HANDBOOK FOR DEVELOPING

JUDICIAL TRAINING STRATEGIES

ON CYBERCRIME AND ELECTRONIC EVIDENCE

Prepared by
Cybercrime Programme Office
of the Council of Europe (C-PROC)

Acknowledgements

The present *Handbook for Developing Judicial Training Strategies on Cybercrime and Electronic Evidence* was prepared under the Global Action on Cybercrime Extended (GLACY+), Global Action on Cybercrime Enhanced (GLACY-e) and iPROCEEDS-2 joint projects of the European Union and the Council of Europe. The work on this document was coordinated by the Cybercrime Programme Office of the Council of Europe (C-PROC) and contributions were received from the following experts: Philippe Van Linthout (Belgium), Jan Kerkhofs (Belgium) and Zahid Jamil (Pakistan).

Contact

Cybercrime Division
Council of Europe Directorate General Human Rights and Rule of Law
F-67075 Strasbourg Cedex (France)
E-mail: cybercrime@coe.int

Disclaimer

Legal notice

The information in this Handbook is intended for general guidance and educational purposes, with the aim of developing or enhancing a national judicial training strategy on cybercrime and electronic evidence and must be considered subject to applicable policies, laws and circumstances in the country concerned. It should not be construed as legal advice or professional guidance. The expertise and general guidance offered in this Handbook draw from the best practices identified throughout C-PROC's capacity-building exercises in countries all over the world and are provided for the consideration and evaluation of the reader.

The examples, descriptions and discussions in this Handbook are intended as options for consideration, rather than as recommendations, encouragement or definitive proposals. Any actions, proposals, measures or policies developed on the basis thereof must be taken with reference to the applicable laws as verified and tested in the relevant jurisdictions by readers.

Links to external publications or websites included in this Handbook are provided as references only, and do not constitute an endorsement by the Council of Europe of those publications or their content. It is the responsibility of the user to evaluate the content and usefulness of information obtained from other such publications/websites.

Contents

1 Background

The continuous expansion of cybercrime in today's highly digitalized societies and the complexity of cases involving electronic evidence requires a comprehensive counteraction strategy. Sustainable judicial training, especially in the field of cybercrime and electronic evidence, is therefore an indisputable must. Prosecutors and judges should to a large extent take care of keeping their knowledge in this area up to date themselves. In their daily work, prosecutors and judges are confronted with new, sometimes very complex challenges, which need to be remedied with appropriate training and exchange of experiences with peers in the same situation.
Given the general deficit of training that many countries are facing in an ever-changing and challenging cyber space, the Cybercrime Programme Office (C-PROC) of the Council of Europe has been supporting over the last decade a vast number of countries to strengthen their capacity to fight cybercrime. In the framework of several capacity building projects, the Council of Europe has elaborated training materials, has facilitated the organisation of judicial training courses on cybercrime and electronic evidence, has created and prepared pools of judges, magistrates, and prosecutors to become national trainers for their peers, has organised webinars on relevant topics to enhance the sharing of experience, and has worked with training institutions to integrate relevant modules into regular curricula.

Starting with 2019, C-PROC supported the community of national judicial trainers by setting up the International Network of National Judicial Trainers ("the Network"). In the Second Meeting of the Network in November 2020, several challenges were identified both generally and at a national level when designing, implementing and delivering training on cybercrime and electronic evidence.

General challenges included pursuing sustainability of judicial training programs, ensuring the continuous update of the structure and contents of judicial training programs, increasing participation of judges and prosecutors, including higher level of judiciary and prosecution services (especially in jurisdictions where trainings cannot be mandated) and reaching all criminal justice authorities.

Challenges identified at a national level included a high turnover of trainers and the need to formulate incentive mechanisms to retain trainers, ensure continuous training of the national trainers, ensuring that trainers are supported by an IT expert and law enforcement officer to deal with technical aspects of electronic evidence and chain of custody, introducing certification programs for national trainers, and networking with regional and international peers.

During the 2022 Plenary meeting of the Network, several action lines meant to respond to these challenges were identified, including the development of this Handbook.

2 Purpose of this Handbook

The Handbook intends to provide national authorities a practical step-by-step approach to creating, implementing, and managing a judicial training strategy on cybercrime and electronic evidence based on the extensive experience of C-PROC in supporting capacity building exercises in countries all over the world. Its purpose is to guide national authorities in formulating a national judicial training strategy specifically for cybercrime and electronic evidence.

The Handbook outlines key considerations for national authorities during the process of conceptualising and preparing an effective national judicial training strategy, including identifying different roles, assigning responsibilities, conducting a needs assessment, drafting objectives, applying principles, creating an implementation plan, formulating metrics, procedures and timelines for evaluation, and guidelines for periodic review. It also provides guidance on the development of a curriculum and course material and its delivery.

While conscious about the different legal systems, traditions and cultures, the Handbook is intended to equip the national authorities with a valuable resource for developing or updating their national judicial training strategies on cybercrime and electronic evidence. It provides a means to design a more robust strategy to overcome challenges that are hindering a sustainable judicial training.

3 Distinguishing between a plan and a strategy

The distinction between a plan and a strategy is important to consider when conceiving a judicial training strategy on cybercrime and electronic evidence. This distinction is important as there is a tendency at the conception stage of judicial training strategies to gravitate towards formulating a plan as opposed to a strategy, which results in a more limited document.

A strategy is a broader, high-level approach that defines the "what" and "why" of an organisation's efforts. A strategy effectively provides a framework for decision-making and guiding long-term direction. In contrast, a plan is a detailed outline of actions and steps designed to achieve specific goals or objectives. The plan often specifies the "how" and "when" of execution. It focuses on the practical and tactical aspects of reaching a desired outcome and can be relatively short-term in nature.

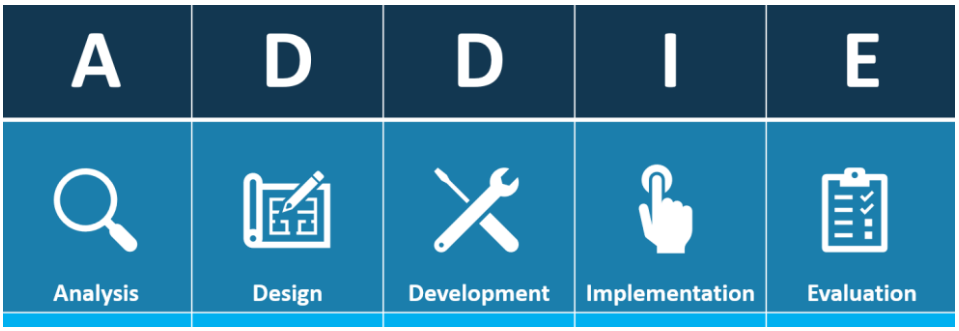
While a plan is a component of a strategy, the strategy encompasses a more comprehensive vision, including the allocation of resources, competitive positioning, and overall objectives, which inform the development of specific plans. For instance, the strategy provides for enabling the criminal justice authorities to prosecute and adjudicate cybercrime cases as specific objective, while a plan will outline to increase the pool of trainers available in a jurisdiction (action item that contributes to achieving that specific objective). This broader nature of a strategy should be kept in mind during the conception, design and development processes.

