
Drafting Cybercrime Legislation

Seminar

Hyderabad, India 25th September 2009

Dr. Marco Gercke

For more information on **ITU's Cybercrime Legislation material** visit the website at: www.itu.int/cybersecurity/
or contact cybmail@itu.int



Committed to connecting the world

Cybercrime Legislation

- Cybercrime has become a major challenge for governments as well as LEA
- It is particularly important if strategies to prevent an abuse of ICT fail
- Cybercrime legislation is therefore considered as an important element of Cybersecurity strategies (see for example the ITU GCA)
- By criminalizing certain serious offences and providing LEA with the necessary instruments to investigate offences (procedural instruments) states can ensure that they are able to identify offenders and take measure to hinder them from acting



Committed to connecting the world

Focus of the training course

- The training course is based on the ITU publication "Understanding Cybercrime: A Guide for Developing Countries"
- Special boxes refer to the guide for further information

See page: 147

Overview

- Introduction
- The phenomena of Cybercrime
- The challenge of fighting Cybercrime
- Drafting Cybercrime legislation

Phenomena of Cybercrime

Definition

- Controversial discussion about defining Cybercrime
- Example 1: *activity in which computers or networks are a tool, a target or a place of criminal activity*
- Example 2: *computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks*

Typology

- Different approaches to develop a typology of Cybercrime
- Offences against the confidentiality, integrity and availability of computer data and systems
- Computer-related offences
- Content-related offences
- Copyright-related offences
- Combined offences

See page: 18

Statistical Information

- Difficult to quantify the impact of Cybercrime
- Various studies available – most of them with a focus on certain businesses or countries
- Example: FBI Computer Crime Survey 2005: Loss to businesses and institutions in the US due to computer crime: 67 Billion US\$
- Despite the difficulties related to such statistics there is an obvious trend towards the use of information technology that could influence the number of computer crimes

See page: 19

Organised Crime

- Cybercrime shows strong links to organised crime
- Distinction between the use of IT by traditional organised crime groups and Cybercrime focused organised crime groups
- Various forms of Cybercrime are already offered by organised crime groups (SPAM, Denial-of-Service Attacks, Virus Attacks)
- Organised crime component enables the use of UN instruments developed to fight organised crime (UNTOC)

CIA Offences

- Offences against the confidentiality, integrity and availability of computer data and systems
- Illegal Access
- Data Espionage
- Illegal Interception
- Data Interference
- System Interference

Illegal Access

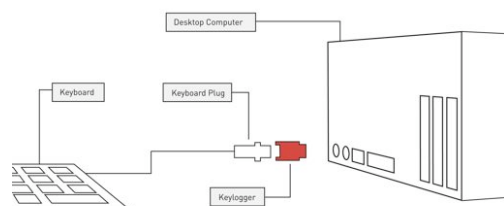
- Accessing (in most cases remotely) a computer, computer system or network without permission
- Traditional computer crime
- In general any computer connected to a network can become the victim of illegal access
- Among the most famous compromised computer systems are: Pentagon, NASA, CIA, German government



See page: 20

Data Espionage

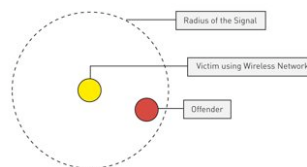
- Valuable and secret information are often stored without adequate protection
- Lack of self-protection especially with regard to small businesses and private computer users
- One example is the use of keyloggers by offernders to get access to credit card information



See page: 23

Illegal Interception

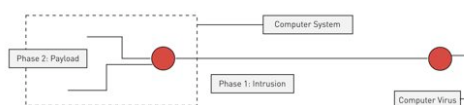
- Network transfer enables the interception of communication
- Vulnerable point is for example the transmission from the computer to the network entry point
- Especially relevant for wireless networks.
- Most cable networks are in addition not protected against the interception of electromagnetic emissions



See page: 25

Data Interference

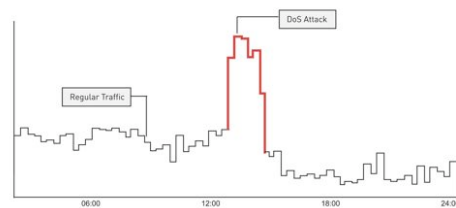
- Negative interaction with regard to computer data
- Example: Computer Virus
- Committing such offence does not necessarily require technical skills.
- Tools available that enable even users without technical background to program viruses



