ITU-EC HIPSSA Project

**Support for Harmonization of the ICT Policies
in Sub-Sahara Africa**

**Workshop on Namibia National Transposition of SADC Model
Laws on Cybersecurity, Windhoek, 30 April 2013**

**Cybercrime and the SADC Model Law
– Guiding principles**

Presenter: *Prof Dr Marco Gercke* ITU Consultant

CYBERCRIME AND COMPUTER CRIME

- The term "cybercrime" is narrower than computer-related crimes as it has to involve a computer network

- Computer-related crimes cover even those offences that bear no relation to a network, but only affect stand-alone computer systems

BRINGING CYBERCRIME AND CYBERSECURITY INTO CONTEXT

CYBERCRIME / CYBERSECURITY

- Cybersecurity is broader than just Cybercrime

- If a government employee accidentally drops an external storage device with important data that were not included in backup-plans it is a serious Cybersecurity incident – but not a crime
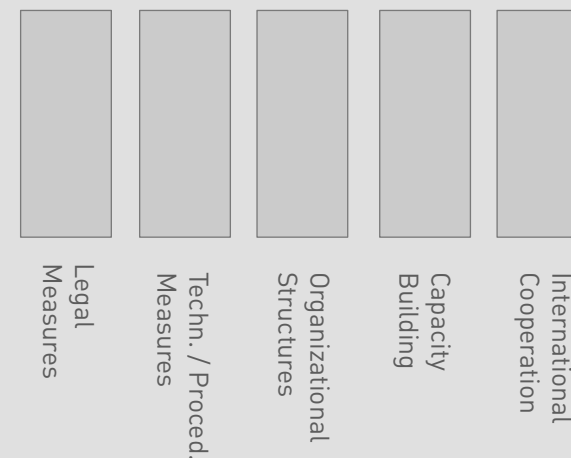
CYBERCRIME / CYBERSECURITY

- Based on the ITU Global Cybersecurity Agenda (GCA) it is possible to divide between 5 different pillars related to Cybersecurity (legal measures, technical and procedural measures, organizational structures, capacity building and international cooperation
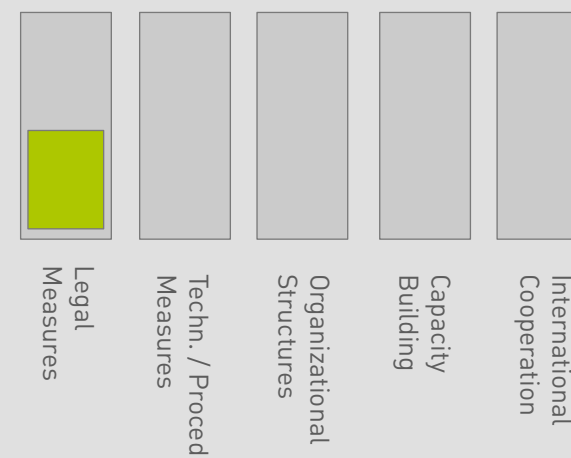
Components of Cybersecurity Strategy (based on ITU GCA)

Legal Measures

Techn. / Proced. Measures

Organizational Structures

Capacity Building

International Cooperation

Context

CYBERCRIME / CYBERSECURITY

- In the beginning of the debate Cybercrime was seen as a part of the pillar dealing with legal measures
- It is certainly true that Cybercrime has a strong legal component
- Without legislation in place law enforcement agencies are unable to carry out investigations and courts cant sentence the accused

Components of Cybersecurity Strategy (based on ITU GCA)

Legal Measures

Techn. / Proced. Measures

Organizational Structures

Capacity Building

International Cooperation

Context

CYBERCRIME / CYBERSECURITY

- Within all pillars Cybercrime needs to be addressed
- In some pillars (such as international cooperation) Cybercrime may even be the dominant part (international cooperation in Cybercrime investigations)
- The same is relevant with regard to legal measures. Cybercrime legislation is in many country the most complex part of a Cybersecurity legal framework

Components of Cybersecurity Strategy (based on ITU GCA)

Legal Measures | Techn./Proced. Measures | Organizational Structures | Capacity Building | International Cooperation
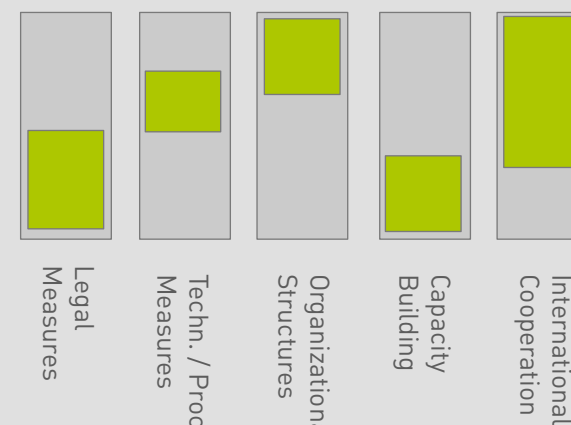
Context

WHAT IS CYBERCRIME ?

