

AFRICAN FORUM ON CYBERCRIME

Judicial Training Principles

Zahid Jamil
Council of Europe

Addis Ababa – 18 October 2018



Principles of Judicial Training on cybercrime and electronic evidence

Judicial training in cybercrime and electronic evidence is a **multidisciplinary** and **practical** type of training, essentially intended for the transmission of **professional techniques** and values complementary to legal education.

Training is **part of the normal working life** of a judge and a prosecutor. **All judges and prosecutors should have time and opportunity** to undertake training as part of the normal working time, unless it exceptionally jeopardises the service of justice.

In accordance with the principles of judicial independence the **design**, **content** and **delivery** of judicial training in cybercrime and electronic evidence are exclusively for **national institutions** responsible for judicial training to determine.

Judicial training in cybercrime and electronic evidence should be crafted in a manner that **responds to the needs** of judges and/or prosecutors by conducting a **needs assessment**, taking into account existing **international standards and cooperation instruments**, in particular the Budapest Convention on Cybercrime.

Judicial training should be designed in **consultation** with appropriate **experts** by **practicing** judicial office holders or **trainers** with appropriate professional skills, under **judicial direction**.

Training in cybercrime should **primarily** be delivered by **judges** and **prosecutors** who have been **previously trained for** this **purpose**.

All judges and prosecutors should receive **initial training** in cybercrime and electronic evidence before or on their appointment.

All judicial office holders should undertake a programme of **continuing education** in cybercrime and electronic evidence. There should also be a system of **incentives** introduced with respect to judicial training in the area of cybercrime.

Judicial office holders **who design and deliver** judicial training in cybercrime and electronic evidence will receive **continuous training and advice** for that purpose.

Active and modern educational techniques should be given **primacy** in judicial training on cybercrime and electronic evidence.

Face to face training and **e-learning** are both core methods of judicial training in cybercrime and electronic evidence. The most effective face to face training is that which requires **active participation** by judicial office holders in a **supportive environment** and gives them the opportunity to **practise** and **develop** skills. The most effective elearning is that which requires judicial office holders to participate in **interactive learning online.**

Partnering with academia or other parties from the public sector could **enhance** the training programmes on cybercrime and electronic evidence and help **covering** a **range of issues** relevant to the judicial role in the field.

Participating in **international projects** for judicial training in cybercrime and electronic evidence **reinforces** the judiciary's position and is key to effectively tackle the cross-border nature of cybercrime and issues related to electronic evidence.

Evaluation of judicial training in cybercrime and electronic evidence should ensure that officers attain the expected **competencies** and should result into **continuous development and improvement**, in a **cost-effective manner**. This activity should be mandated to a **Judicial Training Institute**, where present.

The **highest** judicial authorities should **support** and participate in judicial training in cybercrime and electronic evidence.

States should **provide** national **institutions** responsible for judicial training with **sufficient funding** and other **resources** to achieve their aims and objectives.



Recommendations for National Judicial Training Strategy on Cybercrime & Electronic Evidence



Template

- Vision / Overarching Objective
- Responsibility
- Principles
- Priorities
- Objectives
- Approach
- Implementation
- Evaluation / Review / Improvement



Vision/Overarching Objective

[Articulate the Vision and the Mission statement of the Strategy]

- Identify any possible reference to the National Cyber Security or Cybercrime Strategies and Policies

[Identify the Entity(s) as well as Partners responsible for Oversight, Implementation and Review of the strategy]

- Identify the coordinating authority that should oversee the implementation
- Identify the lead competent authority and any entities/authorities with which to coordinate
- When drafting the strategy take into account the complexity of the legal and technical language
- Mention the consultation process and the stakeholders consulted to arrive at the Strategy

[Insert the Principles that will be the guiding values of the Strategy]

- Select from the “Principles of Judicial Training on cybercrime and electronic evidence”, provided under the GLACY+ Project

[Identify the aspects of the Strategy that should be prioritized]

[List the Objectives and the Targets of the Strategy]

