www.coe.int/cybercrime

Botswana/Council of Europe Cooperation:

Capacity building against cybercrime in Botswana

alexander.seger@coe.int
cristina.schulman@coe.int

Gaborone, 14-15 December 2012

1

Workshop objectives

The workshop is to contribute to the strengthening of the criminal justice capacities of Botswana to meet the challenge of cybercrime through legislation, training and international cooperation.

The workshop is expected to achieve the following results:

- **Participants have a better understanding of strategies and measures to meet the challenge of cybercrime**
- **The legislation of Botswana has been analysed against international standards**
- **Participants are familiar with concepts for judicial and law enforcement training**
- **Needs for further training and other capacity building measures have been identified**
- **Participants have a better understanding of the benefits of the Budapest Convention on Cybercrime for Botswana.**

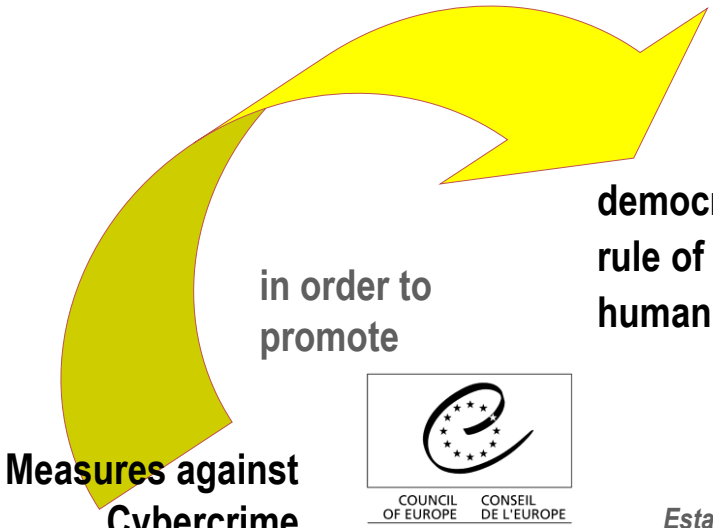
2

Workshop programme	
	Opening
Session 1	About cybercrime and electronic evidence
Session 2	International responses
Session 3	Elements of cybercrime strategies
Session 4	Cybercrime legislation in Botswana
Session 5	Investigation, prosecution, adjudication
Session 6	Judicial and law enforcement training
Session 7	International cooperation
Session 8	Special issues
Session 9	Needs for technical assistance
	Closing: Next steps for Botswana

www.coe.int/cybercrime

3

About Council of Europe … www.coe.int



Established in 1949
Currently 47 member States

4

4

Council of Europe approach on cybercrime

5

Council of Europe: Tools on cybercrime

Useful tools:

- Budapest Convention on Cybercrime (2001)
- Protocol on Xenophobia and Racism by means of computer systems (2003)
- Guidelines for LEA/ISP cooperation in the investigation of cybercrime (2008)
- Judicial training concept (2009)
- Law enforcement training strategies (2011)
- Specialised cybercrime units (2011)
- Criminal money flows on the Internet – Typology study (2012)
- Children benchmark study – discussion paper (2012)
- Cybercrime strategies - discussion paper (2012)
- Electronic evidence guide (January 2013)

See: www.coe.int/cybercrime (Reports)

6

We are here

Workshop programme	
	Opening
Session 1	**About cybercrime and electronic evidence**
Session 2	International responses
Session 3	Elements of cybercrime strategies
Session 4	Cybercrime legislation in Botswana
Session 5	Investigation, prosecution, adjudication
Session 6	Judicial and law enforcement training
Session 7	International cooperation
Session 8	Special issues
Session 9	Needs for technical assistance

7

1 About cybercrime

What is cybercrime?

8

About cybercrime

Session 1

Spoofing
Identity theft
Virus
Trojan
Card fraud
Hacking
Worm
Pharming
Spam
SMSishing
Phishing
Underground economy
Child pornography
Botnets
Cyber-terrorism
Malware
419 fraud
Electronic evidence
Attacks against information infrastructure

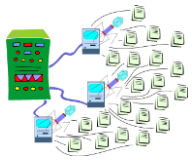
9

9

About cybercrime

Session 1

- Malware
  - Viruses, worms, trojans ►remove security applications, download additional malware, infect files, steal login and account credentials and other data
  - Web remains main vehicle for malware ►infections by visiting infected sites
  - Email threats ► spam as vector for malware and fraud
- Botnets
  - Main tool for cybercrime and
  - Main risk for cybersecurity (DDOS)
  - Organising for cybercrime



- Criminal domains ►anonymous and „bullet proof“ hosting of criminal domains
- Organising for cybercrime
  - underground economy
  - organised crime
  - persistent threats against political or economic targets
- Money mules
- Technology/context
  - Social networking platforms
  - Cloud computing

10

10

About cybercrime

Session 1

Norton 2012 Cybercrime Report

- 1.5 million victims of consumer cybercrime daily
- Global "price tag" of consumer cybercrime: US$ 110 billion/year
- Changing cybercrime: social networks and mobile devices
- 4/10 social network users have fallen victim

RSA monthly

- 49,488 unique phishing attacks in August 2012
- Mobile malware (SMS sniffers, premium dialers, spyware, botnet clients)

11

11

About cybercrime

Session 1

Fraud

Internet Crime Complaint Center, USA (2011 report)

