Training on cybercrime and electronic evidence

Virgil SPIRIDON
Head of Operations
C-PROC, Council of Europe

Brussels, 20 September 2019

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

www.coe.int/cybercrime

COE approach on cybercrime and electronic evidence training

- Deliver training activities (basic/advanced/specialised)
- Train the trainers that further can deliver training
- To involve training institutes
- To facilitate the introduction into national curricula the topics on cybercrime and electronic evidence
- Joint training for LE-Judiciary

Challenges for LE training on cybercrime and electronic evidence

- Identify the needs of the countries
- Prepare the training strategy/plan
- Updated training materials
- Experts
- Profile of the participants in the training activities

COE trainings on cybercrime and electronic evidence

- Resources:
  - developed in house (EEG, FLG, SOP)
  - developed by other LE or international organisations
  - ECTEG
- Cybercrime training (first responder, specialised)
- Electronic evidence training (network forensic, computer forensic, mobile forensic)
- Training format (simulation exercise)
- Support the participation in international/regional training activities

Challenges for judicial training programmes

- Sustainability of judicial training programs
- Continuous update of the judicial training programs
- Getting judges and prosecutors interested in the programs and actively participating
- Programs reach out to all the judges and prosecutors in the country
- Impact assessment/ Measurement mechanism
- Participation and support of the higher level of the judiciary and of the prosecution service

Challenges for judicial training programmes

- High turnover of the trainer judges and prosecutors
  - Incentive mechanisms should be identified to retain trainers in the national pool
  - A mechanism should be established to make sure that the pool of national trainers is periodically joined by newly formed trainers
- The pool of national trainers is kept updated on content
- Trainers to be joined by one IT expert/ LE officer
- Certification programs
- Networking with regional and international peers

WAYS ahead…

- Adoption of a national strategy on judicial training which could ensure:
  - Establishment and maintaining of a pool of national trainers on cybercrime and electronic evidence
  - Initial and Continuous training on cybercrime streamlined in the regular curricula of the respective training institutions
  - Methodology to distribute, in the medium term (2-3 years), introductory notions on cybercrime and electronic evidence to all prosecutors and judges in the country. E-learning platform could be considered to this purpose.
  - Incentives and allocation of time for trainers, for both delivery and professional training

WAYS ahead…

- Adapting training materials to the domestic context
  - Expectations to be communicated to the trainers in advance
  - Focal points to be established in the national judicial/ prosecutors' training academy
  - Systematic evaluation of results achieved and communication of feedback
- Engagement of other national entities and agencies, public and private, who deal with cyber security
- To consider making initial training compulsory for the newly recruited judges/ prosecutors

International Network

- Define priorities of action, including courses to be developed
- Definition of common criteria to establish an evaluation and reporting mechanism on the effectiveness of the training programs
- Agreement on a common mechanism for national trainers' certification
- Periodic meetings to share experiences and get updates
- Cooperation with other Networks


Virgil.spiridon@coe.int
www.coe.int/cybercrime