SMART criteria to set the objectives

- Specific
- Measurable
- Achievable
- Realistic
- Time-bound

Specific and measurable

- Specify the number of people to be trained within a certain timeframe

- Time bound targets
 - Divide the Strategy into Time bound targets:
 - Short term (e.g. 12 months – Provide introductory training with support from external entities)
 - Medium term (e.g. 3 years – Identify and train a pool of resource persons from the national authorities)
 - Long term (e.g. 5 years – Fully sustainable training courses are provided on cybercrime and electronic evidence on a continuing basis)

- Pool of trainers:
 - Consider if and how to establish a pool of resource persons
 - Evaluate the feasibility of setting up a center of excellence, also for the training of trainers, which could act either on national or on regional level

- Target categories of trainees:
 - Specify the Categories of trainees for the judiciary (eg. Judges and Prosecutor)
 - In case the aim is set to train all categories – different professionals may be trained separately, but as a part of the broader training strategy, in coordination with other competent authorities
 - Specify the categories of trainees to be included in the broader strategy: attorneys, police officers, forensic experts etc.
 - Include all levels of any particular category (eg. Magistrate, First Instance Judges up to Supreme Court Judges)
 - Specify if there need to be any difference between prosecutors and judges (establish joint training courses complemented by specialized modules for specific professions)
 - Consider the subdivision of trainees (by region or jurisdiction)
 - Mention the various types, kinds or range of curriculum and trainings that should be prepared and delivered for a specific period

[Identify the elements of the approach to be undertaken]

Multidisciplinary approach

- Adopt the multidisciplinary approach in the broader sense, to include:
 - different disciplines within the law (including international comparative jurisprudence)
 - different skills required to apply the law
 - e.g. science, technology, digital forensics, financial frauds, BEC, IPR, child pornography, digital copyright, terrorism, human trafficking, online sexual exploitation, online drug trafficking, cryptocurrencies, etc.

Mandatory Training

- State the extent to which and details of how training of newly inducted judicial officers and prosecutors should be compulsory
- State the extent to which and details of how the continuing training of sitting (in office) judicial officers and prosecutors should be compulsory (including any exceptions if necessary)

Resources

- State the sources, such as organizations or public funds, and the suitability of the resource

Partners

- Public Sector - Identify State and Public Sector entities that can contribute to the implementation of the strategy
 - Domestic Agencies,
 - Regional Organizations [ASEAN, ECOWAS, SAARC, etc.],
 - International Organizations [Council of Europe, etc.]
- Private Sector – Consider the private sector participation under the supervision of the competent authority (Ministry of Justice etc.), in:
 - assisting in the delivery of the training
 - assisting in the design of the training content

caveat: where there may be potential of a perception of bias or dealing with a potential litigant party these should be avoided or supervisory safeguards should be introduced where Judicial authorities supervise the activities and delivery of the trainings



Implementation

[Include the actual implementation elements]

- Specify how it is expected to achieve the goals
- Specify Modules, Time period and Levels of training
 - (e.g. Introductory/ Intermediate/ Advanced)
- Specify Format of the training
 - Face-to-face
 - Training Materials
 - eLearning
 - Reports
 - Case Studies
 - Podcasts
 - Bibliographies
 - Handbooks and Guidelines
 - Short term exchanges



Implementation

- Identify contemporary subjects that are pressing at the national level in matters related to cybercrime and electronic evidence
- Include practical case-based examples
- There should be consultation and coordination for the implementation of the Strategy with other relevant/specialized authorities where judges and prosecutors are involved in addition to the Judicial Training Institutes
- Judicial Institutes from various countries should assist, coordinate and cooperate with each other for judicial training support, updates on the latest cybercrime activities and case law, collaboration and exchanges



Evaluation / Review / Improvement

[Include the evaluation plan and the periodic updates]

- Define a process for a continuing evaluation, review and improvement of the strategy, possibly undertaken by external/ independent evaluators
- Consider the following dimensions: Effectiveness, Efficiency, Relevance, Coherence, Sustainability.
- Establish an independence to the evaluation based on judicial and non-judicial stakeholders