See page: 27

System Interference

- Definition: attempt to make a computer resource unavailable to its intended users
- Example: Denial-of-Service Attacks
- Importance of the availability of computer resources (E-Commerce / Cloud Computing) increase



See page: 28

Content-related Offences

- Offences against the confidentiality, integrity and availability of computer data and systems
- Erotic / Pornographic Material
- Child Pornography
- Hate Speech
- Religious Offences
- Illegal Gambling
- Libel
- Spam

Erotic/Pornographic Material

- "Sex sells"
- Huge number of sexual related business webpages
- Supported by the possibilities of "anonymous" communication
- Making pornographic material accessible without a proper access control is criminalised in some countries



See page: 30

Child Pornography

- In the past often traded through closed circles (e.g. IRC (Chat) and password protected areas)
- Today a growing number of available images and videos
- Demand / Requests could lead to ongoing abuse of children
- No single definitions of child pornography (esp. with regard to virtual child pornography)

Quality	#	Name	Type	Size	Speed	Chat	Bitrate
100%		child pornography: 14yr old girl	avi	2.765 KB	Cable/...		128
100%		15yr, 17yr sex, pamela anderson, porn, movie, illegal, film, hardcore, ha...	avi	8.318 KB	Cable/...		128
100%		porno, SEX CHILD porno	avi	5.474 KB	Cable/...		128
100%		sp by MGSAAAA (child porn movie)	mpg	10.695...	Cable/...		192
75%		hunny school girls (film, chloesey)	mpg	5.176 KB	Cable/...		128
75%		CP 13yr with man	avi	4.124 KB	Cable/...		128
100%		porn, whigpore movie	avi	3.291 KB	Cable/...		128
75%		sp, Britney Spears, porn, Pamela Anderson, sex	avi	6.491 KB	Modem		160

See page: 32

Hate Speech

- Radical groups use mass communication systems such as the Internet to spread propaganda
- In 2006, over 6,000 such websites existed on the Internet
- Not all countries criminalise these offences



See page: 34

Religious Offences

- The Internet offers advantages for those who wish to debate or deal critically with a subject
- A growing number of websites present material that is in some countries covered by provisions related to religious offences
- Many discussion groups are based on the principle of freedom of speech

child pornography (72)							
Quality	#	Name	Type	Size	Speed	Chat	Bitrate
100%	1	child pornography, 14yr old girl	avi	2.765 KB	Cable...	●	128
100%	1	15yr, 17yr sex, pamela anderson, porn, movie, film, hardcore, ha...	avi	8.318 KB	Cable...	●	128
100%	1	porno, SEX CHILD porno	avi	5.474 KB	Cable...	●	128
100%	1	cp by MOGAAAA (child porn movie)	mpg	10.695...	Cable...	●	192
75%	1	horny school girls (film, chloesey)	mpg	5.176 KB	Cable...	●	128
75%	1	CP 13yr with man	avi	4.124 KB	Cable...	●	128
100%	1	porn, chloesey movie	avi	3.291 KB	Cable...	●	128
75%	1	cp, Britney Spears, porn, Pamela Anderson, sex	avi	6.493 KB	Modem	●	160

See page: 35

Illegal Gambling

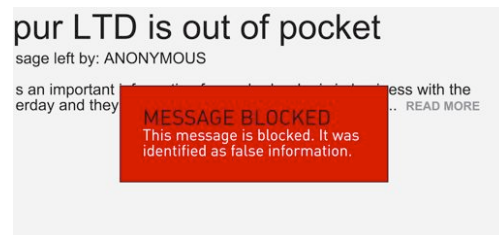
- Internet games and gambling are one of the fastest-growing areas in the Internet
- In addition to classic game of chance online games have become a major attraction in the Internet
- Concerns are especially related to money laundering issues



See page: 36

Libel

- Internet can be used to spread misinformation
- Often offenders take advantage of the fact that providers offering cheap or free publication do not usually require identification of authors or may not verify ID
- Can seriously injure the reputation and dignity of victims as online statements are accessible to a worldwide audience



See page: 37

SPAM

- “Spam” describes the emission of unsolicited bulk messages
- most common scam is e-mail spam
- provider organisations report that as many as 85 to 90 per cent of all e-mails are spam

PETRO VOICE HOLDING
Hot Stock in Momentum play for week

OTC: PHVC
This company is nasdaq bound

Petro Voice in on a roll earning Contrac

This is not a Fly by Night
Real market Cap, Real Earnings

Here are some the latest news on PHVC.