DEFINITION

- There are several difficulties with this broad definition

- It would, for example, cover traditional crimes such as murder, if perchance the offender used a keyboard to hit and kill the victim

- Definition developed during the 10th UN Congress is equally challenging

Common Definition

Computer crime is any activity in which computers or networks are a tool, a target or a place of criminal activity

10th UN Crime Congress

Cybercrime in a narrow sense (computer crime) covers any illegal behaviour directed by means of electronic operations that target the security of computer systems and the data processed by them. Cybercrime in a broader sense (computer-related crimes) covers any illegal behaviour committed by means of, or in relation to, a computer system or network, including such crimes as illegal possession and offering or distributing information by means of a computer system or network

DEVELOPMENT OF COMPUTER SYSTEMS

OVERVIEW

- Ever since the use of computer systems started crimes were discovered

- Over the last 50 years every technical development went along with discovering new types of crime

- Most of the crimes that were first discovered 50 years ago are still relevant

- It is unfortunately not incorrect to say that new crimes were added to the list but almost non removed

1960th

- Introduction of transistor based computer systems lead to an increasing use of computers

- Offences at this time were focusing on the physical damage of computer systems and data

- Example: Student riot cause a fire that destroyed computer systems at a university in Canada

1970th

- Further increase in the use of computer systems and data

- Estimated 100.000 mainframe computer operated in the US only

- Physical damage of computer systems remained a relevant offence

- But new forms of crime were also discovered

1970th

- Illegal use of computer systems (that could lead to great financial losses)

- Manipulation of computer data (without and physical interference with the storage devices

- Computer-related fraud (as more and more businesses and financial institutions switched to computer operations)

- Application of existing legislation to this new methods and targets went along with difficulties

1980th

- Increasing use of personal computers

- Lead to an increase in the potential number of targets

- First cases of software piracy

- In addition malicious software was more frequently produced and distributed

1980th - PORNOGRAPHY

- The possibility to electronically distribute pornography was at this time limited

- Computer systems at this time were text-based and the resolution of screens were limited

- Approaches to visualise pornography by using ASCII signs

- Distribution of pornography was at this time focusing on the distribution of text documents

1990th

- Introduction of the graphical user interface WWW (World Wide Web) in the 1990th lead to an increasing popularity of the network

- It became easier to use the services offered

- In addition it enabled the spreading of pictures, audio and video

- In addition the Internet eased transnational communication

- Went along with several challenges for law enforcement

TODAY

- More than 2 billion Internet user

- More Internet users in developing countries than in developed countries

- Globalization of services (with some services having several hundred million users)

- Increasing number of data

- Increasing reliance on computer services

WHAT ARE DIFFERENCES TO TRADITIONAL CRIME

DIFFERENCE

- Committing a traditional crime in general requires physical presence at the crime scene
- Internet crimes don't necessary require that the offender is physically located in the country – he/she can act from abroad
- This has major impact on the work of police as the enforcement of law is in general limited to the territory.
- Outside the territory police can not arrest a suspect acting from another jurisdiction. Investigating crimes with transnational dimension require international cooperation

NUMBER OF CRIMES COMMITTED

UNCERTAINTY REGARDING EXTENT

- Lack of reporting leads to uncertainty with regard to the extent of crime

- This is especially relevant with regard to the involvement of organized crime

- Available information from the crime statistics therefore not necessary reflect the real extent of crime

HEIISE NEWS 27.10.2007

The United States Federal Bureau of Investigation has requested companies not to keep quiet about phishing attacks and attacks on company IT systems, but to inform authorities, so that they can be better informed about criminal activities on the Internet. "It is a problem for us that some companies are clearly more worried about bad publicity than they are about the consequences of a successful
hacker attack," explained Mark Mershon, acting head of the FBI's New York office.

