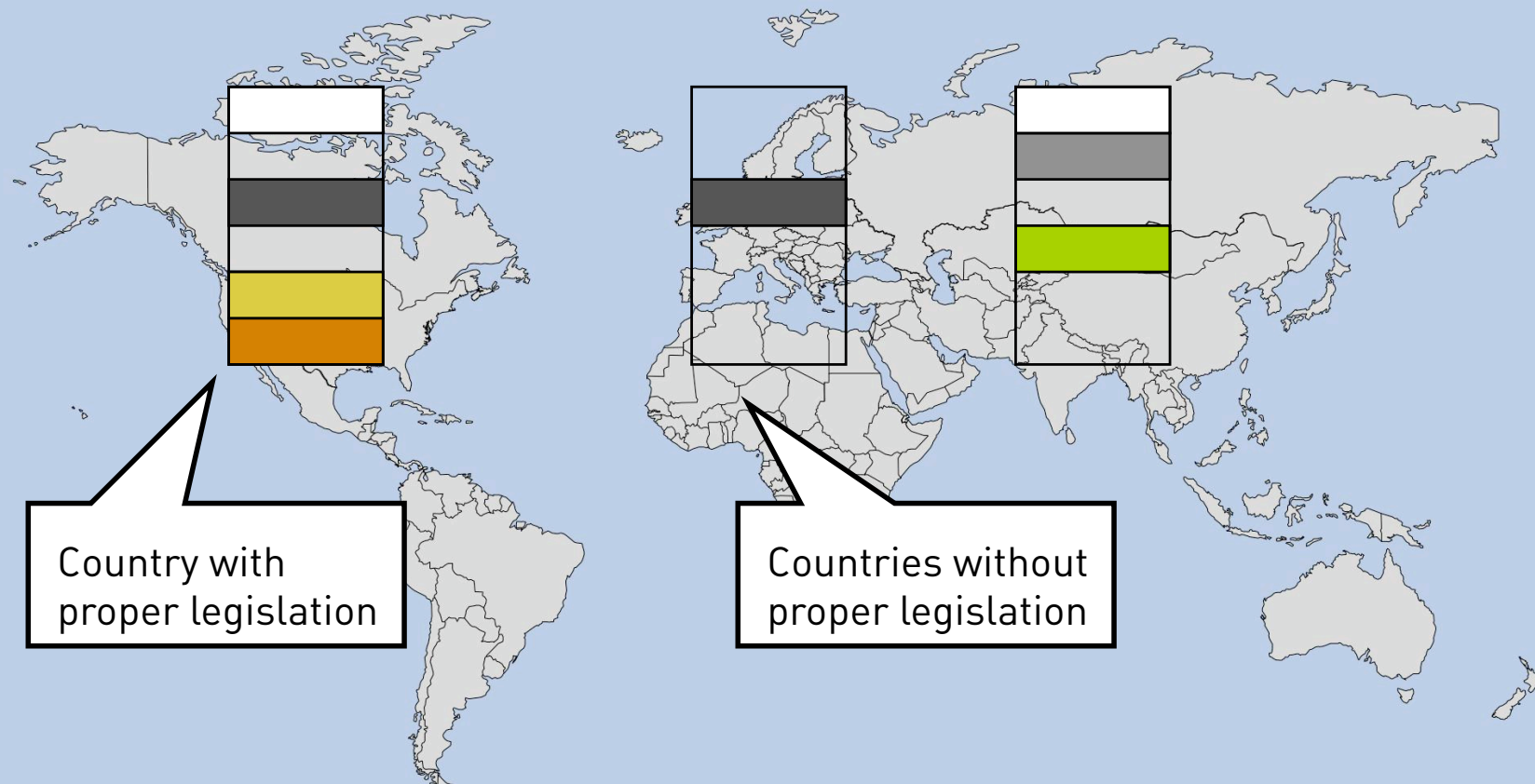
LEGAL FOUNDATION

- 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

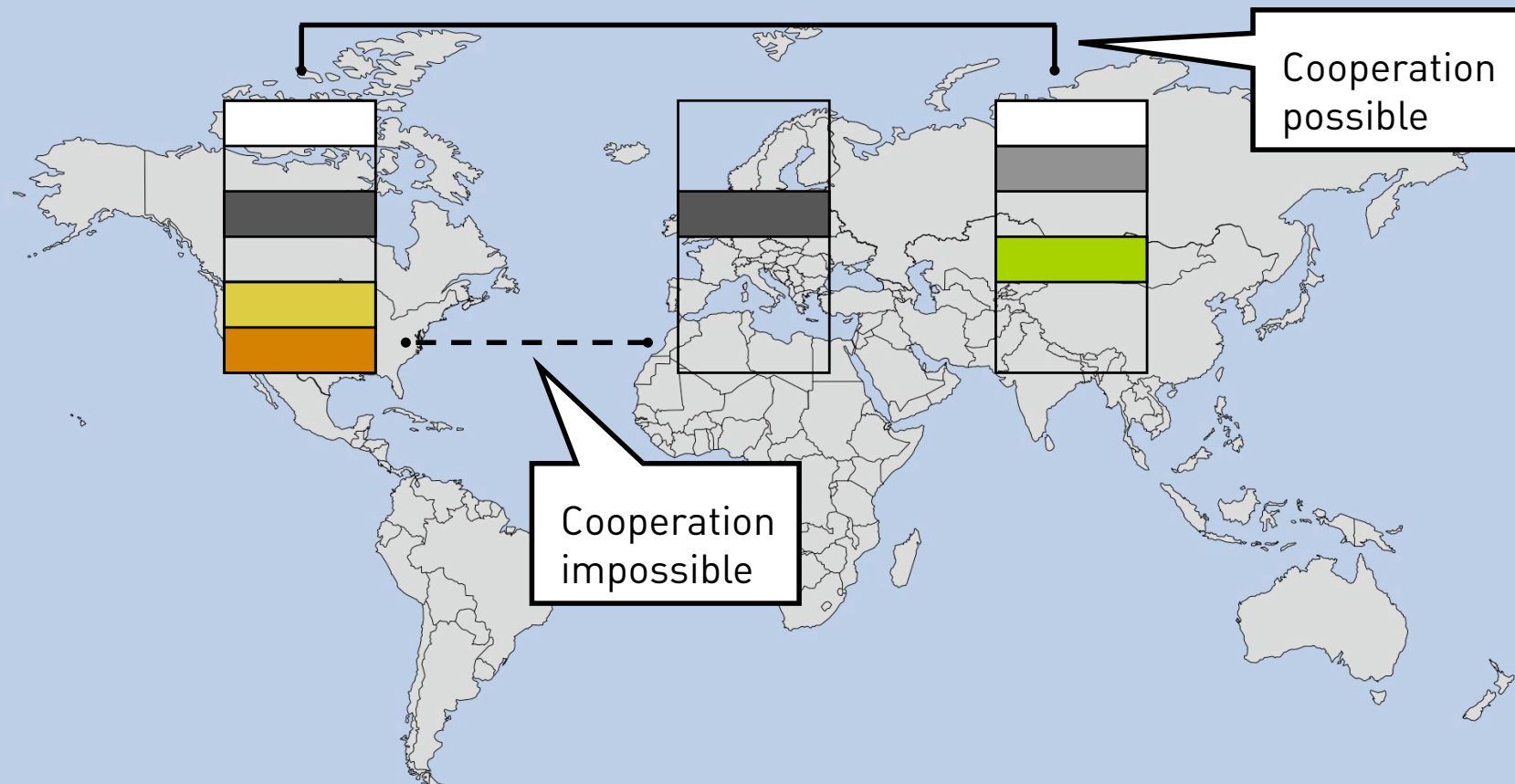
CYBERSECURITY / CYBERCRIME



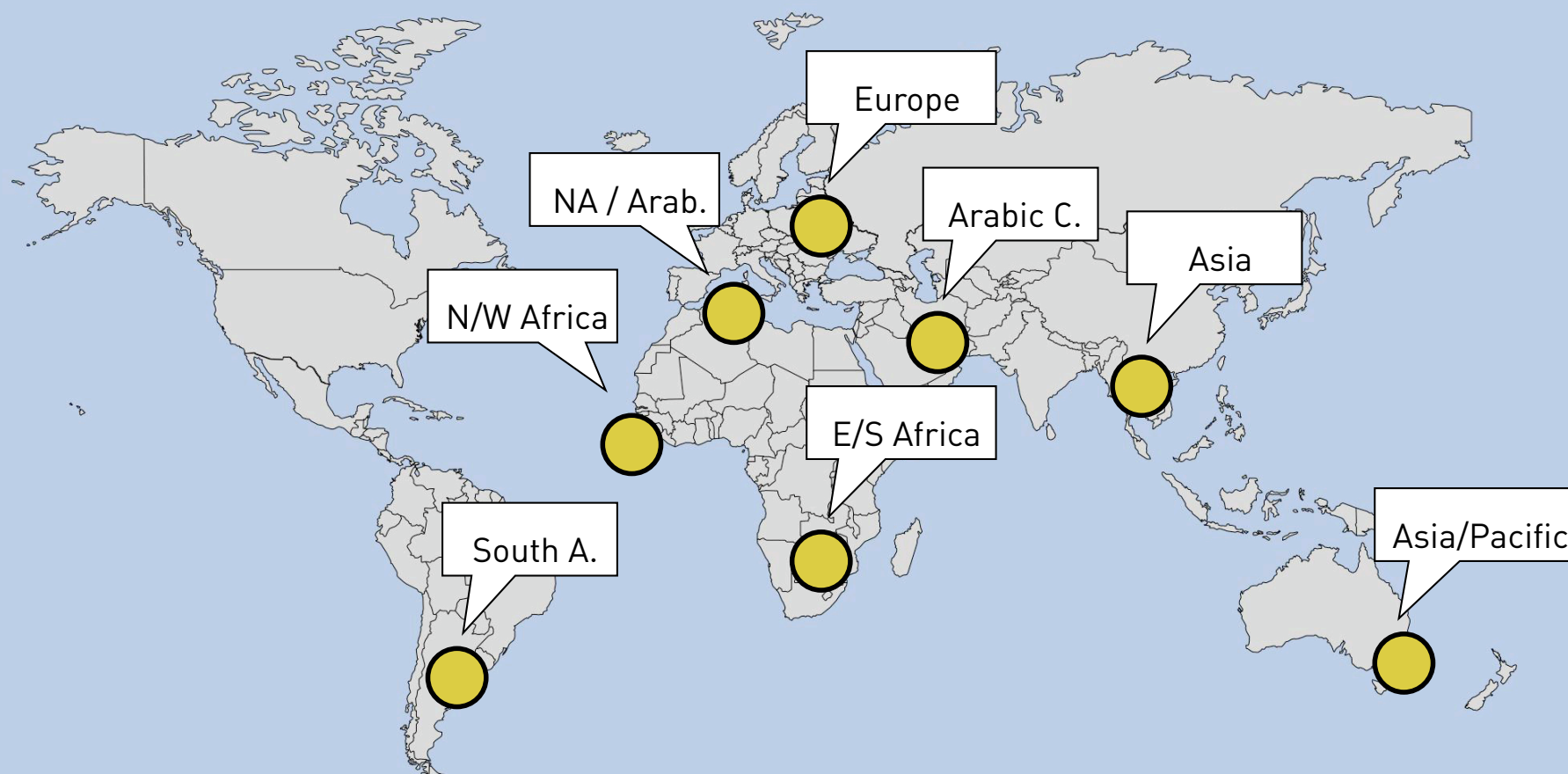
CURRENT SITUATION



CURRENT SITUATION



ITU-D REG. FORUM 2007-2009



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

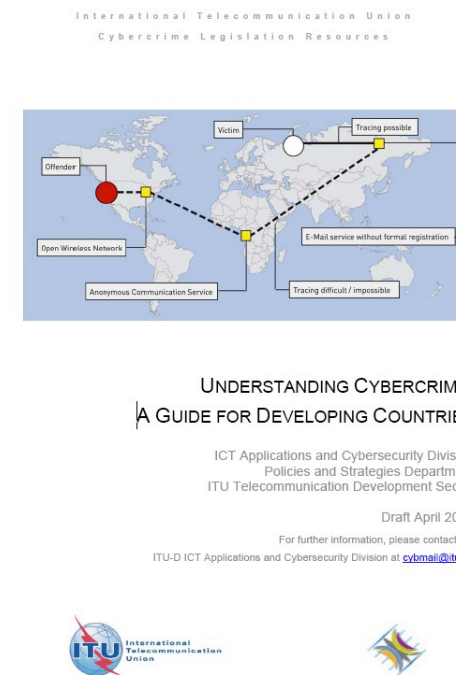
ITU GUIDE



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
- Very positive feedback during the last 2 weeks

ITU GUIDE



CYBERCRIME GUIDE

- ITU is currently working on the translation of the guide to all UN language
- Arabic, Chinese, Russian, French and Spanish version will very likely be available in September

ITU GUIDE



CYBERCRIME GUIDE

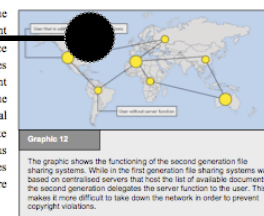
ITU GUIDE

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.²³⁰ Before the transition took place the development of products and services reached a point where very little improvement was possible. The digitalisation²³¹ 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.²³²



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 systems²³³
- The circumvention of digital-rights management systems²³²

File-sharing systems are peer-to-peer²³³ based network services that enable their users to share files with other users.²³⁴ After installing the file-sharing software 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

²³⁰ 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>.