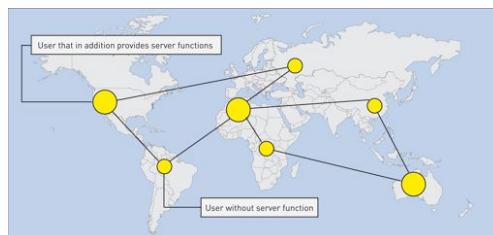
See page: 39

Copyright/Trademark Offences

- Copyright Offences
- Trademark Offences

Copyright Offences

- Digitalisation (Switch from analogue to digital digital distribution) enabled loss free reproduction
- Apart from exchange of copyright-protected songs, music and software
- Circumvention of Digital-Rights Management



See page: 41

Trademark Offences

- "Spam" well-known aspect of global trade
- use of trademarks in criminal activities with the aim of misleading targets
- Domain or name-related offences

● NPW BANK™

Dear Customer,

we would like to inform you, that we need to verify your account. In the last weeks we received a number of complaints with regard to phishing mails. To avoid problems we are asking you to visit the following web-site:

www.npwbank-online.com/security-check/

If you do not go through the procedure within 24 hours we unfortunately need to close your account.

Thank you very much for your cooperation

See page: 44

Computer-related Offences

- Computer-related Fraud
- Computer-related Forgery
- Identity Theft
- Misuse of Devices

Computer-related Fraud

- Fraud one of the most popular crimes on the Internet
- Computer-related fraud enables the offender to use automation
- The main distinction between computer-related and traditional fraud is the target of the act
- Typical examples: Online Auction Fraud, Advance Fee Fraud (419/Nigeria Scam)

My dear friend,

let me introduce myself first of all. My name is Mbuto Butalia. I am the wife of the former President Republic of Thalia. My loved husband recently died in a plane-crash. During the cleaning of this documents I found out that my husband has 10.000.000 US\$ on a secret account.
I would like to transfer this money to my family, that is living in the US. Unfortunately I am not able to transfer the money directly. I would therefore like to ask you for your assistance.
I would like to transfer the 10.000.000 US\$ to your account and ask you if you could transfer 9.000.000 US\$ to my family. The remain 1.000.000 US\$ will be for you. If you agree, I would like to ask you to transfer first of all 10 US\$ to my account so I am able to verify your bank account information.

See page: 45

Computer-related Forgery

- manipulation of digital documents
- includes the scam of “phishing” which is a serious challenge for law enforcement agencies worldwide
- “Phishing” seeks to make targets disclose personal/secret information

See page: 47

● NPW BANK™

Dear Customer,

we would like to inform you, that we need to verify you account. In the last weeks we received a number of complains with regard to phising mails. To avoid problems we are asking you to visit the following web-site:

www.npwbank-online.com/security-check/

If you do not go through the procedure within 24 hours we unfortunately need to close you account.

Thank you very much for your cooperation



Committed to connecting the world

29

Identity Theft

- Term is neither consistently defined nor consistently used
- describes the criminal act of fraudulently obtaining and using another person's identity.
- type of data the perpetrators target varies (SSN, Date of birth, passwords)

See page: 48

● NPW BANK™

Dear Customer,

we would like to inform you, that we need to verify you account. In the last weeks we received a number of complains with regard to phising mails. To avoid problems we are asking you to visit the following web-site:

www.npwbank-online.com/security-check/

If you do not go through the procedure within 24 hours we unfortunately need to close you account.

Thank you very much for your cooperation

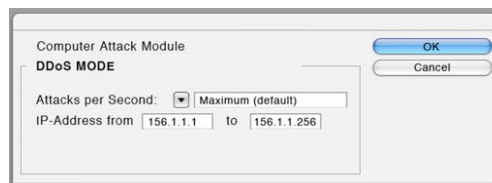


Committed to connecting the world

30

Misuse of Devices

- Cybercrime can be committed using only fairly basic equipment
- More sophisticated offences can be committed using specialist software tools
- tools needed to commit complex offences are widely available over the Internet (eg. To carry out DoS attacks, design computer viruses, intercept communication, ...)