- 314,246 complaints in 2011
- US$ 485 million loss reported

BKA (Germany) – cybercrime situation report 2011

- 59,494 cybercrime offences in narrow sense recorded in 2011
- 26,723 computer-related fraud
- 15,726 interception of data/espionage
- 222,267 cases with Internet as tool for crime

12

12

Botnets

- Zeus Botnet servers takedown by Microsoft and financial groups (March 2012)
- Nitol Botnet takedown by Microsoft (September 2012)

"Trojan.Prinimalka is a banking trojan associated with an attack campaign that received quite a bit of press in October 2012. "Project Blitzkrieg" is "a new cybecriminal [sic] project aimed at recruiting 100 botmasters to help launch a series of lucrative online heists targeting 30 U.S. banks. The Trojan installs a proxy on the victim host and then sends system/web browser details back to the C&C. The botmasters can use this setup to "spoof" banking requests as the unsuspecting banking user" (Arbor Networks Security blog)

DDOS and CIIP attacks

- 1 Nov 2012: 1200+ denial of service attacks in past 24 hours (ARBOR SERT Atlas threat index)
- Estonia 2007
- Georgia 2008
- Korea 2011
- DDOS attacks against civil society organisations
- Hacktivism
- Advanced persistent threats

About cybercrime

Online child sexual violence

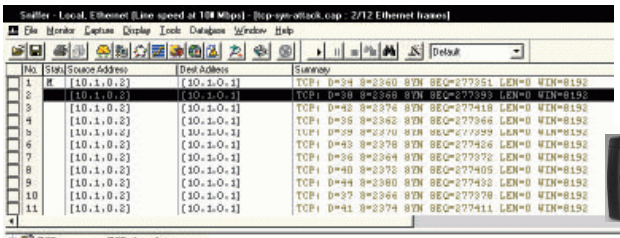
- **Operation Rescue (March 2011) - a global paedophile network consisting of thousands of online members was shattered, resulting in more than 200 children being safe-guarded and 184 offenders arrested across the globe (Virtual Global Taskforce)**

- **OPERATION SNAPSHOT LEADS TO 30 INVESTIGATIONS OF ON-LINE CHILD PREDATORS (Canada, RCMP, 17 October 2012)**

15

About cybercrime

Electronic evidence in relation to ANY crime



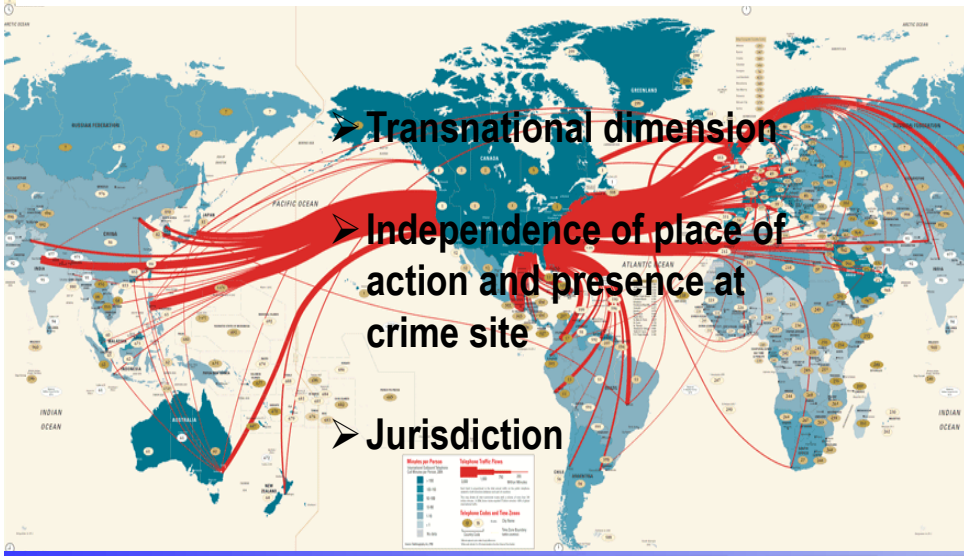
16

16

17

Crime scene

Session 1



18

About cybercrime

How to translate this into a criminal law response?

Substantive law:

- Offences against computer systems
- Offences by means of computer systems

Procedural law:

- Powers for criminal justice authorities to secure volatile electronic evidence in relation to any crime
- Safeguards

International cooperation:

- Efficient cooperation to secure evidence

About cybercrime

Points to retain:

- Cybercrime affects all of us
- Cybercrime and electronic evidence are transversal criminal justice challenges
- Cybercrime and electronic evidence are/should be of concern to all criminal justice authorities

We are here

Workshop programme	
	Opening
Session 1	About cyb crime and electronic evidence
Session 2	Internatio esponses
Session 3	**Elements of cybercrime strategies**
Session 4	Cybercrime legislation in Botswana
Session 5	Investigation, prosecution, adjudication
Session 6	Judicial and law enforcement training
Session 7	International cooperation
Session 8	Special issues
Session 9	Needs for technical assistance
	Closing: Next steps for Botswana

21

3 Cybercrime strategies Session 3

Cybercrime and cybersecurity: what is the difference?