4 Approach to developing a judicial training strategy

Best practices from previously developed Council of Europe training programs [1] were considered when developing a new process flow for drafting an effective judicial training strategy. Therefore, an instructional design system (IDS) [2] known as the ADDIE method (stands for: Team, Analysis, Design, Development, Implementation, and Evaluation) was deliberately chosen and translated into a blueprint, six-step process flow to illustrate the development of a judicial training strategy on cybercrime and electronic evidence.

ADDIE model is a systematic instructional design system used to guide the development of training programs and educational materials. Each phase of the model represents a step in the process of creating a training course or curriculum, ensuring that it is well-structured, learner-centred, results-oriented and sustainable.

While ADDIE is a five-stage process that provides guidelines to identify, create and manage effective training course, the model is scalable and its methodology can be adapted to the introduction and evaluation when developing training strategies.



Given the crucial role of the entity or person analysing, designing, developing, implementing or evaluating in the ADDIE model, an additional Step zero was added to the reflect the various options on determining the entity, person, organisation, institution or working group that will take responsibility for taking the necessary steps within the framework of a judicial training strategy regarding cybercrime and electronic evidence training for judges and prosecutors. As such, the ADDIE model was adapted into the (T)ADDIE model to reflect the central role played by the team, largo sensu, who will prepare and monitor the training strategy. This is addressed in the next Chapter 4.1 on Step zero: Team.

The big advantage is that (T)ADDIE is a cyclic process that will return to the analysis phase to ensure continual improvement to the strategy. Especially in the digital world where everything is in constant flux, it is imperative that training for judges and prosecutors not only be installed in the magistracy's habitat, but that it be, if not continuously, at least periodically re-adjusted to meet current needs. This will help ensure sustainability.

Within the framework of the (T)ADDIE model, this guide proposes a stepwise guide for national authorities to formulate an agile, adaptable and effective national judicial training strategy on cybercrime and electronic evidence. These steps include:

---

[1] Guide For Developing Law Enforcement Training Strategies on Cybercrime And Electronic Evidence, Prepared by Cybercrime Programme Office of the Council of Europe (C-PROC) and INTERPOL Cybercrime Directorate, March 2022, p. 28

[2] An Instructional Design System (IDS) typically refers to a comprehensive framework or approach that guides the development and delivery of effective educational or training materials. It encompasses various methodologies, principles, and tools to create structured and engaging learning experiences. The main goal of an IDS is to enhance the learning process and optimize the transfer of knowledge and skills to the learners.

- Identifying and engaging relevant stakeholders (the TEAM)
- Assessment through landscape mapping, gap analysis and needs assessment (ANALYSIS)
- Applying principles and identifying objectives (DESIGN)
- Developing the strategy and the implementing plan (DEVELOPMENT)
- Implementation of the strategy (IMPLEMENTATION)
- Monitoring and review of the strategy (EVALUATION)

These steps only provide baseline guidance to formulating a judicial training strategy. National authorities may opt to include additional steps in the strategy development process depending on local needs.

4.1 Step 1: TEAM - Identifying and engaging stakeholders

The first step to developing a judicial training strategy is to identify and engage the relevant stakeholders that will be responsible at various stages of drafting and implementation of the strategy. It is not necessary for all stakeholders to be involved in every stage of the strategy as discussed further below. It is therefore essential to recognise the various stages of a judicial training strategy (for further details, please see above, Chapter 4 on Approach to developing a judicial training strategy) before assigning any responsibilities, as different stakeholders may be relevant at different stages and for different roles.

Once the different stages are identified, the next step is identifying which stakeholders are relevant to each stage. Examples of which stakeholders can be considered include:

- Relevant Ministers / Executive Authorities

- Judiciary
- Prosecution / Investigating Magistrates
- Law Enforcement
- Judicial Training Institute
- Already existing national trainers with experience on cybercrime and electronic evidence
- Judges and prosecutors (especially those working with specialized units or courts)
- Academia
- Civil Society
- Industry
- International Organisations

The list of relevant stakeholders will necessarily vary from country to country based on various criteria, including the division of responsibilities, available human capital, legal tradition and culture. For instance, in certain jurisdictions, it may not be considered appropriate for the executive authorities to be involved at any stage of the formulation, implementation and evaluation of the judicial training strategy, even with respect to budget allocations. Depending on the legal system, investigating magistrates or the prosecutor-general may be considered a relevant stakeholder. In some jurisdictions, it may also be relevant to involve military judges.

This identification process should be accompanied by a mapping exercise to determine which stages each stakeholder will be involved in and the roles they may be expected to play at different stages. This will depend on various factors including the availability of resources, the size of a country and the country-specific situation. For instance, it is possible that in a small country, all the identified stakeholders may be involved at each stage of the process and the exclusion of stakeholders may not be necessary. Conversely, it is equally possible in the same example of a smaller jurisdiction, the limited resources may not have sufficient time to be involved at each stage, which may form the basis for exclusion of certain stakeholders for certain stages.

Depending on the domestic context, which stakeholders have the legal mandate, legal powers, appropriate human resources and financial resources, from the very onset of a trai8ning strategy, consideration should be given to identifying the owner of the strategy at a policy level and the owner of the strategy at an implementation level.

It is also conceivable that different positions within each stakeholder group will be engaged at various stages. For instance, the heads of all relevant national authorities may participate in the conception of the judicial training strategy, where they agree on the main principles, goals and objectives. These high-ranking officials, including relevant Ministers, the Chief Justice, and heads of pertinent law enforcement agencies, may not need to be involved in subsequent stages such as drafting of the strategy and implementation of the plan.

As part of identifying and engaging the stakeholders, it is important to identify who will be the owner of a strategy both at a policy level and at a drafting and implementation level:

Owner of strategy at a policy level: At the policy level, the owner of the strategy could be a high-ranking official within the judiciary system, such as the Chief Justice, Prosecutor General, Head of the Cybercrime Unit in the Prosecutors' Office, the head of the Judicial Training Institute (if applicable), or a specialized committee/task force appointed to oversee the conception and development of the strategy. This is because decisions made at these stages require buy-in to secure the necessary approvals and budgetary and other resource allocations.

