COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Workshop on cybercrime and cybersecurity policies and legislation

Cybercrime: criminal justice capacities

San José, Costa Rica, 7-9 March 2012

Alexander Seger
Council of Europe,
Strasbourg, France
Tel +33-3-9021-4506
alexander.seger@coe.int

1

Strengthening criminal justice capacities: tools and good practices

Law enforcement training

LEA training strategies developed under the CyberCrime@IPA project (2011)

Judicial training

Judicial training concept (prosecutors and judges) adopted in 2009 under Global Project on Cybercrime. Now implemented in South-eastern Europe

Specialised cybercrime units

Good practice study on police-type units prepared in 2011 in cooperation with European Union Cybercrime Task Force

www.coe.int/cybercrime

2

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

www.coe.int/cybercrime

3

Law enforcement training strategies - Elements

Training needs analysis

Who	Skills required

Who is to be trained in what?

4

Law enforcement training strategies - Elements

Implementation: training programmes

1. Subjects to be trained
2. Training institutions
3. Delivery of training
4. Training materials
5. Updating of materials

5

2 Judicial training concept

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

www.coe.int/cybercrime

6

Judicial training concept

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

3 Specialised cybercrime services

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.

Specialised cybercrime services

Type 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