Cybercrime@EAP
Cooperation against cybercrime
In the Eastern Partnership region

GLACY
Global Action on Cybercrime
Action globale sur la cybercriminalité

Version 14 October 2014

Judicial training strategies on cybercrime and electronic evidence

Results of the GLACY and CyberCrime@EAP workshop held in Bucharest, 2-3 June 2014

www.coe.int/cybercrime

Funded by the European Union and the Council of Europe

EUROPEAN UNION

COUNCIL OF EUROPE
CONSEIL DE L'EUROPE

Implemented by the Council of Europe

Contents

1 Background

The projects Global Action on Cybercrime (GLACY) and CyberCrime@EAP are joint projects of the European Union and the Council of Europe aimed at supporting countries worldwide (GLACY) or in Eastern Europe (CyberCrime@EAP) in the implementation of the Budapest Convention.

Both projects comprise activities aimed at the training of judges and prosecutors on cybercrime and electronic evidence.

Given the threat of cybercrime and the increasing relevance of electronic evidence in criminal proceedings it is essential that eventually all judges and prosecutors have access to relevant training providing at least basic skills.

In 2009, therefore, the Council of Europe adopted a concept recommending that modules on cybercrime and electronic evidence be integrated ("mainstreamed") into the curricula of judicial training institutions. The concept has been tested successfully in South-eastern Europe and training materials (Basic course, advanced course, Electronic Evidence Guide) have been developed. The implementation of this concept is now supported through the CyberCrime@EAP and GLACY projects also in other regions.

On 2 and 3 June 2014, a workshop was held to this effect at the National Institute of Magistracy in Bucharest, Romania, in order to support the preparation of elements of judicial training strategies in GLACY priority countries (Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga) and countries participating in the Eastern Partnership (Armenia, Azerbaijan, Georgia and Moldova).[1] The opportunity was also used to promote judicial training in Romania, the host country of the workshop.

The present report summarises the results of the Bucharest workshop, including the elements of judicial training strategies prepared during the workshop. It will serve as a basis for further judicial training activities under GLACY and other projects.

Subject to the availability of resources, support under Council of Europe capacity building projects would include:

1. Engagement of judicial training institutions, including promotion of approaches or strategies on training on cybercrime and electronic evidence.[2]
2. Training of trainers (5-day course including 2 days of training skills and 3 days delivery of the standard basic course).
3. Adaptation of the materials developed by the Council of Europe to domestic needs or further improvement of other existing training materials in cooperation with trainers trained.
4. Support to trainers trained in the delivery of basis and advanced courses.
5. Support to training institutions to integrate such training into their regular curricula.

Guidelines for the delivery of judicial training courses on cybercrime and electronic evidence under projects implemented by the Council of Europe have been prepared.[3]

[1] Belarus and Ukraine also participate in CyberCrime@EAP but were not able to send representatives to this specific event.

[2] Through activities such as the workshop held in Bucharest on 2-3 June 2014.

[3] These Guidelines were prepared in September 2014, that is, following the workshop in Bucharest.

2 Elements of a judicial training strategy

During the workshop, representatives from each project area were requested to prepare elements of judicial strategies by addressing the following issues and questions:

2.1 Justification

This part should explain why a training strategy is necessary and why resources should be allocated.

> *What is the impact of technology on crime in your country? Please consider the impact as it relates to electronic evidence, cybercrime, traditional crimes that are impacted by technology. Identify specific crime areas that are impacted such as child protection, economic crime, people trafficking etc. What does this mean for the work of judges and prosecutors?*

2.2 Objective

The objective of a training strategy could typically address the following:

> *Who are the stakeholders in the judiciary that require "cybercrime" and electronic evidence training? Please identify the specific roles that you have identified e.g. generic prosecutor, specialised prosecutor, judge, judicial officer (please use descriptions that are used in your country). What is the expected result and intended impact of a training strategy?*

2.3 Training requirements (needs analysis)

This section should seek to break down the requirements for training as it relates to specific roles within the judiciary as part of an overall strategy.