Owner of strategy at drafting and implementation level: At the drafting and implementation level, the owner will also depend on whether the country has an active judicial training institute or not. If a country has a judicial training institute, the relevant individuals at the judicial training institute will become an appropriate owner of

the strategy in terms of drafting and implementation, particularly if this institute may be primarily responsible for developing, planning and arranging the delivery of the judicial training materials. The question arises whether the presence of a judicial training institute is indispensable and a prerequisite for the development and implementation of cybercrime and electronic evidence training. If judicial training institutes are not present, consideration should be given to create them[3].

There are great differences between countries regarding the presence of judicial training institutes for judges and prosecutors; there are countries with:

- No judicial training institutes present;
- judicial training institutes for judges but not for prosecutors or vice versa;
- separate judicial training institutes both for judges and prosecutors;
- one judicial training institute where judges and prosecutors jointly are being trained.

Recognising the multitude of practices and institutional structures at national level, this Handbook attempts to offer alternatives for these differences, with the ultimate goal of having as final product, a national judicial training strategy on cybercrime and electronic evidence, practical and rooted in the national context.

4.1.1. Presence of (a) training institution(s)

To the extent that a judicial training institution exists, it is obviously recommended that the drafting and implementation of judicial training in cybercrime and electronic evidence takes place within this institutional framework, with the direct involvement of judges and prosecutors. Consideration should be given to involving all relevant units of the training institution/institute: initial training, continuous development etc.

In case of multiple training institutions or different training institutes for judges and prosecutors and to the extend that the legal tradition allows for judges and prosecutors to train together, both or all training institutions should be involved in the drafting and implementation of the strategy. The following should be considered:

- mapping the competences and mandate of each training institution, at what level are they organised, to whom (which silo) are they open for training and from whom do they receive the necessary funds. This is relevant to understand what roles can be allocated for each phase of the ADDIE model in the strategic development phase.
- mapping existing resources (funds and equipment). This topic will be further discussed under Chapter 4.2 on Analysis.
- allocating roles in the ADDIE model to all these institutions based on the mapping exercise

4.1.2. Absence of (a) training institution(s)

While the existence of a judicial training institute is a huge catalyst for the development of sustainable judicial training, and in particular training in cybercrime and electronic evidence, its absence - at least in an initial phase - is not an insurmountable obstacle to developing a cybercrime and electronic evidence training strategy and program for judges and prosecutors.

[3] This requires institutional effort and funding and it a matter larger than the topic of judicial training strategies on cybercrime, thus this topic is not tackled by this Handbook

Certain options exist that can (temporarily) compensate for the lack of a judicial training institute. Obviously, the judicial institutional training setup is directly correlated with the sustainability of the training: the lower the degree of a structured institutional framework (and funding), the lower the degree of sustainability of the training[4].

In absence of a judicial training strategy, in this step (i.e., identifying the owner of the drafting and implementation of the strategy) the following should be considered:

- existence of a training unit in the judiciary (or attached to supreme court) and similarly in the General Prosecutors' Office or Department of Public Prosecutions;
- the mandate of such units (and if such unit is competent to deal with the implementation of both initial and continuous training);
- available resources (financial and human resources).

Several options on how to deal with training in the absence of training institutions are presented in Annex 1.

4.2 Step 2: ANALYSIS - Landscape mapping, gap analysis and needs assessment

A strategy which is exclusively developed based on concepts and thoughts, and in isolation of data, may misidentify the gaps and needs of a particular legal system. Moreover, a plan developed on concepts and thoughts exclusively may face challenges in terms of implementation. It is therefore important to ensure that to a certain degree, the strategy and its conceptualisation is data-driven to. To ensure this, the owner of the strategy at policy level may consider, as part of the analysis process, landscape mapping, gap analysis and needs assessment exercise.

The individuals and institutions identified under Step 1 – Team should be expected to contribute to the collection of relevant data and information about the context and needs from various stakeholders before the strategy is prepared to map the current landscape, identify gaps and assess needs. One way to collect the relevant data is by preparing a questionnaire addressing the existing landscape, aims, objectives, constraints and challenges. These questions may need to be tailored to the national context with the aim of collecting as much information as possible about the current situation, constraints and challenges with respect to training on cybercrime and electronic evidence. The questionnaires for each stakeholder may also require customisation, as it may not be appropriate or relevant to ask certain questions from certain stakeholders.

While appropriate questions may vary from jurisdiction-to-jurisdiction accounting for national experiences, the following are some guiding factors which the drafting team may consider when preparing a questionnaire[5]:

4.2.1. Landscape mapping

The objective of this part of the questionnaire is to place / root the future training strategy in the already existing strategies or plans the country has and the national context and legal tradition:

[4] Training options that can be considered if an institutional, logistical and operational framework has not yet been created for judicial training of judges and prosecutors in the form of a judicial training institute are detailed under Chapter 5 on Development.

[5] The split between the three categories (landscape mapping, gap analysis and needs assessment) is intended only to structure the reading of this Handbook. In practice, there is no need to distinguish while drafting the questionnaire.

- What is the current position with respect to judicial training on cybercrime and electronic evidence? Are there any existing policies or strategies on related topics, such as cybercrime, cybersecurity or judicial training more generally?

- Is there any existing unit(s) which can be mandated to implement a judicial training strategy? Is there a need to establish a new unit or enhance the mandate of an existing unit?

- Is there any training strategy on cybercrime and electronic evidence for law enforcement? How does it impact the future judicial strategy?

- Who is the intended target of the judicial training on cybercrime and electronic evidence? What is the level of experience and trainings[6] of the identified actors to be targeted by the training strategy?

Are they strictly only judges and magistrates and prosecutors or does the scope extend to other participants in the criminal justice system, such as law enforcement officials, defence attorneys, forensic experts, court officers or others? This scope may depend on the national context, although generally judicial training strategies target judges, magistrates and prosecutors.

Best practices and experience from many cases in different countries have shown that in terms of the fight against cybercrime and the handling of electronic evidence, successful investigation, prosecution and trial is possible only when all parts of the chain in the system are equally well-trained. They are, after all, the necessarily interconnected links of the fight against cybercrime. Therefore, training targeting all actors in the criminal justice system should be considered.

- Are there any statistics available with respect to the number of actors (i.e., how many judges, magistrates and prosecutors would need to be targeted by training)?

- Are there prosecutorial units or courts specialised on cybercrime?

4.2.2. Gap analysis

The objective of this part of the questionnaire is to identify the existing conditions and the missing elements that need to be addressed in the strategy:

- What are the main challenges faced by criminal justice authorities with respect to the investigation, prosecution and adjudication of cybercrimes?

