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
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.
CURRENT SITUATION

Country with proper legislation

Countries without proper legislation
CURRENT SITUATION

Cooperation possible

Cooperation impossible
• 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 focusing 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
• During 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 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
Examples and Explanation

References and Sources (if available from publicly available sources)
• 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
• 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
• 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
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.
• 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
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.
http://www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html
cybmail@itu.int
info@cybercrime.de