> *Who needs to be provided with what skills? Please provide role specific key points that should be learned.*[4]

2.4 Training capabilities and resources

Training capabilities and resources required will differ between countries and even between courses within programmes. There are generic requirements; however each course training pack that is developed should contain a detailed list of all the resources required for each event. This will include details of classrooms, technology, trainers as well as specifics for each course delivery.

---

[4] *By way of example, the following are some of the considerations for first responders and are given as a guide to assist: Check the necessary authorisations; conduct preparatory research* concerning *the subject of the investigation; identify the appropriate tools to meet the needs of capture or seizure; recognise devices capable of storing electronic evidence; consider the volatility of data and its preservation; isolate the scene and secure the electronic evidence sources to prevent contamination and external interference; determine whether to capture electronic data or to seize electronic devices; keep a record of the state of the device and potentially relevant information in the immediate vicinity; choose and apply the appropriate power off method for the device; photograph and label the components of the device making specific reference to ancillary leads and connections to the device; appropriately package, seal and label the device in accordance with current procedures; capture and preserve electronic evidence in accordance with legal and organisational requirements; document the electronic evidence capture so that all actions can be reproduced by a competent third party; create a product of the data sources to a suitable medium.*

These requirements should be identified during the course development phase. The availability of trainers is another key consideration. It is often the case with countries developing their capacity to deal with cybercrime and electronic evidence, that they do not have an adequate number of trainers with suitable knowledge. It is essential that all potential resources be considered, such as academia and industry trainers, as well as international organisations and training resources.

Who will teach the students? Please identify whether there are sufficient trainers available in your country to implement a training strategy. Explain whether they will be from existing Judicial training centres, subject specialists from the police, academia or industry or a combination of these entities. If there are insufficient in-country trainers, please explain how your country will obtain trainers to assist in the delivery of training.

How will the training be delivered? Please explain what resources are available to implement the strategy. Identify the requirements for a cybercrime training centre; include technical resources as well as other logistical requirements. Also consider how industry and academia resources may be utilised in support of the strategy. Also consider which training may be delivered at regional as well as national level and in which languages. Please also consider issues of certification and academic accreditation.

2.5 Other considerations

There are a number of actions that may be included within the plans of all countries in the region.

2.6 Implementation of the strategy

It is important that each project area begins to prepare and adop national cybercrime training strategies at an early stage. It is essential that judicial training institutions take ownership and drive this process.

Each project area has begun to identify how this may be achieved, and this is dealt with in some detail in the sections below. The regional working group that is created under this project should begin to work together and should continue to do so during and after the project, to provide support, share information and assist in the development of compatible training in and between countries.

3 COUNTRY/AREA SPECIFIC STRATEGY OUTLINES

3.1 Armenia

3.1.1 Justification for training strategy

Despite the fact that the Criminal Code RA (CC RA) has a special chapter on Cybercrime (Chapter 24 – Crimes against computer information security), in most cases these crimes are committed in the economic sphere, especially for crimes against property. The relevant articles of Criminal Code of RA are the following:

- Theft committed by means of computer: Article 181 CC RA
- Legitimizing (legalizing) illegally obtained income: Article 190 CC RA

Chapter 24 CC RA
Crimes against computer information security

Article 251 Access (penetration) into computer information system without permission
1. Penetration into information stored in a computer system, network or on storage media, and part or the whole information system protected by law, without permission, committed with violation of the protection system and negligently caused change, copying, obliteration or isolation of information, or spoilage of computer equipment, computer system or other significant damage, is punished with a fine in the amount of 200 to 400 minimal salaries, or correctional labor for 6 months to 1 year, or with imprisonment for the term of up to 2 years.
2. The action,
1) committed with abuse of official position,
2) committed by a group with prior agreement,
3) which negligently caused grave consequences, is punished with a fine in the amount of 300 to 500 minimal salaries, or correctional labour for 1-2 years, or with arrest for the term of 1-3 months, or with imprisonment for the term of up to 5 years.