Not all the challenges that will be identified can be addressed by the training strategy. However, the drafters of the strategy should give proper consideration to all challenges, as they might affect the way the strategy will be designed. For example, it may be that the identified challenge is the absence of a specialized cybercrime unit at

[6] On cybercrime and electronic evidence

prosecutorial level or the shortage of judges / prosecutors. Even if these challenges will not be addressed in the development phase of the training strategy on cybercrime and electronic evidence, their impact on the overall strategy should be at least be noted for future revisions (please see Step 6. Evaluation).

- What are the main challenges currently being faced in relation to judicial training on cybercrime and electronic evidence? Are there any particular focus areas which have been identified?
- Who decides what topics will be included in the curricula? Is this done yearly and based on which criteria?
- What human, technical and financial resources are available for judicial training on cybercrime and electronic evidence? What is the source of these resources?
- Is there a pool of national trainers? If yes, what is the total pool available to deliver training on cybercrime and electronic evidence? Are these trainers part of a specialised training institute?
- To what extent is international technical assistance required for the drafting, implementation, and evaluation of the strategy?
- What steps can be taken to ensure that the strategy can be implemented in a sustainable manner?

4.2.3. Needs assessment

The objective of this part of the questionnaire is to identify the training needs (in terms of resources, actors, necessities etc), with the aim of structuring the design of the objectives of the strategy (for details please see Step 3. Design). The following questions can be considered:

- Is cybercrime and electronic evidence addressed in initial and continuous training for judges and prosecutors? Are these voluntary or mandatory?
- What topics are covered under judicial training on cybercrime and electronic evidence (both initial and continuous)?
- Are the topics the same for judges and prosecutors?
- Is there a structured modular approach to training: basic/introductory, advanced and specialized trainings?
- Are there any existing standardised training materials on cybercrime and electronic evidence?
- Has the (existing) pool of trainers received training on cybercrime and electronic evidence? What is the nature and level of training received? Have the trainers been trained in training skills?
- What mode of delivery is generally used to train judicial officials (i.e. online/hybrid)?
- What is the assessment model of training (passing score, mere finalisation of the course)?
- Is there any mandatory minimum training points / hours to be achieved each year by each judge/prosecutor?

In addition to these questions, it may prove useful to roll out a survey addressed to the final beneficiaries of the future strategy – the judges and the prosecutors. The aim of such exercise is to understand the perception of the needs directly from the targets of the strategy and integrate it /address the identified needs in the design and development phase. Such inclusive approach has the advantage of preparing the audience for the future strategy (announces the process of change).

4.3 Step 3: DESIGN – Applying the principles and setting the objectives

Once the landscape mapping, gap analysist and needs assessment is completed, the next step should be to begin a design of the strategy. Some areas in which challenges were outlined in the previous step (Analysis) may include financial resource constraints, technical expertise shortages, lack of standardisation, absence of facilities, outdated or ineffective training materials. These challenges will have to be factored in setting the objectives of the strategy and prioritize them.

4.3.1. Applying the principles

Principles are meant to be high-level statements that outline fundamental values that guide the overall development of the strategy and implementation of the plan. While the objectives contain specific, measurable targets or outcomes which the plan will seek to achieve, the principles guide how these objectives are set as well as the implementation plan towards achieving the objectives.

It is possible that a country may have principles with respect to judicial training which may also be equally applicable to judicial training on cybercrime and electronic evidence. In this case, the same principles may be restated directly into the strategy or with minor modifications wherever appropriate.

For countries which do not have general codified principles related to judicial training, there are several examples of judicial training principles that countries can consider and adapt based on their domestic needs and taking into consideration some unique considerations related to training related to cybercrime and electronic evidence. These include the Principles of Judicial Training on Cybercrime and Electronic Evidence which were devised during a meeting of several jurisdictions organised by the Council of Europe. These principles are briefly summarised in Annex 2.

There are also principles adopted by the European Judicial Training Network (EJTN) and the International Organisation for Judicial Training (IJOT) which are not specific to cybercrime and electronic evidence. The principles for a judicial training strategy on cybercrime and electronic evidence can draw upon these existing international practices. However, it is equally important to factor in some differentiating factors related to cybercrime and electronic evidence, particularly the extremely fast pace of technological developments which will necessitate a degree of agility and flexibility that may not necessarily be required for judicial training in other areas.

With respect to sustainability, there are several principles that authorities may consider incorporating into the strategy. For example, authorities should not focus on ad-hoc training but instead should focus on standardising training to ensure level-setting for all targets. Similarly, adequate trainers should be available for the training and sufficient resources should be made available.

Another important principle that should be considered in relation to sustainability should be to incentivise judges to become a trainer. This can be achieved in different ways through a more specific objective and clearly defined plan. Options may include considering the delivery of training as credits for promotion, preferred geographical

placements, providing opportunities to participate in trainings in other jurisdictions for cross-fertilisation, and other incentives to improve retention of trainers and to encourage other skilled individuals to join the pool of trainers.

4.3.2. Preliminary considerations before setting the objectives

With the view of setting the specific objectives, there are several additional considerations which may be relevant to factor. While some of these considerations seem more relevant to the preparation and delivery of the judicial training materials rather than formulating a judicial training strategy, they also present interest when formulating the strategy:

Who is the **intended target of the judicial training on cybercrime and electronic evidence**?

What is the **scope of the intended training on cybercrime and electronic evidence**? There is a misperception that training on cybercrime and electronic evidence is a specialised type of training, similar to training on subjects such as human trafficking or narcotics. It is therefore important for policymakers to understand and appreciate the foundational nature of basic training on cybercrime and electronic evidence and acknowledge that the needs of a country will be to cover all the targets (whether in-service or trainee).

Can the different targets of the judicial training on cybercrime and electronic evidence be trained together? There are legal cultures where both prosecutors and judges receive the same training from the beginning and are part of the magistracy that comprises both groups. These are countries where investigating magistrates and judges are considered to be equally part of the judiciary, but just in different roles. On the other hand, in other legal traditions, the judiciary does not want to train with prosecutors or investigators as this may be viewed as undermining the independence of the judiciary. Therefore, there are countervailing views with respect to how trainings should be organised which will ultimately depend on the local legal tradition.

How will learning needs be assessed prior to development or updating of training materials? For judicial training on cybercrime and electronic evidence to be effective, it is important to identify the specific learning needs and goals of the target audience. What skills, knowledge, and competencies do they need to acquire? Only when there is a good picture of who needs training on cybercrime and electronic evidence and when there is a good inventory of what is already available should any decisions with respect to training materials be made. It should be noted that these training needs will vary from target group to target group. One option is to conduct a Training Needs Assessment (TNA) – a systematic process of identifying gaps between desired and actual knowledge, skills, and competencies within a specific target group, which may be prosecutors and judges or even other actors in the criminal justice space. It also listens to the specific needs in the field of prosecutorial and court magistrates who handle cybercrime cases day after day. In the context of cybercrime and electronic evidence training, conducting a TNA is crucial to ensure that the training program effectively addresses the needs of the intended audience and provides relevant and impactful content. Certain functions come with certain cyber knowledge. Not everyone needs to know everything. What is certain is that a cybercrime baseline is necessary in any jurisdictional organisation. The mode of the TNA can vary depending on the national context, although surveys, interviews, focus groups and analysis of existing training materials. The TNA can also rely on any feedback received from trainers and participants from previous training sessions. All this information should be analysed to determine priority areas where training is most needed.