22

22

Cybercrime vs cybersecurity

Cybersecurity

Typically defined as:

the protection of the confidentiality, integrity and availability of computer data and systems in order to enhance security, resilience, reliability and trust in ICT

Motivated by:

- Reliance on ICT -> national interest
- Economic potential of ICT
- CIIP -> National security

Protection against:

- Non-intentional incidents
- Intentional attacks by state and non-state actors against ICT (c-i-a attacks)

Measures:

- Protection, mitigation, recovery through technical, procedural, institutional measures (vulnerability analyses, early warning/response, CERT/CSIRTs, etc)
- Cybercrime legislation, investigation, international cooperation

Cybercrime vs cybersecurity

Cybercrime

Defined as:

- Offences against computer data and systems (c-i-a offences) (Articles 2-6 Budapest Convention)
- Offences by means of computers (such as Articles 7-10 Budapest Convention)

Motivated by:

- Crime prevention and criminal justice

Protection against:

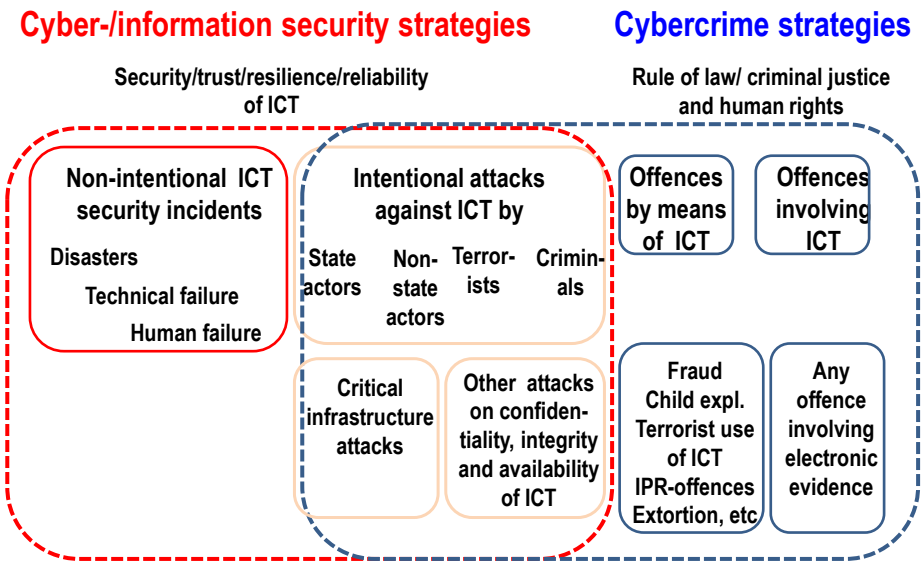
- Intentional attacks against and by means of computers
- Any crime involving electronic evidence on a computer system

Measures:

- Investigation, prosecution, adjudication
- Conditions and safeguards
- Prevention
- Technical and other measures

Cybercrime vs cybersecurity

Session 3



25

25

Elements of a cybercrime strategy

Session 3

Objective

Protection against:

- Intentional attacks against and by means of computers
- Any crime involving electronic evidence on a computer system

- Cybercrime reporting
- Prevention
- Legislation, incl. safeguards and data protection
- Specialised units
- Interagency cooperation
- Law enforcement training
- Judicial training
- Public/private cooperation
- Effective international cooperation
- Financial investigations and fraud/ML/TF prevention
- Protection of children

26

26

What policies & strategies in Botswana?

We are here

Workshop programme	
	Opening
Session 1	About cybercrime and electronic evidence
Session 2	**International responses**
Session 3	Elements of cybercrime strategies
Session 4	Cybercrime legislation in Botswana
Session 5	Investigation, prosecution, adjudication
Session 6	Judicial and law enforcement training
Session 7	International cooperation
Session 8	Special issues
Session 9	Needs for technical assistance
	Closing: Next steps for Botswana

2 International responses

About the

Budapest Convention on Cybercrime

About Budapest Convention

Opened for signature November 2001 in Budapest

Followed by Cybercrime Convention Committee (T-CY) = Committee of the Parties

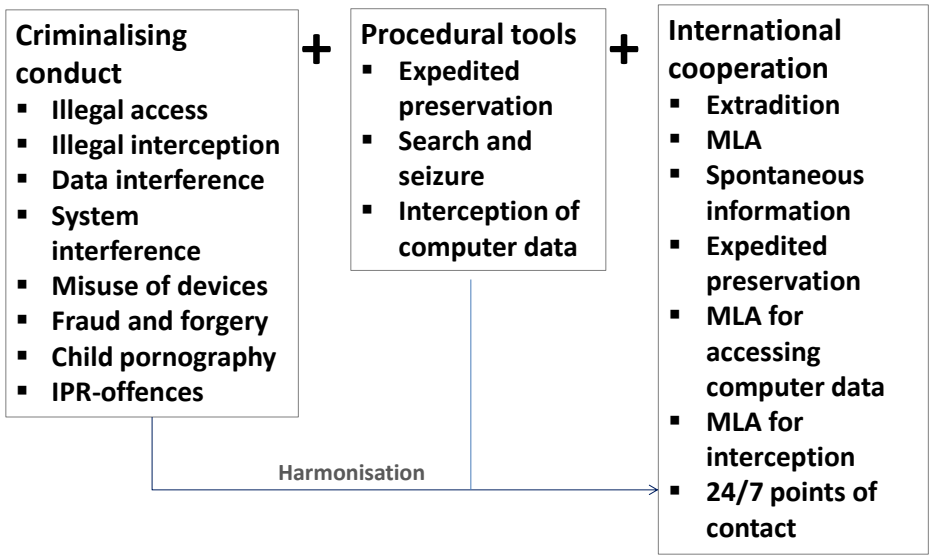
As at December 2012:

- 38 parties (35 European, Australia, Japan and USA)
- 9 signatories (European, Canada, South Africa)
- 8 states invited to accede (Argentina, Chile, Costa Rica, Dominican Republic, Mexico, Panama, Philippines, Senegal)

= 56 states are parties/are committed to become parties

- Many more have used Budapest Convention as a guideline for domestic legislation

Scope of the Budapest Convention on Cybercrime



31

31

International standards: Substantive criminal law

Article	Budapest Convention	Domestic law of Botswana
Art. 1	Definitions	Sections 2 (interpretation) CCRCA 2007
Art. 2	Illegal access	Sections 4 (unauthorised access to a computer or computer system) and 5 (to computer service)
Art. 3	Illegal interception	Sections 5 (1b) (unauthorised access to computer service) and 9 (unlawful interception of data)
Art. 4	Data interference	Sections 7 (unauthorised interference with data) and 12 (damage to a computer or computer syst)
Art. 5	System interference	Section 8 (unauthorised interference with a computer or computer system) and 12 (damage to a computer or computer system)
Art. 6	Misuse of devices	Section 10 (unlawful possession of devices or data) and 11 (unauthorised disclosure of password)

32

32

International standards: Substantive criminal law

Article	Budapest Convention	Domestic law of Botswana
Art. 7	Computer-related forgery	Section 15a (cyber fraud)
Art. 8	Computer-related fraud	Section 15b (cyber fraud)
Art. 9	Child pornography	Section 16 (1b) and (3) (electronic traffic in pornographic or obscene material)
Art. 10	IPR offences	
Art. 11	Attempt, aiding, abetting	
Art. 12	Corporate liability	

33

International standards: Procedural law

Article	Budapest Convention	Domestic law of Botswana
Art. 15	Conditions and safeguards	
Art. 16	Expedited preservation	Section 20 (Preservation order)
Art. 17	Expedited preservation and partial disclosure of traffic data	Section 21 (Disclosure of preserved data)
Art. 18	Production order	Section 22 (Production order)
Art. 19	Search and seizure	Section 23 (Access, search and seizure)
Art. 20	Real-time collection traffic data	Section 24 (Real-time collection of traffic data)
Art. 21	Interception of content data	-
Art. 22	Jurisdiction	Section 3

34

Budapest Convention: Impact 11 years on

Session 2

Achievements:

- Process of legislative reforms worldwide
- Increased criminal justice measures
- Increased trust and cooperation between parties
- Global outreach, global impact: 56 countries ratified, signed, invited to accede. Cooperation with at least another 50 countries
- Catalyst for capacity building
- Increased legal certainty and trust by private sector
- An essential element of norms of behaviour for cyberspace
- Contribution to human rights and the rule of law in cyberspace
- Protecting you and your rights

Update (Dec 2012)

1. T-CY started assessment of implementation by Parties
2. Transborder access: towards Guidance Note and Protocol

35

Acceding to the Budapest Convention

Session 2

Treaty open for accession (article 37)

Phase 1:

- A country with legislation in place or advanced stage
- Letter from Government to CoE expressing interest in accession
- Consultations (CoE/Parties) in view of decision to invite
- Invitation to accede

Phase 2:

- Domestic procedure (e.g. decision by national Parliament)
- Deposit of the instrument of accession

36

36

Acceding to the Budapest Convention

Benefits

- ✓ Trusted and efficient cooperation with other Parties
- ✓ Participation in the Cybercrime Convention Committee (T-CY)
- ✓ Participation in future standard setting (Guidance Notes, Protocols and other additions to Budapest Convention)
- ✓ Enhanced trust by private sector
- ✓ Technical assistance and capacity building

"Cost": Commitment to cooperate

Disadvantages?

International standards

Legislation of Botswana seems to be largely in line with the Budapest Convention on Cybercrime
+ benefits:

▶ Accession by Botswana?

We are here

Workshop programme	
	Opening
Session 1	About cyb crime and electronic evidence
Session 2	Internation responses
Session 3	Elements cybercrime strategies
Session 4	**Cybercrime legislation in Botswana**
Session 5	Investigation, prosecution, adjudication
Session 6	Judicial and law enforcement training
Session 7	International cooperation
Session 8	Special issues
Session 9	Needs for technical assistance
	Closing: Next steps for Botswana

39

4 Cybercrime legislation in Botswana Session 4

Legislation:

What do you need?

What do you have already?

40

40

What conduct is a crime?

▶ Substantive criminal law

Article 2 of the Convention: illegal access

Establish as criminal offences under domestic law, when committed intentionally, the access to the whole or any part of a computer system without right. A Party may require that the offence be committed by infringing security measures, with the intent of obtaining computer data or other dishonest intent, or in relation to a computer system that is connected to another computer system

Cybercrime and Computer Related Crimes Act Chapter (2007)

4. Unauthorised access to a computer or computer system

(a) accesses the whole or any part of a computer or computer system, knowing that the access he or she intends to secure is unauthorised; or

(b) causes a computer or computer system to perform any function as a result of unauthorised access to such system […]

5. Unauthorised access to computer service

(a) secures access to any computer or computer system for the purpose of obtaining, directly or indirectly, any computer service […]

The legal framework: Substantive criminal law

Session 4

Article 3 of the Convention: Illegal interception

Establish as criminal offences under domestic law, when committed intentionally, the interception without right, made by technical means, of non-public transmissions of computer data to, from or within a computer system, including electromagnetic emissions from a computer system carrying such computer data. A Party may require that the offence be committed with dishonest intent, or in relation to a computer system that is connected to another computer system.