Article 252 Change in computer information
1. Change in information stored in a computer, computer system, network or on storage media, or entering obviously false information therein, in the absence of elements of property theft, or infliction of property damage by deception or abuse of confidence, which caused significant damage, is punished with a fine in the amount of 200 to 500 minimal salaries, or with correctional labor for the term of up to 1 year.
2. The same action which:
1) was accompanied with access (penetration) into a computer system or network without permission;
2) was committed by abuse of official position,
3) was committed by a group with prior agreement,
4) negligently caused grave consequences, is punished with a fine in the amount of 300 to 500 minimal salaries, or with correctional labor for the term of up to 2 years, or with arrest for the term of 1-3 months, or with imprisonment for the term of up to 2 years.

Article 253 Computer sabotage
1. Obliteration (sabotage) of computer data or software, isolation or making it unusable, spoilage of computer equipment or destruction of the computer system, network or on storage media, is punished with a fine in the amount of 300 to 500 minimal salaries, or with correctional labor for the term of up to 1 year, or with arrest for the term of 1-3, or with imprisonment for the term of up to 2 years.
2. The same action:
1) accompanied with access (penetration) into a computer system or network without permission;
2) negligently caused grave consequences, is punished with correctional labor for the term of up to 2 years, or with imprisonment for the term of up to 4 years.

3. The acts envisaged in part 1 or 2 of this Article which wilfully caused severe consequences, are punished with imprisonment for 3-6 years.

Article 254 Illegal appropriation of computer data

1. Copying or appropriating in any other way, of computer data stored in the computer system, network or on storage media, interception of transmitted data by means of computer communication, is punished with a fine in the amount of 200 to 400 minimal salaries, or correctional labour for the term of up to 1 year, or with arrest for the term of up to 2 months, or with imprisonment for the term of up to 2 years.
2. Forcing the submission of data mentioned in part 1 of this Article stored in the computer system, network or on storage media, by threat of publicizing defamatory information concerning a person or his close relatives, facts which the aggrieved wishes to keep secret, or with a threat to use violence against the person or his relatives, or against the person who manages this information, with a threat to destroy or damage the property, is punished with correctional labor for the term of up to 2 years, or with arrest for the term of 1-3, or with imprisonment for 2-5 years.
3. Actions envisaged in parts 1 or 2 of this Article which:
1) were accompanied with use of violence against the person or his close relatives;
2) were committed by a group with prior agreement;
3) inflicted significant damage to the aggrieved;
4) were committed with the purpose of obtaining particularly valuable information, are punished with imprisonment for the term of 4 to 10 years.
4. Actions envisaged in parts 1, 2 or 3 of this Article which:
1) were committed by an organized group;
2) were accompanied with infliction of damage to health or other grave consequences, are punished with imprisonment for the term of 6 to 12 years.

Article 255 Manufacture or sale of special devices for illegal penetration into a computer system or network

Manufacture of special hardware or software for the illegal penetration into a protected computer system or network for the purpose of sale, is punished with a fine in the amount of 300 to 500 minimal salaries, or correctional labor for the term of up to 1 year, or with arrest for the term of up to 2 months, or with imprisonment for the term of up to 2 years.

Article 256 Manufacture, use and dissemination of hazardous software

1. Development of computer software for the purpose of obliteration, isolation, changing of data stored in the computer system, network or on storage media, or for making changes in existing software, or developing software with special viruses, their use, or dissemination of storage media with such software, is punished with a fine in the amount of 300 to 500 minimal salaries, or correctional labour for the term of up to 1 year, or with arrest for the term of 1-3, or with imprisonment for the term of up to 2 years and a fine in the amount of 100 to 300 minimal salaries.
2. The same action,
1) Committed with mercenary motives,
2) Committed by a group with prior agreement,
3) which negligently caused grave consequences, is punished with imprisonment for the term of 2 to 5 years.

Article 257 Breach of rules for operation of a computer system or network

1. Breach of rules for operation of a computer system or network by the person who is entitled to enter this system or network, if this negligently caused obliteration, isolation, change in computer data, caused disruption in the work of computer equipment, or other significant damage, is punished with deprivation of the right to hold certain posts or practice certain activities for up to 5 years, or correctional labour for the term of up to 1 year.
2. The same action committed during the operation of a computer system or network containing particularly valuable data, is punished with imprisonment for the term of up to 2 years.