What learning objectives are being targeted? Based on the learning needs and goals identified, the implementing agency should create clear and measurable learning objectives for the judicial training being offered to the target audience. These objectives will guide the content development and assessment strategies in later phases. In jurisdictions where multiple training courses are being considered, the learning objectives will

necessarily vary. While all targets should receive a basic level of training on cybercrime and electronic evidence, policymakers may consider whether there is a need to also have tiered learning objectives, which are based on time, geography and specialisation. For example, it may be more relevant for targets who deal with proceeds of crime to receive more advanced training on virtual currencies, while such a training may not be as important for magistrates who hear cases pertaining to traditional crimes.

What are various strategic options for delivering the training to the various targets? There are several options available in terms of how to implement training. These options are not mutually exclusive and can all be considered as part of a modular delivery plan. Broadly speaking, the stakeholders responsible for organising trainings can either target a specific institution or organise trainings to which different trainings can be organised.

- **Targeting a specific institution:** If a specific institution is being targeted (such as, for example, the specialised agency for money laundering cases), there are again two options.
  - **Delivering trainings at the specific institution's location:** The first is for the trainers to deliver the training at the premises of the institution. It may be beneficial to conduct the training at the institution itself if the nature of the job would not allow an extended absence for the participants and such trainings are relatively easier to scale. However, such a training may have a more limited geographic reach.
  - **Organizing residential training for the specific institution:** the other is to organise a residential training which can be conducted off-site, where the participants will be required to reside. A residential training may be beneficial however as it would allow representatives of the institution based in different offices to work together. However, a residential training is relatively more expensive and may not be feasible where the targets cannot take an extended absence from their professional duties.
- **Calling different institutions to participate in a training:** Another option is to not target a specific institution in a training but to call multiple different institutions to a training organised externally. This may be organised at the premises of the institution responsible for organising the training, one of the participating institutions or may be a residential training which is conducted off-site, such as a hotel or other similar venue. The primary benefit of such a training is it allows different participants in the criminal justice system to be trained together, often allowing for cross-fertilisation of knowledge and networking. It is important however to ensure that the training being provided is appropriate and relevant for all the participants.

In addition to the above, a judicial training strategy must also consider **which modes of delivery should be considered when implementing the training aspects of the strategy**. For instance, it may consider where it is appropriate to have in-person trainings, hybrid trainings (where trainees may be gathered in a single location but trainers join remotely) or virtual trainings. Relevant considerations should include the pool of trainers, the size of a country, availability of required infrastructure, time and other resource constraints. The mode of delivery may also depend on type of training course, as certain courses will be significantly more effective when delivered in-person.

Is there a need to involve other expert training organisations? Regardless of whether training programs already exist at the national level, the supply of training at the international level is very extensive. Numerous supranational and international organisations and institutions focus on capacity building for law enforcement and the judiciary in matters of cybercrime and electronic evidence. There is a range of in-person, online or hybrid international training in cybercrime and electronic evidence, but also on related hot topics such as virtual assets,

blockchain technology, international cooperation, public-private cooperation, artificial intelligence, etc., in which judges and prosecutors from various corners of the world can participate. Depending on the funding of the respective courses, these are usually profitable in terms of cost.

Examples include:[7]

- Council of Europe projects
- Training programs of ERA (European Law Academy), based in Trier, Germany
- Training programs of the EJTN (European Judicial Training Network)
- Training programs of the OSCE (Organisation for Security and Co-operation in Europe)
- Training programs of the IAP (International Association of Prosecutors)
- Training given by Interpol or Europol
- Training facilitated and organised by Eurojust or by Eurojust projects, such as, for example, the WBCJ project (Western Balkan Criminal Justice Project)
- Trainings organised by the EJCN (European Judicial Cybercrime Network)
- Training organised by TAIEX (Technical Assistance and Information Exchange instrument of the European Commission)

Making efficient use of these existing training courses and training programs at the international level is highly recommended. Not only for countries or organisations that want to start creating a pool of national experts within their organisation, but also in terms of continuous training of already trained national trainers. After all, training in cybercrime and electronic evidence is never finished, but is a permanent task. Irrespective of outreach to international organisations, national authorities should continue to independently develop, assess and implement their strategies.

It is important that sustainability is considered when assessing whether outreach to international organisations is necessary. Any outreach and assistance sought from international organisations should be sustainable. For instance, collaborations should be used to build domestic capacity and to conduct training of trainers and evaluation of national trainers.

What are the different levels and types of training courses? The strategy should outline the approach for the development of the training materials to address the assessed needs. For instance, it should identify potential different levels of training courses, such as:

- introductory courses
- advanced courses
- specialised courses
- training of trainer courses
- training methodology/training skills courses

In addition to considering different levels, different types of training courses should be consider, such as:

- theory-based training
- case-based training
- mock hearing exercises
- technology-driven cases

Moreover, while a judicial training strategy need not identify specific training modules, considering subject areas, and how to create target specific training modules that will be most effective in delivery should be considered.

[7] The reference to Europe or European institutions does not necessarily imply that it is reserved for member states of Europe. Generally, training programs are also open to non-EU countries.

For example, authorities that deal with or consider mutual assistance requests may require more specialised training on international cooperation and related topics but such training may not be relevant for other criminal justice authorities who are not involved in that process. Similarly, it may not be efficient to teach advanced technical skills to criminal justice authorities. The strategy should therefore provide a degree of flexibility with respect to the contents of training materials, to ensure that the training is most effective.

What is an appropriate frequency of training? Another consideration when developing the strategy is the frequency of trainings and how frequently refreshers should be conducted. This should both address the frequency at which the responsible institutions organise trainings, as well as the frequency at which each target should receive training. This may require different considerations by the relevant authorities, including the size of the pool of trainers and trainees, financial resources, geographical factors and the nature of the training. To the extent possible, when drafting the strategy, the possibility of ensuring annual in-service basic refreshers for participants should be considered. This will not only ensure that the participants can refresh and update their knowledge (based upon any emerging trends and threats, technological developments and legal developments) but also provides a more effective post-training survey / feedback gathering opportunity to determine the effectiveness of the trainings in achieving the identified objectives.