²³¹ See Hornsack, Die Musikindustrie unter Einfluss der Digitalisierung, Page 34 et seqq.

²³² Apart from these 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.

²³³ Safer, Copyright and the Organised Crime Report 2004, page 148.

²³⁴ Digital Rights Management describes access control technology used to limit the usage of digital media. For further information see: Copyright Watch, Recent developments in the field of digital rights management – available at: http://www.wipo.int/documents/en/meetings/2003/scr/pdf/scr_10_2.pdf, Lehmann, Digital Rights Management: The Skeptics' View – available at: http://www.eff.org/IP/DRM/20030401_drm_skeptics_view.pdf.

²³⁵ Peer-to-Peer describes direct connectivity between participants in networks instead of communicating via conventional centralized server-based structures. See: Schindler/Fischback/Schwin, Core Concepts in Peer-to-Peer Networking, 2005 – available at: <http://www.idea-group.com/downloads/abstracts/Subramanian01.pdf>, Andreatelli/Theotakis/Spoinellis, A Survey of Peer-to-Peer Content Distribution Technologies, 2004 – available at: <http://www.spinellis.gr/pubs/jml/2004-ACMCS-p2p/html/AS04.pdf>.

²³⁶ GAO, File Sharing, Selected Universities Report Taking Action to Reduce Copyright Infringement – available at: <http://www.gao.gov/new.items/d04503.pdf>, Ripeanu/Foster/Iamnitschi, 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-04-mateiPAPERS-ic.pdf](http://people.cs.uchicago.edu/~matei/PAPERS/ic-04-mateiPAPERS-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/p2p/p2p040223/p2p.pdf>, Service/Guennadi/Griffith, A Measurement Study of Peer-to-Peer File Sharing Systems – available at: <http://www.cs.washington.edu/homes/griffith/papers/tmcs.pdf>.

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

ITU GUIDE

al attacks on the computer system.²⁰⁴ If offenders are able to access the hardware. For most criminal legal systems, remote physical cases do not differ from classic cases of damage or destruction of property. However, for cybercrimes, the financial damages caused by attacks to the computer system are often much higher than for physical attacks.

are web-based attacks against

207

of malware (like ransomware) are self-propagating and can harm the transfer processes. They can be spread by:

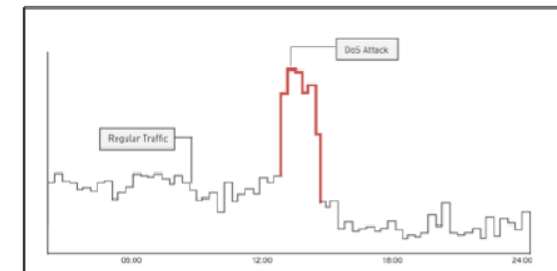


Figure 5

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 files. It asked to 'renew their license' and contact PC Cyborg Corporation for payment. For more

PHENOMENA

- During the discussion yesterday the “Advance Fee Fraud” was mentioned
- Guide contains detailed description of the phenomenon as well as the legal response
- Further solutions provided by the ITU Cybercrime Legislation Toolkit

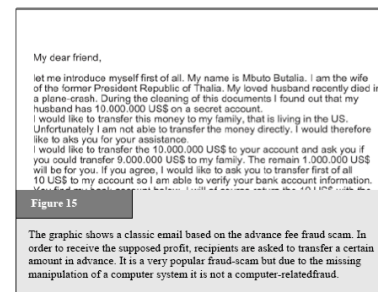
ITU GUIDE

2.7.1. Fraud and Computer-related Fraud

Computer-related fraud is one of the most popular crimes on the Internet,³⁷¹ as it enables the offender to use automation³⁷² and software tools to mask criminals’ identities.

