COUNCIL OF EUROPE CONSEIL DE L'EUROPE

www.coe.int/cybercrime

Concept paper: cybercrime training for judges and law enforcement

Octopus Interface conference: Cooperation against cybercrime (Strasbourg, 23-25 March 2010)

Cristina Schulman
Council of Europe
Strasbourg, France
Tel +33-3-8841-2103
cristina.schulman@coe.int

Why a concept on cybercrime training for judges and prosecutors?

- increasing number of offences against or committed through ICT and cases involve electronic evidence stored on computer systems or other devices

- judges and prosecutors must be prepared to deal with cybercrime and electronic evidence

- in most cases, judges and prosecutors encounter difficulties in coping with the new realities of the cyber world

- ensure the independence of judges and prosecutors while allowing them to have access to private sector expertise

The concept: background

- Lisbon Network Bureau: involve LN in drafting the concept with the Project on Cybercrime (Bucharest, 20 March 2009)

- Replies of 11 European judicial training institutions to a questionnaire (Belgium, Croatia, Georgia, Germany, France, Netherlands, Poland, Portugal, Romania, Spain, "the former Yugoslav Republic of Macedonia") and the United Kingdom

- Meeting with representatives from Belgium, Ireland, Italy, Portugal, Netherlands, UK and private sector (Lisbon, July 2009)

- Workshop with training institutions representatives, judges and prosecutors of the 11 countries, private sector, the European Judicial Training Network and the Lisbon Network (Strasbourg 3-4 September 2009)

Information suggested:

- in most countries cybercrime training offer is far too limited
- both initial and in-service training cover only basic level
- very few courses are offered, reaching only a very small number of judges and prosecutors
- standardised training materials for replicable training are usually not available and
- they do not allow a judge or prosecutor to progress from basic to advanced level in a systematic manner
- with few exceptions training offering knowledge at advanced level for judges and prosecutors is not available

The concept

The purpose:

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

The objectives:

- enable training institutes to deliver initial and in-service cybercrime training based on international standards
- equip the largest possible number of future and practicing judges and prosecutors with basic knowledge on cybercrime and electronic evidence
- provide advanced training to a critical number of judges and prosecutors
- support the continued specialisation and technical training of judges and prosecutors
- contribute to enhanced knowledge through networking among judges and prosecutors
- facilitate access to different training initiatives and networks.

The 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**

- It includes also **typical training modules** to provide basic and advance knowledge on cybercrime and electronic evidence

- The concept shows **how judicial training institutions can benefit from support by industry and academia** through standardised training programmes and other means

1. Institutionalising initial training

- practical training on the job - at least part of such training to be related to cybercrime and electronic evidence

- training is provided by judicial training institutions - their curricula should contain basic level module on cybercrime and electronic evidence

- specific training modules should be standardised to be replicable and allow candidates to progress from basic to advanced levels

2. Institutionalising in-service training

- In-service training institutions should offer at least one basic level module on cybercrime and electronic evidence (to equip with basic knowledge judges and prosecutors who had not such training in their initial training)

- offer courses for advanced knowledge

3. Standardised and replicable courses modules

- Develop standardised courses or modules that can be replicated at a broad scale in a cost-effective manner and allow to progress from basic to advanced

- Evaluate the existing basic and advanced level courses that could be integrated into the curricula of initial or in-service training programmes

- Subsequently, a standard basic and advanced course to be recommended

- Such courses and training to be delivered by local trainers in local languages and only limited needs of international trainers

4. Access to training/self training materials

- Training materials need to be developed reflecting common international standards and good practices

- Develop standardised training materials for judges and prosecutors in a way that leaves sufficient room to take into account domestic systems and legislation

- On-line courses should be developed and made available

5. Pilot centres for basic and advanced training

- A number of pilot centres for basic and advanced training of judges and prosecutors on cybercrime and electronic evidence should be established to:
  - test and further develop standardised courses and materials, disseminate good practices, carry out research on training, maintain a register of trainers, offer training of trainers, provide training to other countries with similar systems and languages
  - Pilot centres should coordinate their work with each other with the support of the Council of Europe
  - Judges and prosecutors, who are prepared to become specialists, consider participating in training through the centres of excellence for law enforcement and industry

6. Enhancing knowledge through networking

- Make use of existing networks for judges or prosecutors (such as GPEN)

- Creation of an international network of cybercrime or e-crime judges (similar to GPEN for prosecutors)

- the Council of Europe should map initiatives and networks and establish a portal with links, brief information and contact details on different networks to facilitate:

  - access by judges and prosecutors to cybercrime-related networks and existing training materials and the coordination among networks

7. Public Private Cooperation

- Support of the private sector:
  - could be beneficial as the private sector disposes of relevant subject matter expertise
  - must not be conceived to potentially secure favourable decisions in court or to generate business
  - provided in a transparent manner or through international organisations, academia, training initiatives or other third parties
  - Judicial training institutions may make use of private sector expertise when designing training programmes, training materials and delivering courses

The way ahead?

- Promote implementation of the concept throughout Europe and beyond

- Provide specific support to training institutions that are prepared to include cybercrime training into their curricula (the whole concept or elements of it). For example:

  - developing and providing access to training curricula and materials

- Cooperation with partners to support the implementation in:
  - Europe
  - Egypt
  - India
  - Pakistan
  - Georgia
  - Other countries and regions

THANK YOU FOR YOUR

ATTENTION

CRISTINA.SCHULMAN@COE.INT