5. Unauthorised access to computer service

9. Unlawful interception of data

A person who intentionally and by technical means, without lawful excuse or justification, intercepts-

(*a*) any non-public transmission to, from or within a computer or computer system; or

(*b*) electromagnetic emissions that are carrying data, from a computer or computer system, commits an offence and shall on conviction be sentenced to a minimum fine of P10,000 but not exceeding P40,000, or to or to imprisonment for a minimum term of six months but not exceeding two years, or to both.

43

43

The legal framework: Substantive criminal law

Session 4

Article 4 of the Convention: data interference

Establish as criminal offences under domestic law, when committed intentionally, the damaging, deletion, deterioration, alteration or suppression of computer data without right.

Article 5 of the Convention: system interference

Establish as criminal offences under domestic law, when committed intentionally, the serious hindering without right of the functioning of a computer system by inputting, transmitting, damaging, deleting, deteriorating, altering or suppressing computer data.

7 Unauthorised interference with data

(a) destroys, deletes, suppresses, alters or modifies data;

(b) renders data meaningless, useless or ineffective;

(c) obstructs, interrupts or interferes with-

(i) the lawful use of data, or

(ii) any person in the lawful use of data; or

(d) denies access to data to any person entitled to it […]

8. Unauthorised interference with a computer or computer system

(a) hinders or interferes with the functioning of a computer or computer system; or

(b) hinders or interferes with a person who is lawfully using or operating a computer or computer system […]

term "hinder"

44

44

The legal framework: Substantive criminal law

Session 4

Article 6 - Misuse of devices

1 Establish as criminal offences under domestic law, when committed intentionally and without right:

a the production, sale, procurement for use, import, distribution or otherwise making available of:

i a device, including a computer program, designed or adapted primarily for the purpose of committing any of the offences established in accordance with the above Articles 2 through 5;

ii a computer password, access code, or similar data by which the whole or any part of a computer system is capable of being accessed

10. Unlawful possession of devices or data

- manufactures, sells, procures for use, imports, exports, distributes or otherwise makes available, a computer or computer system or any other device, designed or adapted for the purpose of committing an offence under this Act
- receives, or is in possession of, one or more of the devices under subsection (1),
- found in possession of any data or programme with the intention that the data or programme be used, by the person himself or herself or by another person, to commit or facilitate the commission of an offence under this Act

[…]

45

45

The legal framework: Procedural law

Session 4

What legal powers for investigators and prosecutors:

▶ Procedural criminal law

+ safeguards

46

46

The legal framework: Procedural law

Procedural measures in Botswana

20. Preservation order
21. Disclosure of preserved data
22. Production order
23. Access, search and seizure
24. Real time collection of traffic data
17. Unlawful disclosure by service provide

Interception of content data?

The legal framework – procedural law safeguards

Procedural powers (articles 16 to 21 Budapest Convention) are to be:

"subject to conditions and safeguards provided for under its domestic law which shall provide for the adequate protection of human rights and liberties..." (article 15)

The legal framework – procedural law safeguards

- **Principle of proportionality**, meaning in particular that "the power or procedure shall be proportional to the nature and circumstances of the offence". For example, particularly intrusive measures, such as interception, are to be limited to serious offences
- **Judicial or other independent supervision**
- **Grounds justifying the application of the power or procedure and the limitation on the scope or the duration**
- **Powers and procedures must be reasonable and "consider the impact on the rights, responsibilities and legitimate interests of third parties"**

49

The legal framework – issues

- **Illegal access to computer or computer system (Section 4) versus illegal access to computer service (Section 5): what is the difference?**
- **Access with the intent to commit an offence (Section 6): how to prove?**
- **Illegal interception: unlawful interception of data (Section 9) versus unauthorised access to computer service (Section 5b): what difference?**
- **Illegal interception: no provisions in Botswana?**
- **Admissibility of electronic evidence?**
- **Status of *Electronic Records (Evidence) Bill (EREB) was drafted in 2007?***

50

We are here

Workshop programme	
	Opening
Session 1	About cyb crime and electronic evidence
Session 2	Internation responses
Session 3	Elements cybercrime strategies
Session 4	Cybercri egislation in Botswana
Session 5	**Investigation, prosecution, adjudication**
Session 6	Judicial and law enforcement training
Session 7	International cooperation
Session 8	Special issues
Session 9	Needs for technical assistance
	Closing: Next steps for Botswana

51

5 Specialised cybercrime services

Once you have the laws: what is next?

- Specialised institutions
- Law enforcement training
- Judicial training

52

52

Specialised institutions (good practice study)

Session 5

Primary role of specialised cybercrime units:

- Investigating and/or prosecuting offences against computer data and systems
- Investigating and/or prosecuting offences committed by means of computer data and systems
- Carrying out computer forensics with respect to electronic evidence in general

Strategic task:

- Cybercrime strategies
- Legislation
- Analysis, intelligence
- Reporting systems, etc.

Tactical tasks:

- Conducting investigations
- Coordination operations
- Collection and analysis of electronic evidence, etc.

