COOPERATION AGAINST CYBERCRIME

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Harmonising cyber laws in the ECOWAS region

Regional workshop, Accra, Ghana, 18-21 March 2014

Training on cybercrime and electronic evidence

Alexander.seger@coe.int

www.coe.int/cybercrime

1

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

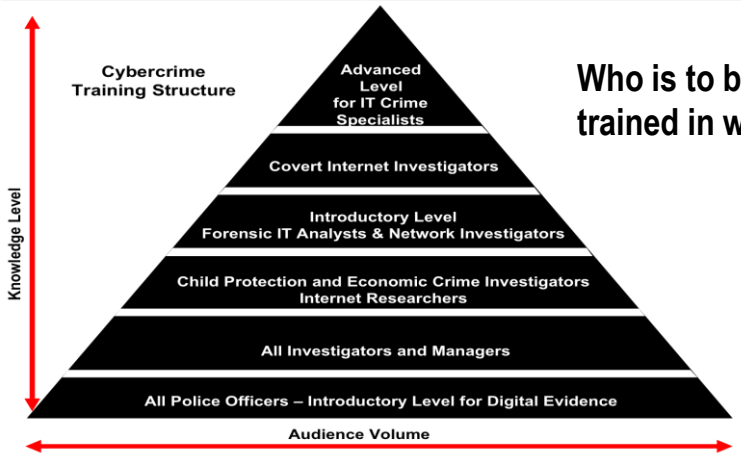
To ensure that LEA agencies/officers have the skills/ competencies necessary for their respective functions to

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

2

Law enforcement training needs analysis

Who	Skills required



Who is to be trained in what?

3

Law enforcement training materials

Council of Europe:

- **Electronic evidence guide**
- **First responder training pack**

European Cybercrime Training and Education Group (ECTEG):

- **Training materials prepared and updated**
- **Access to these materials …**

4

Judicial training concept 2009 (CoE)

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

5

Judicial training concept 2009 (CoE)

Approach proposed:

1. Institutionalising initial training
2. Institutionalising in-service training
3. Standardised and replicable courses/modules
4. Access to training/self-training materials
5. Pilot centres for basic and advanced training
6. Enhancing knowledge through networking
7. Public private cooperation

6

Judicial training concept : implementation

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

7

Judicial training concept : implementation

Similar support through GLACY project on Global Action on Cybercrime to:

1. Mauritius (Party to Budapest Convention)
2. Morocco (invited to accede to Budapest Convention)
3. Senegal (invited to accede to Budapest Convention)
4. South Africa (signed Budapest Convention)

See concepts, reports and materials at: www.coe.int/cybercrime

8