Automation enables offenders to make large profits from a number of small acts.³⁷³ One strategy used by offenders is to ensure that each victim’s financial loss is below a certain limit. With a ‘small’ loss, victims are less likely to invest time and energy in reporting and investigating such crimes.³⁷⁴ One example of such a scam is the Nigeria Advanced Fee Fraud (see Figure 15).³⁷⁵

Although these offences are carried out using computer technology, most criminal law systems categorise them not as computer-related offences, but as regular fraud.³⁷⁶ The main distinction between computer-related and traditional fraud is the target of the fraud. If offenders try to influence a person, the offence is generally recognised as fraud. Where offenders target computer or data-processing systems, offences are often categorised as computer-related fraud. Those criminal law systems that cover fraud, but do not yet include the manipulation of computer systems for fraudulent purposes, can often still prosecute the above-mentioned offences.



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 hide the identity by using anonymous communication services

ITU GUIDE

Internet was developed, it was however, much more difficult to get access to Internet user can get access to those instructions.

lines to analyse targets.⁵⁹⁸ A training manual was found during investigations highlighting how useful the Internet is for gathering information on engines, offenders information (e.g., buildings) that help in reported that insurgents in Pakistan used satellite

Means of Control

s - from phone calls to the Internet - technical standards to discussions about the Internet is no and even structure.⁶⁰¹ The

l by laws and law-makers and law enforcement agencies have started to imposing a certain degree of central control.

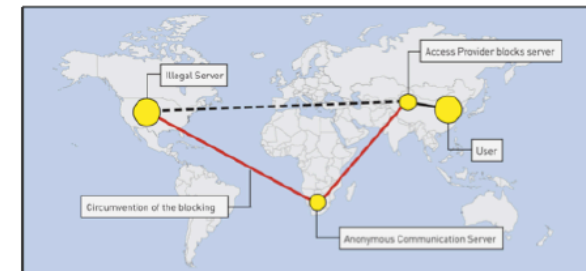


Figure 28

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.

CHALLENGE

- During the discussion yesterday the challenges of botnets and internet cafes were mentioned
- The guide provides a description of the phenomenon “botnet” as well as possible solutions for investigations involving internet cafes and examples for registration obligations

ITU GUIDE

control (See
ation

ious risk
vary,

up to a
ernet
part of a
minal



Figure 32

One example for automation processes is the dissemination of Spam. Millions

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

ITU GUIDE

Stanford Draft Convention

The informal¹¹⁹⁰ 1999 Stanford Draft Convention does not include the Convention on Cybercrime the Draft Convention does only cover an intended system interference.

Example from National Legislation

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

§ 1037. Fraud and related activity in connection with computer systems

(a) In General – Whoever, in or affecting interstate or foreign commerce or financial institutions,

(1) accesses a protected computer without the authorized consent of the owner of the computer, or
transmission of multiple commercial electronic messages,

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

ITU GUIDE

Stanford Draft Convention

The informal¹¹⁹⁰ 1999 Stanford Draft Convention does not in Convention on Cybercrime the Draft Convention does only c 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 connection

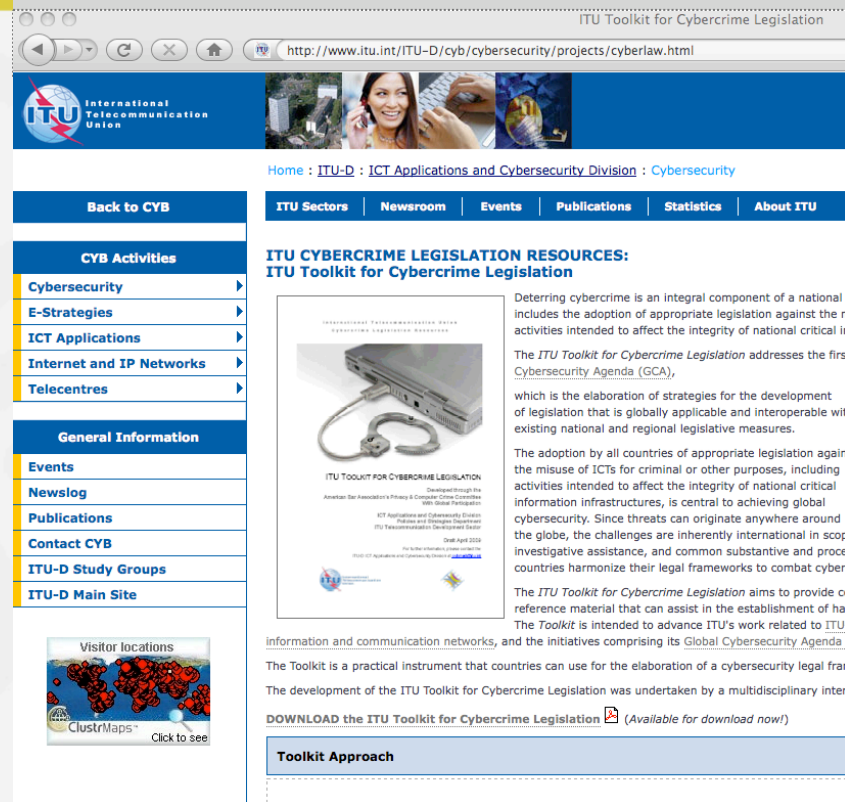
(a) In General – Whoever, in or affecting inters