4.3.3. Setting the specific objectives

After completion of the landscape mapping and needs assessment and in line with the formulated / existing principles, the authorities will be in a more informed position to begin drafting the strategy. The first step of designing a judicial training strategy on cybercrime and electronic evidence is to identify objectives.

It is important to have specific objectives as opposed to generic objectives, as all the parts of the strategy will be formulated with a view to achieving the objectives. All objectives must be based on a certain rationale which is linked to the needs, opportunities and challenges identified during the landscape mapping and the needs assessment.

The objectives should be formulated based on data and tailored to the specific national context. Although certain objectives may be the same across different jurisdictions, many objectives may only be appropriate in some countries. This variation may be due to different reasons including the level of resources and facilities, level of existing capacity, geographical factors, etc.

For example:

- an objective to introduce basic training on cybercrime and electronic evidence for all magistrates may not be necessary where magistrates already undergo basic training as part of their general magisterial training.
- an objective to establish a dedicated agency which is responsible for judicial training may not be appropriate for jurisdictions which already have a functional judicial training institute. For such jurisdictions, specific objectives can be formulated based on landscape mapping, needs assessment and challenges identified that would overall enhance the capacity of the existing judicial training institute.

Objectives can relate to various topics, including institutional reforms, enhancing the capacity and reach of training institutes, enhancing the size and capacity of the pool of trainers, developing training materials, mechanisms to evaluate the effectiveness of the training, etc.

With each objective, also, there will necessarily be certain assumptions which need to be considered. These assumptions are factors which are outside the control of the authorities responsible for achieving the objective. For instance, where a certain objective may require a budgetary allocation that can only be achieved through the Parliament, an assumption for that objective will be that Parliament will make the required allocation. Clearly defined assumptions will help ensure that the policymakers and implementers have foresight with respect to any impediments when it comes to implementing the policy.

Objectives should be accompanied by indicators. Indicators, in the context of objectives, are measurable variables or parameters that allow tracking progress toward achieving those objectives.

In order to be effective, the indicators should be **S**pecific, **M**easurable, **A**chievable, **R**elevant and **T**ime-Bound (SMART).

If we take the example of the objective of expanding the delivery of basic judicial training on cybercrime and electronic evidence to judges residing in five targeted rural areas, SMART indicators may include:

- Identifying two trainers in each targeted rural area within 4 weeks
- Identifying twelve target judges in each targeted rural area within 4 weeks
- Identifying a location for delivery of training in each jurisdiction within 4 weeks
- Allocating appropriate budget for delivery of training within 8 weeks
- Delivering the training in five targeted rural areas within 16 weeks
- Collecting feedback from trainers and target judges (completion) within 17 weeks

5 Step 4: DEVELOPMENT - Developing the implementation plan

As noted in Chapter 3 of this document, there is a tendency to conflate a strategy with a plan. It should always be remembered that a plan is a pillar of a strategy, but not the strategy itself. The purpose of the plan is to outline the specific actions and steps that relevant stakeholders are expected to take to achieve the objectives. Based on the principles, the plan is supposed to outline actionable, timebound, scoped and measurable items that must be implemented to achieve the objectives.

Each objective outlined may have one or more required outcomes. Each of these required outcomes will require a clearly defined plan, which should include clearly defined action items, associated timelines, resource requirements and sources.

The plan will necessarily depend on the objectives outlined in the strategy. For example, if one of the objectives is to constitute a dedicated agency which is responsible for judicial training, the plan should outline how this

objective will be achieved. These steps will necessarily vary from jurisdiction to jurisdiction but may potentially include:

- description of any legislation or other regulation that will need to be passed and the key elements which will be included in this legislation or other regulation (such as the form the agency will take).
- description of legislative plan, such as responsibilities for drafting and introducing the document in the legislature or other body and associated timelines.
- identification of the source of funding, resources and facilities for the establishment and operation of the agency and timeline for provision of funding, resources and facilities.
- identification of stakeholders responsible for managing the allocated resources
- identification of stakeholders responsible for oversight
- identification of the management and operational structure of the agency
- identification of the mandate and functions of the agency
- anticipated timelines for establishment of the agency

In addition to the above, a plan may also contain specific milestones or action items and metrics to measure completion or success. For instance, if one action is to introduce a legislation, associated action items may be the drafting of the legislation with certain minimum predefined criteria, introduction of the legislation in Parliament, passing of the legislation by Parliament, and then various aspects related to the implementation of the legislation.

Similarly, other objectives will also require associated plans. For instance, if there is an objective to train 100 judges living in predefined rural areas, the plan would need to address various aspects, such as how to select judges, which domestic and international agencies will be engaged, what the nature of the training will be, who will be responsible for formulating the training materials, what will the source of the budget be, as well as other aspects.

The plan can be outlined in narrative form, or alternatively, in matrix form, with specific action items specifically described. For illustrative purposes, if we take the objective of establishing a dedicated agency for training on cybercrime and electronic evidence, an indicative plan may look like the following:

Objective	Baseline	Indicators	Timeline	Responsibility	Budget Requirement	Budget Source
To establish a judicial training institute Assumption: The legislature will pass the law required to establish the institute.	There is no dedicated judicial training institute	Draft legislation which describes structures, functions, mandate, powers of dedicated agency and clear provisions regarding oversight, budget, etc.	[x]	Ministry of Justice Judiciary Prosecution	N/A	N/A
		Introduce draft legislation in legislature	[x]	Ministry of Justice	N/A	N/A
		Legislature to pass the legislation		Ministry of Justice		

		Appointment of management team of dedicated agency	[x] weeks after passing of legislation	Ministry of Justice	Necessary budget per year	National budget
		Procurement of office space for dedicated agency	[x]	Head of Dedicated Agency	Necessary budget per year	National budget
		Appointment of staff of dedicated agency	[x]	Management of Dedicated Agency	Necessary budget per year	National budget

Similarly, each indicator for each objective must be considered separately, as there must be a clear process for implementation. Indicators are the core of a judicial training strategy (of any strategy, in general) and will ultimately determine the effectiveness of the strategy, it is important that policymakers carefully consider and prepare the plan clearly in line with the needs and objectives identified.

6 Step 5: IMPLEMENTATION

After developing a strategy, the implementors take these action items and push them in the direction set out in the strategy to achieve its overall objectives.

Different stakeholders will be engaged as implementors, and various sub-groups may be formed to execute the required action.

Depending on the jurisdiction, one single institution could be appointed to oversee the strategy, or a committee of the key stakeholders could be created with this purpose. For further details, please see Chapter 4.1.

7 Step 6: EVALUATION - Review of the strategy

The strategy itself should be revised periodically, especially when it is found inefficient or unrealistic. The strategy team must regularly review the goals, objectives, and required actions were properly defined. This should be done on the basis of effective measuring of the results of implementation (Step 5) as well as structured reviews and evaluation (detailed in this section).