3. Actions envisaged in parts 1 or 2 of this Article which negligently caused grave consequences, are punished with imprisonment for the term of 2 to 5 years.

3.1.2 Objectives of the training strategy

The stakeholders in education are police officers (specialized employers), prosecutors (by a specialized department of General prosecutor office and one representative of the local prosecutors) and judges (on Criminal cases).

Prosecutor structure

The structure of the Staff consists of:
- The central body of the Staff,
- The territorial subdivisions of the Staff.

14. The subdivisions of the staff can be established for performing other functions of the Staff, stipulated by law.
15. The structure of the Staff is established by the Prosecutor General.
16. The central body of the staff consists of the structural subdivisions of the Staff. The residence of the Staff is the General Prosecutor's office of the Republic of Armenia.
17. The territorial subdivisions of the Staff are organized according to the procedure stipulated by the p. 8 of the RA law "On Prosecutor's office", excluding the General Prosecutor's office.

Number of Prosecutors - 365

Court structure

The court structure is regulated by the Constitution of RA and the Judicial code.
The following articles from the Judicial code of RA are relevant for the Court structure:

Article 3 The Courts
1. The highest judicial instance of the Republic of Armenia, with the exception of constitutional justice matters, is the Cassation Court of the Republic of Armenia (hereinafter, "the Cassation Court"), which is called to ensure the uniform application of law.
2. First instance and appellate courts shall also function in the Republic of Armenia.
3. The following are the first instance courts:
1) Courts of universal jurisdiction; and
2) Administrative court
4. The following are the appellate courts:
1) The criminal appellate court.
2) The civil appellate court; and
3) The administrative appellate court.
5. Administrative Court and the administrative appellate Court specialized courts.

Article 4 The Judge
1. A person appointed in accordance with the procedure defined by law to any of the positions of Cassation Court Chairman, Chamber Chairmen and judges, or first instance or appellate court judges or court chairmen is a judge.
2. Any judge is vested with the power to administer justice.

The number of Judges – 230

3.1.3 Training requirements (needs analysis)

Training is relevant for all stakeholders groups: officers, prosecutors and judges.

- For the police to effectively disclose and investigate these crimes.

- For prosecutors to effectively oversee the legality of the investigation and effectively defended the charge in court.
- For Judges to effectively implementation of justice.

3.1.4 Training capabilities and resources

Currently, for the prosecutors and judges, training programs on cybercrime investigation and defence charge in the court are developed. The students will be trained as specialist (expert) of the Scientific and Research department of the Justice Academy of the RA and computer expert of Justice Academy of RA.

In present, in the "Modern problems of criminal law" course for the candidates for the position of prosecutors and judges, there is a part entitled "Problems of qualification cybercrime" (2 academic hours).

For the preparation of the strategy and course of lectures, the Bucharest workshop training materials, experience of law enforcement of the RA and assistance to computer specialist will be used, as well as scientific papers, comments (Criminal code of RA) and international law enforcement experience.

All the training programmes are examined in the Scientific and Research Department of the Justice Academy.

3.1.5 Other considerations

Having in mind that cybercrime has a transnational nature, it is necessary to promote international cooperation in the fight against cybercrime, to provide common rules.

The development of guidelines for the implementation of prosecutorial supervision over the implementation of laws in the investigation of crimes in the sphere of computer information and defence charge in the court is also important.

The length of the training courses should not exceed 3 -5 days. As there are no specialized trainers in the country, there is the need to develop trainings of trainers and also country specific training materials.

3.2 Azerbaijan

3.2.1 Justification for training strategy

Rapid development of information technologies around the world, including Azerbaijan, leads to emergence of new types of problems and threats. Issue of Internet security becomes immediate with the growth of internet usage, as mankind's achievements in the field of information technology are not always used in good faith.

Taking into account the rising impact of modern Information Technology on crime and the specific areas where cybercrime are committed: Economic crimes, Fraud, Forgery, Traditional crimes, there is a specific need for judicial training to meet these challenges.