(1) accesses a protected computer without transmission of multiple commercial electronic

ITU WEBSITE

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

ITU GUIDE



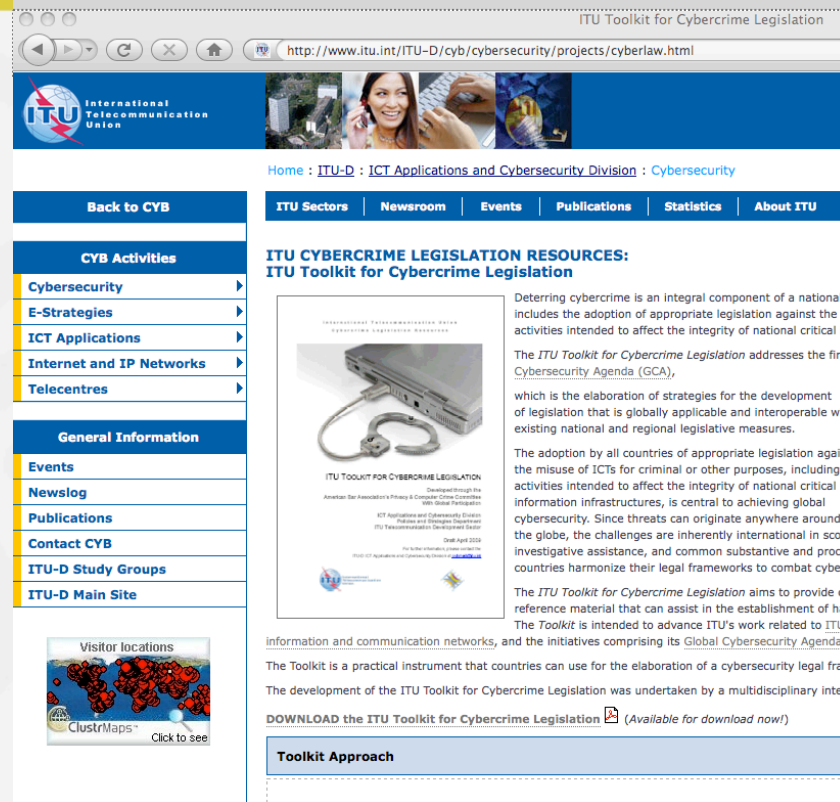
The screenshot shows the ITU Toolkit for Cybercrime Legislation website. The browser address bar displays the URL: <http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html>. The website header includes the ITU logo and the text "International Telecommunication Union". Below the header, there is a navigation menu with links to "ITU Sectors", "Newsroom", "Events", "Publications", "Statistics", and "About ITU". The main content area is titled "ITU CYBERCRIME LEGISLATION RESOURCES: ITU Toolkit for Cybercrime Legislation". It features a large image of a computer monitor and keyboard, with the text "ITU TOOLKIT FOR CYBERCRIME LEGISLATION" and "Download through the American Bar Association's Privacy & Computer Crime Committee Web Global Participation". The text describes the toolkit as a practical instrument for the elaboration of a cybersecurity legal framework, aimed at providing reference material to assist in the establishment of harmonized legal frameworks. A "Download the ITU Toolkit for Cybercrime Legislation" button is visible, with a note "(Available for download now!)".

COMMENTS

cybmail@itu.int

info@cybercrime.de

ITU GUIDE



The screenshot shows the ITU Toolkit for Cybercrime Legislation website. The header includes the ITU logo and the title "ITU Toolkit for Cybercrime Legislation". The main content area is titled "ITU CYBERCRIME LEGISLATION RESOURCES: ITU Toolkit for Cybercrime Legislation". It features a sidebar with navigation links such as "Back to CYB", "CYB Activities", "General Information", and "Visitor locations". The main text describes the toolkit as a practical instrument for the elaboration of a cybersecurity legal framework, developed by the ITU in cooperation with the Global Cybersecurity Agenda (GCA). It mentions that the toolkit is available for download and provides a link to the "Toolkit Approach" section.