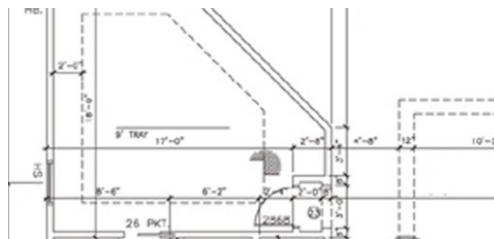
See page: 44

Combined Offences

- Cyberterrorism
- Cyberlaundering

Cyberterrorism

- Terrorist organisations use Internet technology in various ways
- Propaganda
- Information gathering
- Preparation of real-world attacks
- Publication of training material
- Communication
- Terrorist financing
- CIIT attacks



See page: 51

Cyberwarfare

- Use of ICTs in conducting warfare
- Network-based attacks are generally cheaper than traditional military operations
- Incidents in Estonia and Georgia highlight the potential of attacks

ERROR

Due to ongoing military operations this service is not available. We

See page: 57

Challenge of Cybercrime

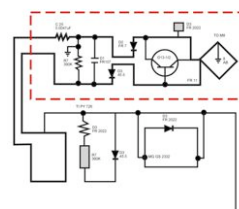
Possibilities

- Improvement of information technology enables the law enforcement agencies to carry out investigations that were not possible previously
- Automated search for key-words / hash-values
- Great chance for public private partnership (eg. Microsofts CETS)



Dependence

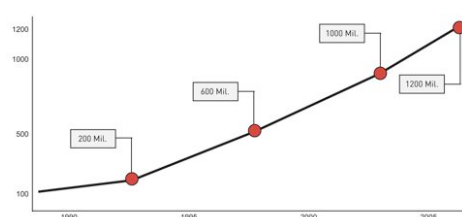
- Increasing dependence of society and businesses on information technology
- ICT is more and more intensively integrated into the everyday life as well as used to run critical infrastructure
- Examples: Energy supply, transportation, stock exchange, communication



See page: 64

Number of users

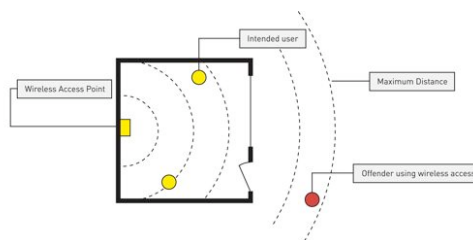
- popularity of the Internet and its services is growing fast
- over 1 billion Internet users worldwide
- In 2005, the number of Internet users in developing countries surpassed the number in industrial nations



See page: 65

Availability of Devices & Access

- Only basic equipment is needed to commit computer crimes
- Hardware, Software and Internet access
- Criminals can use public terminals, open wireless networks, compromised networks or prepaid services to access the Internet with very little chance to trace them back



See page: 66

Availability of Information

- Millions of websites
- Powerful search engines
- „Googlehacking“
- Detailed instructions how to carry out attacks available
- Training manuals published by terrorist organisations

„Bic Bomb“

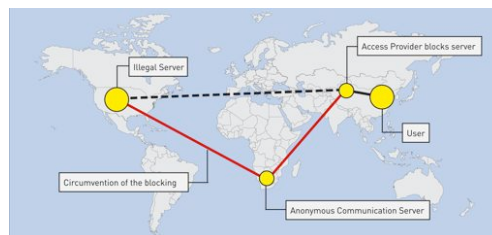
Construction, with the
 connect it to the blue
 before you mix the
 automatic.
 Direct with the remote
 with 20% beta-sol. and

	10mg M
	3mg Su
	3mg Ra

See page: 67

Missing control instrument

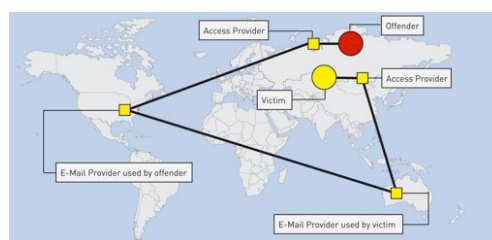
- All mass communication networks - from phone networks used for voice phonecalls to the Internet - need central administration and technical standards to ensure operability
- The Internet was originally designed as a military network based on a decentralised network architecture
- Resisting against control many control approaches



See page: 68

International dimension

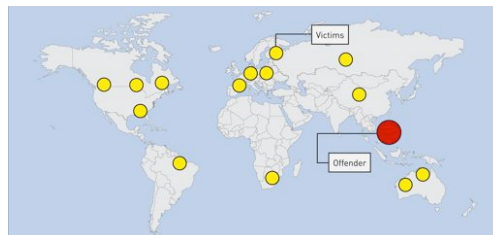
- Many data transfer processes affect more than one country
- Further, many Internet services are based on services from abroad e.g., host providers may offer webspace for rent in one country based on hardware in another.