3.2.2 Objectives of the training strategy

Stakeholders:
- Prosecutors
- Judges
- Police investigators and operational staff
- Trainers of the Justice Academy (Ministry of Justice)
- Trainers of Science and Education Center (Prosecutor General's Office)
- Forensic experts

The above mentioned stakeholders should be trained according to their needs.

3.2.3 Training requirements (needs analysis)

In order to identify and obtain feedback from respective institutions and discuss all technical issues related to the training process, a study visit to Baku is strongly recommended. In this respect representatives from each stakeholder should be consulted and their needs assessed.

3.2.4 Training capabilities and resources

The training of trainers programme would be useful for further retraining of the prosecutors and judges, as there is an insufficient number of local trainers.

Moreover, the visit to Baku would enable the experts to identify the needs that need to be covered during training programmes.

3.2.5 Other considerations

The training courses should include examples and concrete criminal cases and how the investigation was conducted, information regarding the general criminal case, from the beginning to the end of the case.

The Training Strategy should include how to organize the training courses in an effective manner and also how to integrate the training courses in the curricula of the training centres.

The public institutions responsible for the training of judges and prosecutors are the Justice Academy and the Science and Education Centre (only for prosecutors). These institutions should be able to make the training part of their training curricula.

3.3 Georgia

3.3.1 Justification for training strategy

Technology increases the number of crimes time to time in Georgia. Issues which are related to the crime committed by the technology are digital evidence, cybercrime (whether or not it should be considered as evidence), cybercrime as well as traditional crimes such as bribery, murder, etc. Electronic evidence seized from the mobile operators is of a great importance in terms of specifying the route of offender.

Specific areas of the crime are especially economic crimes such as theft, fraud. There is also increased number of crimes such as thieving money from other people's bank account by using their name and personal information. There are also evidences of taking money from the bank accounts by using false credit cards.

The issue of cybercrime and cyber security became crucially important after 2008 war as there have been mass cyber-attacks on government and nongovernment internet resources.

3.3.2 Objectives of the training strategy

The stakeholders in the judiciary field that require "cybercrime" and digital evidence training are: judges, assistant judges and other court personal, prosecutors and police investigators.

Due to the fact that judges are dealing with various cases in the courts, it is crucially important for them to have knowledge of issues related the cybercrime. It is worth pointing out that judges in Georgia are very interested in cybercrime issues and as a result of their request the High School of Justice (HSoJ) has already scheduled to conduct a workshop on cybercrime in June, 2014.

According to the fact that investigation of cybercrime is conducted by the Ministry of Internal Affairs, it is important for police investigators to have basic skills of investigating cybercrime and gathering evidences. Apart from this, there is no prosecutor specialized in cybercrime and therefore they need to acquire basic skills related to cybercrime. It will be helpful to establish special unit of prosecutors, which will be in charge of conducting investigation of cybercrime.

3.3.3 Training requirements (needs analysis)

Due to the novelty of cybercrime judges and prosecutors need to be familiar with various aspects of cybercrime to acquire practical skills and knowledge in terms of investigating and dealing with the cybercrime. Therefore all the above mentioned key points would be useful to be learned.

3.3.4 Training capabilities and resources

Trainings for students of the High School of Justice (the only institution providing trainings for judicial candidates, judges, judges' assistants and other court personal) are conducted only by sitting judges who have proper knowledge and can share best experiences with the students. In order for the School to provide trainings on cybercrime, it is important the curriculum to be developed with the involvement of foreign expert (which at the same time should be a judge) as there are not sufficient trainers available in Georgia. The curriculum should be developed in cooperation with Georgian experts, who will be trainers of the School. It will be useful also to provide study visits for Georgian experts involved in the process of developing the curriculum in order to share the best practice and consider it respectively. The next step is conducting ToT for experts involved in creating curriculum and after they acquire sufficient knowledge of what to teach and how to teach the School will be able to provide trainings for judicial candidates as well as siting judges and other court personal.

Trainings for prosecutors are provided by the Training Centre of Ministry of Justice, however they also have not got sufficient trainers and therefore there is a need of involving international experts in order to train prosecutors and police investigators. After training of small pool of prosecutors they will be able to conduct local trainings.