53

Specialised institutions

Session 5

Types of specialised units:

- Cybercrime units (crimes against and by means of computers)
- High-tech crime units (crimes against computers)
- Computer forensic units
- Central units (policy, analysis, coordination, support)
- Crime-specific units (e.g. carding, CAM)
- Prosecution-type units

Creating a specialised unit – Steps:

1. Assessing needs and making a decision
2. Legal basis
3. Manager of the unit
4. Staffing the unit
5. Training programme
6. Equipment and other resources
7. Independence of and knowledge about unit
8. Action plan / evaluation mechanism

54

Specialised institutions

What specialised institutions / what specialisation in Botswana

- For cybercrime investigation / prosecutions?
- For computer forensics?

55

We are here

Workshop programme	
	Opening
Session 1	About cyb crime and electronic evidence
Session 2	Internation esponses
Session 3	Elements cybercrime strategies
Session 4	Cybercrim egislation in Botswana
Session 5	Investigat , prosecution, adjudication
Session 6	**Judicial and law enforcement training**
Session 7	International cooperation
Session 8	Special issues
Session 9	Needs for technical assistance
	Closing: Next steps for Botswana

56

6 Training

Law enforcement training strategies - Elements

Justification for adopting/investing in a strategy:

- Reliance on ICT
- Most crime involve e-evidence
- All LEOs to be trained
- Technological developments

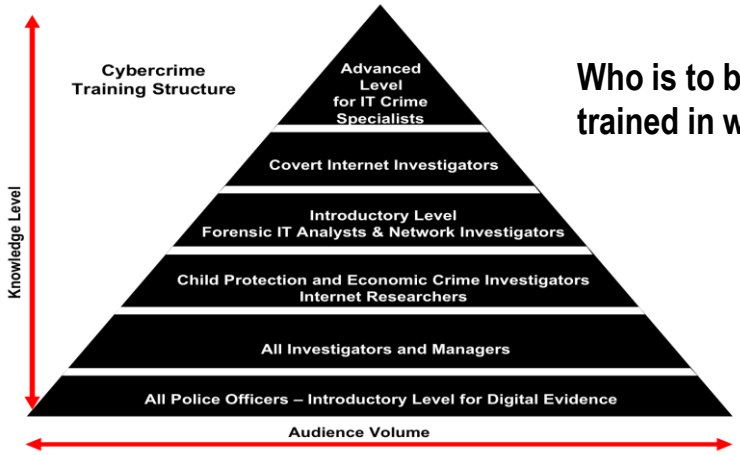
Objective of a strategy

To ensure that LEA agencies/officers have the skills/ competencies necessary for their respective functions to

- investigate cybercrime
- secure electronic evidence,
- carry out computer forensics analyses for criminal proceedings
- assist other agencies
- contribute to network security

Law enforcement training needs analysis

Who	Skills required



Who is to be trained in what?

Judicial training concept

Session 6

Core problem:

- All judges and prosecutors must be prepared to deal with cybercrime
- Existing training too limited and ad hoc, not institutionalised
- Standardised initial and in-service training required
- Need possibility to progress from basic to advanced levels

Purpose of concept 2009:

- to help judicial training institutions develop training programmes on cybercrime and electronic evidence for judges and prosecutors
- to integrate such training in regular initial and in-service training

59

59

Judicial training concept

Session 6

Approach supported in South-eastern Europe:

1. Develop modules for basic and advanced training on cybercrime and electronic evidence
2. Train trainers
3. Deliver pilot training
4. Institutionalise: integrate such training in the regular curriculum of judicial training institutions
5. Establish centre for judicial training to network and update materials

60

60

LEA and judicial training

What training is available / needed in Botswana

- ▶For law enforcement?
- ▶For judges and prosecutors?

We are here

Workshop programme	
	Opening
Session 1	About cyb crime and electronic evidence
Session 2	Internation responses
Session 3	Elements cybercrime strategies
Session 4	Cybercrim egislation in Botswana
Session 5	Investigat , prosecution, adjudication
Session 6	Judicial a law enforcement training
Session 7	**International cooperation**
Session 8	Special issues
Session 9	Needs for technical assistance
	Closing: Next steps for Botswana

7 International cooperation

How to enable efficient international cooperation?

International cooperation

Article	Budapest Convention
Art. 23	General principles (subsidiarity)
Art. 24	Extradition
Art. 25	General rules
Art. 26	Spontaneous information
Art. 27	MLA in absence of treaty
Art. 28	Confidentiality
Art. 29	Expedited preservation
Art. 30	Partial disclosure traffic data
Art. 31	MLA accessing data
Art. 32	Transborder access
Art. 33	MLA collection traffic data
Art. 34	MLA interception content
Art. 35	24/7 point of contact

Efficiency of provisions to be assessed by T-CY in 2013

International cooperation: 24/7 CP

Article 35 – 24/7 Network

1 Each Party shall designate a point of contact available on a 24/7 basis, in order to ensure the provision of immediate assistance for the purpose of investigations or proceedings concerning criminal offences related to computer systems and data, or for the collection of evidence in electronic form of a criminal offence. Such assistance shall include facilitating, or, if permitted by its domestic law and practice, directly carrying out the following measures:

a the provision of technical advice;

b the preservation of data pursuant to Articles 29 and 30;

c the collection of evidence, the provision of legal information, and locating of suspects.