This review should be based on any learnings during the process of preparing the strategy and implementing the plan There are necessarily aspects of the strategy and its various components which will prove effective, while other aspects may not prove to be effective. It is possible that certain aspects of a strategy may be too idealistic, inappropriate, impractical or incorrect for a particular country. For instance, it is possible the strategy may initially have included a principle that judges and prosecutors should be trained together. However, after some experience in implementing the associated plans, it was noticed that due to the local legal tradition, judges were not willing to participate in a joint training with prosecutors, due to which the number of participating judges had declined. This may be addressed as part of the renew process. Another possibility is that the strategy initially suggested that all judicial training should be voluntary, but it was seen that the number of criminal justice professionals volunteering for the training was very low, which necessitates mandating at least a basic level of training.

The scope of the review should not only be limited to adapting from experience with the strategy itself. Rather, the strategy should also be reviewed to account for a change in external circumstances, which may necessitate

new needs, objectives, principles, and plans. For instance, in the event of a long-term pandemic, it is possible that a judicial training strategy which was focused primarily on the principle of conducting in-person judicial training on cybercrime and electronic evidence may need to be revised, and appropriate principles, objectives and plans related to e-learning may need to be incorporated. Likewise, if a country is facing new threats related to cybercrime, perhaps there may be a need to change the directional focus of the strategy to account for this. Over time, the availability and need for resources may also change, which may also require review.

The judicial training strategy should define which stakeholders are supposed to review the strategy, the frequency of reviews, the metrics for review, and all other relevant factors.

Ultimately, the review process will consider whether the indicators were met and more broadly whether the objectives were achieved. This may be based on metrics may include the following:

- **Effectiveness:** How effective has the judicial training strategy been in achieving each of its stated objectives? What changes are required to improve the effectiveness of the strategy? If the objectives have been clearly defined, the effectiveness of most objectives may be verified through concrete statistics.
- **Efficiency:** Is the training strategy cost-effective in terms of resource allocation and outcomes achieved? Are there any redundant or unnecessary components that could be streamlined or eliminated?
- **Relevance:** Does the training structure and content align with the specific criminal justice system architecture and the needs and challenges identified in the needs assessment? Does the training strategy allow for responsiveness to changes in technology, laws, regulations, and emerging legal issues?
- **Coherence:** Does the training strategy align with the broader goals and mission of the criminal justice system? Does the training strategy integrate well with other ongoing initiatives? Does the training strategy consider the interplay between various stakeholders and ensure their cooperation and coordination?
- **Sustainability:** To what extent have the capacity building efforts introduced pursuant to the strategy been made to ensure that the training institutes or other relevant stakeholders can sustain the training? How many national trainers has the training program successfully trained? How many training courses have these trainers delivered? To what extent have the trainings been rolled out to different regions? What level of reliance is there on international expertise?

The strategy should also identify the frequency of its assessment/evaluation. Although the frequency may vary depending on the duration of the strategy itself and upon domestic context, an annual review may be appropriate in most cases. However, it may also be appropriate to conduct ongoing monitoring of certain aspects of the strategy for which institutions which are responsible for implementation may be required to prepare and submit progress reports.

The strategy should also identify relevant institutions which will be responsible for evaluation of the strategy. These may match the stakeholders who initially drafted the policy or may also include other stakeholders who were responsible for implementation of the strategy. In addition, the specific responsibilities for these institutions may be identified in the evaluation process. For example, the authority responsible for organising the trainings may also be made responsible for the collection and provision of relevant data about the trainings it delivered and training-specific evaluations.

Annex 1 – Training structures in absence of a training institution

Options that can be considered if an institutional, logistical and operational framework has not yet been created for judicial training of judges and prosecutors in the form of a judicial training institute, include:

Option 1: Structured on-job-training (OJT)

On-the-job training is a way for professionals to learn work-related processes and knowledge by observing and performing tasks on the job. OJT focuses on integrating professionals into their daily (new) work environment (induction phase). Structured OJT is designed and delivered in a clearly defined, methodical manner. It usually includes a clear training agenda with tasks, instructions, and a timetable for completing the training. Each professional goes through the same training agenda and activities for a particular job. For a structured OJT to reach its envisaged impact, it should contain a monitoring and evaluating phase (including track record systems to account for the trained professionals). For further details on monitoring and evaluation, please see Step 5. Evaluation.

In terms of training in cybercrime and electronic evidence for judges and prosecutors, this implies that the OJT is developed and implemented by each institution (public prosecutor's office, prosecutor general's office, district court, appellate court, supreme court, etc) separately, in function of their specific needs. Obviously, different entities can also organise this jointly: for example, different (organisations within the) districts or jurisdictions can join hands and develop a joint OJT strategy, sending, exchanging or rotating "trainees" between various departments or mentors with a view to acquiring the appropriate specialised knowledge required by a well-defined (cyber) function.

Notwithstanding OJT certainly has its value (and is relatively inexpensive), it cannot be considered a stand-alone training tool or training strategy for the judiciary in matters of cybercrime and electronic evidence. Indeed, it requires that specialised trained colleagues already be available in the workplace, who must then be at least partially made available to supervise and train the colleagues to be trained. On top of that, the OJT may not be able to cope with the very high demand and the diverse and broad need to familiarise substantially a very large group of judges and prosecutors (in different levels according to specialisation and needs) with at least the basics of cybercrime and electronic evidence.

OJT can thus rather be considered a valuable component that can add value as part of a broader modular training strategy.

Option 2: In-house training

It has many similarities with the on-job-training (OJT). In-house training is training that is carried out internally within an organisation and is led by the organisation. You don’t outsource it to an external third-party training provider or hire a professional trainer. Everything is handled by existing in-house employees or trainers. It is cost efficient, however it requires that a certain level of expertise is already available within the organisation. In terms of training in cybercrime and electronic evidence for judges and prosecutors, the same considerations as made for the OJT come into play.

However, it is a very useful (complementary) method once a sufficient number of well-trained and knowledgeable trainers are present within the organisation. In that case, topical in-house training can be an absolute added value. Participation from various organisations can usually be organised relatively easily: for example, in-house training can be provided by the prosecutor's office of district X, inviting colleagues from districts Y and Z to participate in the organisation, supplying trainers/expertise and participants. This is also a very efficient method

for the judiciary in certain cases to cope with **a pressing need for training and expertise sharing on specific topics in a very short time with respect to a well-defined group**. For example, if it is experienced that many colleagues are confronted at a certain moment in an investigation with cryptocurrencies and virtual assets, then in-house training can be implemented and executed very efficiently in a very short time, where knowledgeable colleagues give a larger group of colleagues a good topical baseline in an in-house training setting. Obviously, this assumes and necessitates that a certain level of expertise already exists within the organisation so that it can be shared.