See page: 69

Independance

- In general criminals need to be present at the crime scene
- With regard to Cybercrime this is not the case
- As the location of the criminal can be completely different from the crime site, many cyber-offences are transnational.
- International cybercrime offences take considerable effort and time



See page: 71

Automation

- With regard to Cybercrime offenders can often automate processes
- Example: SPAM
- By automating processes offenders can gain great profit by designing scams that are based on a high number of offences with a relatively low loss for each victim

See page: 72

Resources

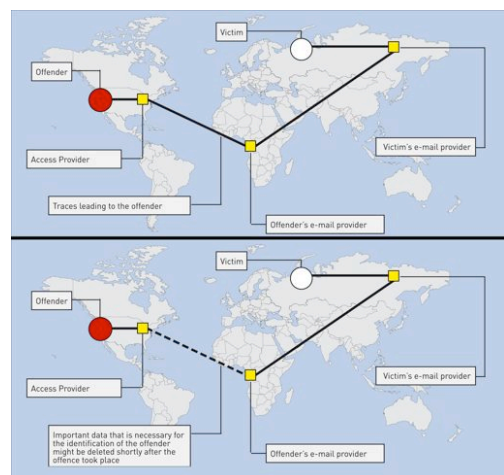
- Background: Botnets
- Botnet: group of compromised computers running programs under external control
- Current analysis suggests that up to a quarter of all computers connected to the Internet could be infected with software making them part of a botnet
- Used for DoS attacks, Sending SPAM, File-Sharing

See page: 72



Speed of exchange process

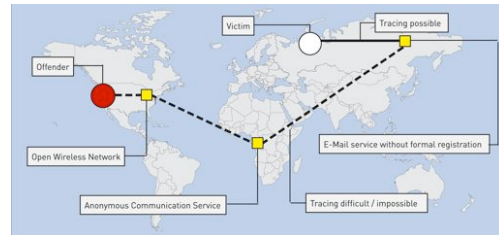
- The transfer of an e-mail between countries takes only a few seconds
- leaves little time for law enforcement agencies to investigate or collect evidence



See page: 73

Anonymous communication

- Using Internet services generates various electronic evidence
- Certain Internet services make it difficult to identify offenders
- Offenders can hide their identities through, for example, the use of fake e-mail addresses or anonymous communication services



See page: 75

Encryption technology

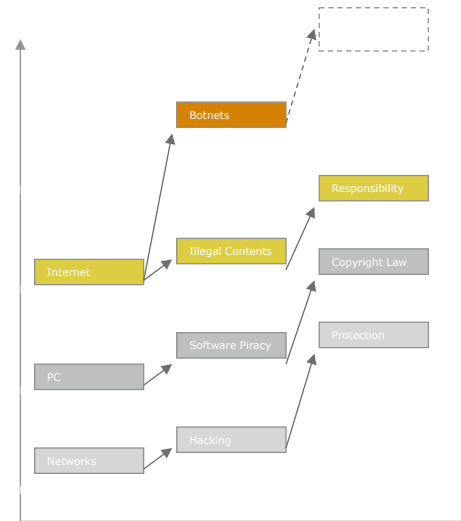
- Another factor that can complicate the investigation of cybercrime is encryption technology
- Like anonymity, encryption is not new, but computer technology has transformed the field
- Using a 56-bit encryption, a single computer would take up to 2,285 years to break the encryption



See page: 75

Legal challenge

- Proper legislation is the foundation for the investigation and prosecution of cybercrime
- Drafting legislation is going along with unique difficulties
- The main challenge for national criminal legal systems is the delay between the recognition of potential abuses of new technologies and necessary amendments to the national criminal law



See page: 79

Drafting Cybercrime Legislation

Necessary steps

- Drafting Cybercrime legislation is in general not based on out-of-the-box solutions but custom made approaches taking into account legal traditions
- Analysing the known extent of offences and threats
- Analysing the current legislation (substantive criminal law, procedural law, international cooperation, responsibility of service providers, ...)
- Comparing national legislation to international standards (if available)
- If gaps exist with regard to international standards a review of the legislation should be taken into consideration to improve the possibility to carry out international investigations
- If with regard to certain crimes no international standards exist, best practice examples from countries with comparable legal systems, can be taken into consideration. Cybercrime Guide provides an overview about such examples.

Thank You!

For more information see the ITU website at:

www.itu.int/cybersecurity/

or e-mail cybmail@itu.int