2 a. A Party's point of contact shall have the capacity to carry out communications with the point of contact of another Party on an expedited basis.

b. If the point of contact designated by a Party is not part of that Party's authority or authorities responsible for international mutual assistance or extradition, the point of contact shall ensure that it is able to co-ordinate with such authority or authorities on an expedited basis.

3 Each Party shall ensure that trained and equipped personnel are available, in order to facilitate the operation of the network.

65

The legal framework: International cooperation

International cooperation on cybercrime and electronic evidence:

▶ what challenges for Botswana?

66

We are here

Workshop programme	
	Opening
Session 1	About cyb crime and electronic evidence
Session 2	Internation responses
Session 3	Elements cybercrime strategies
Session 4	Cybercrim egislation in Botswana
Session 5	Investigat , prosecution, adjudication
Session 6	Judicial a law enforcement training
Session 7	Internatio cooperation
Session 8	**Special issues**
Session 9	Needs for technical assistance
	Closing: Next steps for Botswana

67

8 Related specific issues

Session 8

- Data protection
- Online sexual violence against children
- Financial investigations and money laundering

68

Data protection

Session 8

Why data protection?

- Data protection/privacy a fundamental right
- Condition for human rights, democracy and rule of law
- Condition for law enforcement cooperation
- Condition for off-shoring
- Helps protect confidentiality, integrity and availability of data and systems

"Personal data" is any personal information which can lead to the identification of someone

69

Data protection

Session 8

Council of Europe data protection standards

"Data Protection Convention 108"
Convention for the Protection of Individuals with regard to Automated Processing of Personal Data (28 January 1981)

"Data Protection Protocol 181"
Additional Protocol to Convention 108 "regarding supervisory authorities and transborder flows" (2001)

Soft-law Recommendations (14)
Rec(1987)15 Use of personal data in the police sector
Rec(2010)13 Processing of personal data for profiling

70

Data protection

Session 8

Future of Convention 108

Open for accession by non-member states

- Uruguay invited in 2011
- Accession under consideration in other countries

Modernisation of Convention 108

Modernisation underway to

- Meet new challenges of information and communication technologies
- Provide for follow up (monitoring) mechanism
- Draft text finalised in Nov 2012 for negotiation in 2013

71

About the Lanzarote Convention on sexual violence against children

Session 8

Opened for signature October 2007 in Lanzarote

Followed by Lanzarote Convention Committee (T-ES) = Committee of the Parties

Open for accession by any country (Morocco invited to accede November 2012

As at November 2012:

- 23 Parties
- 22 Signatories

It provides for:

- Preventive measures
- Specialised authorities and co-ordinating bodies
- Protective measures and assistance to victims
- Intervention programmes or measures
- Recipients of intervention programmes and measures for persons
- Information and consent
- Substantive law
- Investigation, prosecution and procedural law
- International cooperation
- Monitoring mechanism

72

Budapest +Lanzarote = Benchmarks

Session 8

Lanzarote Convention

- Substantive criminal law
  - Art 18 Sexual abuse
  - Art 19 Child prostitution
  - Art 20 Child pornography
  - Art 21 Child participation in pornographic performances
  - Art 22 Corruption of children
  - Art 23 Solicitation of children for sexual purposes

+

Budapest Convention

- Substantive criminal law
  - Article 9 Child pornograpy
- Procedural law (scope and specific provisions)
  - Expedited preservation
  - Search and seizure
  - Interception
  - etc
- International cooperation (general and specific provisions)

73

73

Legislative benchmark study: work in progress

- Objective: to demonstrate how the Budapest and Lanzarote Conventions can be used by any State as benchmarks for developing substantive criminal law
- Provisions covered (almost all covering multiple acts):
  - Article 18 LC: sexual abuse
  - Article 9 BC and Article 20 LC: child pornography
  - Article 21 LC: participation of a child in pornographic performances
  - Article 19 LC: child prostitution
  - Article 22 LC: corruption of children
  - Article 23 LC: grooming
  - Aggravating circumstances
  - Who is a child/minor
- 45 countries covered in the present version

74

74

Legislative benchmark study: definitions

Child pornography
(Article 9 Budapest / Article 20 Lanzarote Conventions)

The term "child pornography"= pornographic material that visually depicts:

- a minor engaged in sexually explicit conduct
- a person appearing to be a minor engaged in sexually explicit conduct
- realistic images representing a minor engaged in sexually explicit conduct
- any material that visually depicts a child engaged in real or simulated sexually explicit conduct or any depiction of a child's sexual organs for primarily sexual purposes

75

75

Legislative benchmark study

Example: Child pornography (Article 9 BC and 20 LC)

Conduct	Covered	Partially	Not / unclear
Producing child pornography/for the purpose of distribution through a computer system	40	5	
Offering child pornography	37	7	1
Making available child pornography	37	6	2
Distributing child pornography	42	2	1
Transmitting child pornography	36	3	6
Procuring child pornography for oneself or for another person	31	1	13
Possessing child pornography	38	4	3
Knowingly obtaining access	18	7	20

76

76

Definition of 'child pornography' in Botswana

Section 16 CCRCA: Electronic traffic in pornographic or obscene material

***b*) "child pornography" includes material that visually or otherwise depicts-**
(i) a child engaged in sexually explicit conduct;
(ii) a person who appears to be a child engaged in sexually explicit conduct; or
(iii) realistic images representing a child engaged in sexually explicit conduct;
(*c*) "child" means a person who is under the age of 14 years;
(*d*) "sexually explicit conduct" means any conduct, whether real or simulated, which involves-