Option 3: Training outsourcing

Training outsourcing is the strategy for which an institution utilises an external supplier for the management of training processes and/or activities. Training outsourcing is the broader term, which includes multiple forms, or strategies, for utilising external resources.

A prerequisite - and disadvantage - is already that there is sufficient funding, since outsourcing judicial training is generally very costly to the extent that the outsourcing turns to specialised private consultancy. Evidently, outsourcing can also be considered in cooperation with academia or other government institutions capable of providing topical expertise for the benefit of judges and prosecutors. For example: training institutions of national investigative authorities (police academies, …) or intelligence services (State Security, Military Intelligence Services, …), CERTs, national cyber security institutions or organisations. The feasibility of such options depends largely on national legislation, customs and legal traditions (common law, civil law, hybrid). In addition to the institutional (un)feasibility, it should be noted that the outsourcing of training in cybercrime and electronic evidence for judges and prosecutors has the very significant disadvantage that, in principle, it is not given by trainers who are professional peers of the participants. It has been recognized that "*training in cybercrime should primarily be delivered by judges and prosecutors who have been previously trained for this purpose*"[8]. It should indeed be recognized that the specific professional challenges and questions of judges and prosecutors regarding cybercrime and electronic evidence are very concrete and manifest from day-to-day practice and confrontation with concrete issues in concrete cases. The answers to these concrete (legal) questions can hardly be outsourced and dealt with by organisations or trainers who do not or cannot have a thorough feel for the professional biotope of judges and prosecutors.

This is not to say that outsourcing cannot be part of a judicial training strategy. Well considered and well targeted outsourcing can certainly add value to the judiciary to import topical knowledge that is not (yet) available within the organisation. It has to be recognised that many of the topical issues are very often of a technical nature and also could be covered by LEA; it is therefore recommended to closely align and work together with the law enforcement community in order to provide the judiciary with topical technical expertise on the right level (e.g., block chain technology, virtual currencies, dark web investigations, malware technology, ransomware, …).

[8] GLACY+, "Principles of Judicial training on cybercrime and electronic evidence", Cebu, Philippines, 14 December 2017 (16 principles drawn from the Judicial Training Principles adopted by the European Judicial Training Network and from international best practices).

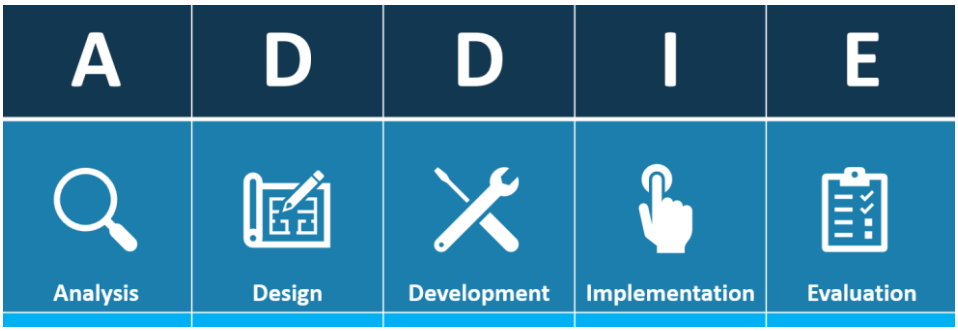
Annex 2 – Principles of Judicial Training on Cybercrime and Electronic Evidence

- Judicial training in cybercrime and electronic evidence is a multidisciplinary and practical type of training 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.
- Content and delivery of judicial training in cybercrime and electronic evidence are exclusively for national institutions responsible for judicial training to determine.
- Training materials 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.
- 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 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, which should have system of incentives.
- 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
- 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 is key to effectively tackle the cross-border nature of cybercrime and 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.

Annex 3 – (T)ADDIE Approach to developing judicial training materials

It is expected that judicial training strategies formulated by many countries will have the objective of either developing new training materials related to cybercrime and electronic evidence, or to update existing training materials to achieve the other objectives outlined in the strategy. The purpose of this document is to guide national authorities to formulate a national judicial training strategy on cybercrime or electronic evidence. It is not intended to serve as a guide to develop the training materials or to provide specific guidance with respect to training materials.

However, this document provides some guidance with respect to a sustainable approach to developing judicial training materials on cybercrime and electronic evidence. This approach will facilitate developing training materials which are effective in achieving the broader goals of the judicial training strategy.



Step Zero: Team

- Identify the team which will be responsible for the process to develop judicial training materials through the ADDIE process. This may include stakeholders, including any judicial training institute, representatives of judicial officials, prosecutors, law enforcement, academia, and other domestic and international experts.
- Assign specific responsibilities for the team constituents throughout the ADDIE process.

Step One: Analysis

- Identify the target audience for the training. Are they law enforcement professionals, legal experts, IT personnel, prosecutors and judges, or a mix of different roles?
- Determine the specific learning objectives. What skills, knowledge, and competencies do participants need to gain from the training?
- Conduct a needs assessment to identify gaps in current knowledge and skills related to cybercrime and electronic evidence handling.
- Identify any legal and ethical considerations that need to be addressed during the training.

Step Two: Design

- Create a detailed training plan that outlines the course structure, topics, and sequence of instruction.
- Develop the curriculum and content for the training. This may include modules on cybercrime types, digital forensics, evidence preservation, chain of custody, legal procedures, international collaboration, transborder access to data, crypto currencies, and more.
- Choose appropriate instructional strategies and methods, such as lectures, case studies, hands-on labs, simulations, and interactive activities such as mock trials.

- Design assessments and (online) quizzes that align with the learning objectives and measure participants' understanding.

Step Three: Development

- Develop the training materials based on the design phase. This includes creating presentations, lesson plans, handouts, interactive materials, videos, and any other resources needed.
- Build any necessary technological components, such as online learning platforms or virtual labs for hands-on practice.[9]
- Ensure that all content is accurate, up-to-date, and relevant to the training objectives.

Step Four: Implementation

- Deliver the training to the target audience. This could be done through in-person workshops, online courses, webinars, or a combination of methods.
- Monitor the training sessions to address any technical issues or participant questions.
- Encourage active participation and engagement from the participants to enhance the learning experience

Step Five: Evaluation

- Collect feedback from participants to gauge their satisfaction with the training content, delivery, and overall experience.
- Assess participants' performance against the learning objectives through post-training assessments or tests.
- Analyse the effectiveness of the training in closing the identified knowledge and skill gaps.
- Use the evaluation results to refine and improve future iterations of the training program, and use them as the beginning of analysis for future design.

[9] Such as the e-learning HELP online platforms from the Council of Europe https://help.elearning.ext.coe.int/