IMPACT OF CYBERCRIME

ECONOMIC IMPORTANCE

- Extent of economic damages caused by cybercrime is controversially discussed

- Many companies (esp. small and medium size businesses) do not report attacks and costs

MISLEADING INFORMATION

- Information that are listed in search engines can influence consumers and business partners in their decisions

- A posting that an e-commerce company is involved in fraudulent activities can for example negatively influence the operator of an online store

- Offenders are setting up websites, manipulate search engines and charge companies to remove the posting

OPPORTUNITIES

OPPORTUNITIES

- Availability of computer technology improved the ability of law enforcement to carry out investigations

- DNA sequence analysis and finger print databases are examples for an emerging use of information technology in traditional criminal investigation

AUTOMATE

- Software tools are available to automate investigations

- Significant reduction of time for an investigation

- One example is the Software PERKEO that detects child pornography pictures on the basis of hash values

AUTOMATE

- Automation techniques can also be used to identify copyright violations

- One example is file-sharing monitoring where software tools can automatically detect copies of copyright-protected art-work made available

- Another example is the automatic scanning of scientific work (like PhD)

OPPORTUNITIES

- Case example 1: Within an investigation of a murder case law enforcement was unable to identify a murder based on search engine history. They were able to use search engine logs on the suspects computer to identify places he was interested in.

DEVICES PROCESSING DATA

- Devices do often store information that are valuable for traditional investigation

- The user do not necessary have knowledge about such operation

- One example is the iPhone that stored the geo-location of the user and thereby enabled the reconstruction of movements/travel

DEVICES PROCESSING DATA

- In addition to "general" meta data the photos might include GPS data that shows where the photo was taken

DIFFERENT CATEGORIES OF CYBERCRIME

Substantive Criminal Law

	Illegal Access to a Computer	Illegal Remaining in a Computer	System Interference	Illegal Interception	Illegal Access to Computer Data	Illegal Data Input	Illegal Aquisition of Comp. Data	Illegal Data Interference	Illegal Use of Data	Violation of Data Protection Regul.	Illegal Devices / Misuse of Devices	Computer-related Fraud	Computer-related Forgery	Indecent Material	Pornography	Child Pornography	Solicitation of Children	Dissemination of Racistic Material	Identity-related Crime	SPAM	Threat and Harassment	Disclosure of an Investigation	Copyright Violation	Violation of Secrecy
Commonwealth Model Law (2002)	✔		✔	✔				✔			✔					✔								
ECOWAS Draft Directive (2009)	✔	✔	✔	✔		✔		✔	✔		✔				✔	✔		✔			✔			
COMESA Model Bill (2011)	✔		✔	✔	✔			✔			✔	✔				✔								
CoE Cybercrime Convention (2001)	✔		✔	✔				✔			✔	✔	✔			✔							✔	
Draft African Union Convention (2011)	✔	✔	✔	✔		✔		✔	✔	✔	✔	✔	✔			✔		✔				✔		✔
SADC Model Law	✔	✔	✔	✔		✔	✔			✔	✔	✔	✔		✔	✔		✔	✔	✔	✔	✔		

CIA Offences · Data Protection Violation · **Computer-related Offences** · **Illegal Content** · Safeguarding Proced. Law · Copyright Violations

Partly covered
✔ Covered

International Telecommunication Union — Committed to connecting the world

European Commission

Jurisdiction

	Territory	Ships and Aircrafts	Nationality	Habitual Residence	Concurrent Jurisdiction
CoE Cybercrime Convention (2001)	✔	✔	✔		
Draft African Union Convention (2011)					
Commonwealth Cybercr. Model Law (2002)	✔	✔	✔		
SADC Model Law	✔	✔	✔		

Criminal Procedural Law	Search	Activating a computer system	Extending Search to other location	Seizure	Record of Seized Data	Copying data	Mainting integrity of data	Rendering data inaccessible	Expedited preservation	Data rention	Partial disclosure	Production Order	Interception of Content	Collection of Traffic Data	Forensic Tools	Transborder Access	Criminal Record Database	Assisting Police	Obligation to disclose passords
CoE Cybercrime Convention (2001)	✔		✔	✔		✔	✔	✔	✔		✔	✔	✔	✔		✔		✔	
Commonwealth Model Law (2002)	✔			✔	✔	✔	✔	✔	✔		✔	✔	✔	✔				✔	
Draft African Union Convention (2011)	✔					✔			✔				✔						
SADC Model Law	✔	✔	✔	✔		✔	✔	✔	✔		✔	✔	✔	✔	✔			✔	

International Telecommunication Union
Committed to connecting the world

European Commission

Thank you for your attention!

INTERNATIONAL TELECOMMUNICATION UNION