Recourses available:

The High School of Justice: the School has premises for conducting training which is well equipped, including technical equipment. Therefore, after developing curriculum and ToT the School can provide trainings for candidate judges, sitting judges and other court personal. However the School does not have relevant software program which is needed for learning specific issues related to the cybercrime.

The same applies to the Training Center of the Ministry of Justice.

3.3.5 Other considerations

The Georgian representatives expressed their need that the Council of Europe would provide foreign experts (consultants) who will be involved in the process of developing curriculum on cybercrime and also to organize study visits for the Georgian expert to share the best practice and get involved in Training of Trainers.

Providing materials and guidelines already prepared on the cybercrime issues will be useful.

3.4 Mauritius

3.4.1 Justification for training strategy

The fast economic and social development of Mauritius during the past decade has alongside brought a rapid development in the IT sector. ICT is important and essential to the economic development of Mauritius. Its negative impact is unfortunately potentially considerable. This negative impact is not limited to the economic sector but can have far reaching social consequences. The negative economic impact refers to economic crimes, unlawful data interference, while the negative social impact raises issues as Harassment, child pornography, obscenity, defamatory statements.

3.4.2 Objectives of the training strategy

The Institute for Judicial and Legal Studies (IJLS) has a wide mandate under The Institute for Judicial and Legal Studies Act 2011. It has the statutory mandate to deliver training to all the stakeholders in the administration of justice. Of note, it also provides Continuing Professional Development (CPD) to all law practitioners.

As at present, the IJLS has not delivered any training on Cybercrime and Digital Evidence. This is not because it does not realize the importance of same. It had started to enlist the assistance of the French Ecole de la Magistrature but had put on hold the project when it was made aware of the Glacy Project.

All the stakeholders in the administration of criminal justice need training ie police prosecutors, state prosecutors from the Office of the Director of Public Prosecutions and judges. The Institute also plans to include courses on cybercrime and electronic evidence in its CPD programme to law practitioners.

3.4.3 Training requirements (needs analysis)

At this initial stage which ideally should last for 12 months, an introductory course on cybercrime and electronic evidence for the stakeholders in the administration of criminal justice as identified above is necessary.

Before considering more advanced training, all the stakeholders should be familiarized with the nature and evidential value of electronic evidence.

3.4.4 Training capabilities and resources

A TOT Programme is called for at this stage. A small contingent of trainers must be identified and constituted (e.g. 16 participants) from the police prosecutors, state prosecutors, law practitioners and judges. This contingent must be constituted as quickly as possible. A polite request is now made to the Council of Europe for assistance to deliver the first TOT training to this first contingent if possible before the end of the year.

Ideally, this first contingent will deliver its first training by beginning of December 2014. The Institute will also prospect for relevant local resource persons and faculties. Thus a team of judges can be constituted to prepare a paper on the evidential value of electronic evidence. The Institute has also research assistants and will soon be put on the preparation of this paper, which will be a useful training tool.

The IJLS has the physical space and logistics to deliver the training. The major difficulty is to find the initial team of trainers and provide training for them. The IJLS has already links with countries

in the region Reunion Island and the Seychelles. The IJLS welcomes cooperation with its regional neighbours.

3.4.5 Other considerations

The collection of electronic evidence is very important. For the training of the prosecutors and judges to be meaningful, it is important that this aspect should be taken in the national strategy development.

Training in cybercrime and electronic evidence should also develop into mainstream training and should become part of the curriculum of the training of lawyers and judges.

3.5 Moldova

3.5.1 Justification for training strategy

Information technology affects different aspects of the crime spectrum and national legislation Moldavian distinguish between computer enabled crimes and computer dependent crime and therefore traditional crimes committed with the use of information technology will be dealt properly if the judiciary and law enforcement will be trained to understand the role played by the technology in the commission of a crime.