77

77

Child pornography in Botswana

16. Electronic traffic in pornographic or obscene material
(3) A person who-
(*a*) publishes child pornography or obscene material relating to children through a computer or computer system;
(*b*) produces child pornography or obscene material relating to children for the purpose of its publication through a computer or computer system;
(*c*) possesses child pornography or obscene material relating to children in a computer or computer system or on a computer data storage medium;
(*d*) publishes or causes to be published an advertisement likely to be understood as conveying that the advertiser distributes or shows child pornography or obscene material relating to children; or
(*e*) accesses child pornography or obscene material relating to children through a computer or computer system, commits an offence and shall be sentenced to a minimum fine of P40,000 but not exceeding P100,000, or to imprisonment for a minimum term of two years but not exceeding three years, or to both.

78

78

Solicitation of children for sexual purposes/ grooming (Article 23 Lanzarote Convention)

The intentional proposal, through information and communication technologies, of an adult to meet a child who has not reached the age below which it is prohibited to engage in sexual activities with a child for the purpose of committing any of the following offences and where this proposal has been followed by material acts leading to such a meeting:

- engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities
- producing child pornography

79

79

Legislative benchmark study

Example: Grooming (Article 23 LC)

Conduct	Covered	Partially	Not / unclear
Grooming for the purpose of			
• engaging in sexual activities with a child who, according to the relevant provisions of national law, has not reached the legal age for sexual activities	18	3	24
• producing child pornography	17	3	25

80

80

Grooming in Botswana

(4) A person who, by means of a computer or computer system, communicates with-
(*a*) a person who is, or who the accused believes is**, under the age of 18 years, for the purpose of facilitating the commission of the offence of child pornography under this Act**, or the offences of prostitution, rape or indecent assault under the Penal Code;
(*b*) a person who is, or who the accused believes is, **under the age of 16 years, for the purpose of facilitating the commission of the offences of abduction or kidnapping** of that person under the Penal Code; or
(*c*) a person who is, or who the accused believes is, **under the age of 16 years, for the purpose of facilitating the commission of the offence of defilement or any sexual offence** of that person under the Penal Code,
commits an offence and shall be sentenced to a minimum fine of P40,000 but not exceeding P100,000, or to imprisonment for a minimum term of two years but not exceeding three years, or to both.

Some issues identified

- **Age limit in relation to child pornography or other forms of exploitation and abuse: Protect all children up to the age of 18, irrespective of the age of sexual consent**

- **Child pornography vs. adult pornography: the protected legal interest**

Financial investigations and money laundering

Linking anti-money laundering and anti-cybercrime worlds

MONEYVAL / Global Project on Cybercrime: Typology study

Criminal money flows on the Internet: methods, trends and multi-stakeholder counteraction

Start: Octopus Conference & MONEYVAL Plenary 2009
End: Adopted/published March 2012

(see: www.coe.int/cybercrime (reports)

Note:
Revised 40 Recommendations of FATF:
consider joining Budapest Convention

83

Financial investigations and money laundering

Study: Cybercrime and predicate offences on the Internet

- Fraud
  - identify theft
  - man-in-the-middle-attacks
  - payment card fraud
  - account take over
  - mass-marketing fraud
  - pyramid schemes
  - confidence and action fraud
- Child abuse materials
- Counterfeit medicines
- IPR
- Extortion
- Many other forms of traditional crimes committed on the Internet

84

Financial investigations and money laundering

Session 8

Study: Red flags and indicators for potential money laundering

- Persons holding large number of accounts with the same Internet payment services provider
- Discrepancies between submitted customer identification and IP address
- Suspicious IP addresses, and suspicious usernames
- Log-ins or attempting log-ins from non trusted IP addresses or from user's ID previously identified as associated with suspicious activity
- Unusual conditions and complexity of the transaction: high frequency of money transfers in a short time, large and diverse source of funds, large and diverse payment methods for the beneficiaries
- Etc.

85

Financial investigations and money laundering

Session 8

Study: Countermeasures – The way ahead

- Research and other measures to prevent/mitigate AML/TF and cybercrime risks
- AML/CTF and anti-cybercrime strategies
- Legislation (harmonised with Budapest Convention and Convention 198)
- Reporting mechanisms
- Guidance and typologies for financial and non-financial institutions
- Specialised cybercrime units
- Inter-agency cooperation and parallel financial investigations when pursuing cybercrime and money laundering
- Public-private cooperation and information exchange on criminal money flows on the Internet
- Training of criminal justice and AML authorities in cybercrime and electronic evidence matters
- International cooperation between FIUs and Cybercrime Units

86

We are here

Workshop programme	
	Opening
Session 1	About cyb crime and electronic evidence
Session 2	Internation responses
Session 3	Elements cybercrime strategies
Session 4	Cybercrim egislation in Botswana
Session 5	Investigat , prosecution, adjudication
Session 6	Judicial a law enforcement training
Session 7	Internatio cooperation
Session 8	Special is es
Session 9	Needs for technical assistance
	Closing: Next steps for Botswana

87

9 Technical assistance & next steps

Session 9

What technical assistance needs for Botswana?

1. Legislation
2. Specialised institutions
3. Law enforcement training
4. Judicial training
5. International cooperation
6. Public/private cooperation
7. Data protection
8. Child online protection
9. Financial investigations

Thank you!

www.coe.int/cybercrime

88