There is a large variety of crimes with which the prosecutors and judges are confronting. The specific steps that need to be undertaken are:

- identifying the specific needs and targets
- development of different training materials considering the initial training and the continuous training
- to adopt by the Council the introduction in the general curriculum for initial training for judges and prosecutors for following topics
- substantive law – cybercrime, trends and modus operandi
- procedural law and theory on electronic evidence
- forensic in computer crime / the role of the expert in the trial/the object f the expertise
- investigative methodologies on different type of cybercrime (intrusions, botnet etc.)
- international cooperation under the CCC
  - for continuous training
  - basic - with the possibility to upgrade the level of information disseminated
  - on the same topics
- collection of best practices in courts (case studies)

3.5.2 Objectives of the training strategy

In Moldova, there are no specialized courts, no specialized investigative prosecutors; however specialized unit within GPO for policy reasons, specialized police units ongoing process.

In conclusion, training is needed at all levels even though there is some knowledge (the existing courses in place).

3.5.3 Training requirements (needs analysis)

The information is specific to law enforcement powers and procedure however the prosecutor is the leader of the investigation either supervising the investigation either being involved directly and therefore such information is needed.

There is a need to implement specific basic knowledge for all parties of the judiciary system and to pursue on continuous training for advanced skills.

Securing evidence is crucial for the prosecution and proper working methodologies are needed to be disseminated throughout the judiciary. Knowing and following procedures make the evidence legal, predictable, traceable, reliable, completed etc. These are considered working methods.

Special investigative powers are considered important and critical in obtaining evidence. The legal and the technical aspects of such proceedings are either important (real time data collection, real time traffic data collection, computer searches seizure, computer data analysis, other type of expertise on viruses, programming etc.)

However, the investigation methodology is also considered important:

- where to find the evidence and how to obtain it in different practical cybercrime cases
- how to investigate a botnet, an intrusion etc.
- how to correctly bring charges and sustain charges with the proper evidence package
- what it is to be proven in different types of crime
- collection of case studies, working books
- glossary of terms, definitions, common understanding

Dedicated guides for specific aspects of investigating methodology are to be considered (e. g. securing physical evidence, gathering, preservation and examination of evidence).

3.5.4 Training capabilities and resources

The present state of facts is that there is a lack of trainers for both initial and continuous training. The current lack of trainers could be covered by common database of available trainers and their specific domains (e.g. IT knowledge, comparative law, international cooperation).

A way to get more trainers is to train the trainers, to recruit practitioners and train them to teach where possible. Practitioners have to be encouraged to train and to disseminate knowledge.

Besides the identified need for trainings of internal trainers, the possibility of using external trainers was stressed out. We are exploring the possibility to attract academia and private sector into the training programs.

There are training rooms within the National Institutes equipped with computers and technology specific for training. Even tough, existing logistics are still to be urgently upgraded and adapted for studying specific methods of cybercrime investigation.

Now it is difficult to identify the practical needs in terms of how many computers, technical features etc. E-leaning is to be considered.

Identifying resources form academia and private sector that can be involved in judiciary training is to be explored at least for very specific areas such as programming, virus analysis or else. Complex teaching team consisting in technicians and legal practitioner needs to be considered.

Exchanges with other dedicated centres (institutes of magistracy or similar institutions for judicial training) from abroad are important.

3.5.5 Other considerations

There is the need for the Council of Europe to assist Moldova in promoting the training strategy and also to assist Moldova in the preparation of the training materials and TOTs.

3.6 Morocco

3.6.1 Justification for training strategy

Le Maroc subit à l'instar des autres pays des attaques de criminalité numérique. Ce grave fléau touche à titre d'exemple : Vol de la propriété intellectuelle et artistique, usurpation d'identité, atteinte à la vie privée, manipulation d'images pour publication dans les réseaux sociaux, problèmes de pédophilographie (des étranger qui s'installent au Maroc pendant leur vacances et créent des banques d'images mettant en avant des relations sexuelle avec des enfants mineurs), paralysie des systèmes d'information et des réseaux d'information de certains organismes Publics, infiltration dans des boites E-mail privées. Telles sont les principales infractions constatées à travers l'utilisation illicite de la nouvelle technologie en informatique.

3.6.2 Objectives of the training strategy

L'objectif, c'est d'assurer une formation spécifique destinée à des Magistrats en matière de la cybercriminalité et de la preuve électronique.

L'Institut Supérieur de la Magistrature Marocain a parmi ses missions, la réalisation de la Formation Initiale des futurs Magistrats et la Formation Continue des Magistrats en fonction.
S'agissant de la Formation Initiale, Elle dure 24 mois avec alternance cours à l'Institut et stages effectués dans les différents tribunaux. Le thème de la cybercriminalité est enseigné dans le cadre du module du Droit Pénal avec un cours d'une durée de trois heures uniquement. Il n'existe pas, à ce jour, un **module consacré exclusivement à la cybercriminalité**.

Quant à la Formation Continue et Spécialisée, elle s'articule autour : des Sessions d'Etudes, des Séminaires et des Stages au Maroc et à l'Etranger. Dans ce cadre, il est proposé la formation d'un groupe de Magistrats-Formateurs sur la criminalité électronique et ce, par l'actualisation et le renforcement de leur savoir-faire pour devenir «*Magistrats Référents*» capables d'assurer à leur tour des cours académiques en matière de la cybercriminalité soit au profit des futurs magistrats en cours de formation à l'Institut ou au profit des magistrats en fonction dans les Tribunaux.

3.6.3 Training requirements (needs analysis)

Les attentes en matière de formation sur la criminalité électronique, c'est d'abord et dans un premier temps d'atteindre la réalisation d'une formation de base qui englobe les éléments suivants :

- La nature des menaces liées aux réseaux numériques.
- Les dispositifs juridiques de lutte contre la cybercriminalité.
- Les techniques d'investigations numériques et les procédures d'établissement de la preuve.
- Les questions et les réponses juridiques à mettre en place ainsi que la jurisprudence dans ce domaine qu'elle soit nationale ou internationale.

3.6.4 Training capabilities and resources

Les futurs Formateurs Magistrats doivent être sélectionnés parmi les magistrats du parquet et les juges d'instruction disposant d'une expérience en matière pénale, d'un fond juridique et d'un savoir-faire, et leur faire bénéficier d'une **Formation Technique** qui consiste dans un premier stade à des cours d'initiation de base donnés par des compétences locales ou par des compétences étrangères.

Dans un 2ème stade ou niveau avancé, ils auront besoin des compétences extérieurs afin d'assurer des cours sur les menaces les plus sophistiquées. Ces cours avancés peuvent nécessiter du matériel et des logiciels importants.

Parallèlement à cette formation technique un contenu juridique s'avère indispensable par la citation d'un certain nombre de procès réels avec tous les aspects juridiques qui l'entourent.

Le contenu de la formation juridique nécessite que se soit au niveau 1 ou niveau 2, la formation sur la problématique juridique. Le conseil de l'Europe est sollicité à aider l'Institut à l'élaboration d'un plan de formation avec un contenu bien défini, et aussi par le savoir des experts en matière de cybercriminalité et de la preuve électronique. et ce, en vue de former un nombre de « Magistrats Référents » qui prendront la relève en assurant la formation des magistrats tant qu'au niveau central qu'au niveau régional, ainsi et dans le cadre de la coopération, nous serions amenés à délivrer des formations au profit des pays de la région qui la sollicitent.

Nous souhaitons aussi lancer un programme de certification qui garantira la qualité de la formation délivrée, et qui permet d'avoir un réseau d'experts nationaux formés selon les standards internationaux. Cette certification peut être préparée avec la participation du Conseil de l'Europe.

3.6.5 Other considerations

On s'inspirant des documents du Conseil de l'Europe et en s'appuyant sur l'expérience et l'expertise de ses Spécialistes, on peut dans un futur proche, étudier les modalités de la mise en place d'une première formation après avoir déterminer :

- La durée,
- La catégorie ciblée.
- La disponibilité des magistrats (fréquence).

Certaines matières seront assurées par des intervenants locaux, d'autres seront assurées par des experts proposés par le conseil de l'Europe ; le programme sera finalisé et validé.

Enfin L'Institut est conscient de l'ampleur et de la gravité de ce phénomène qu'est la cybercriminalité ; ce fléau qui ne cesse inlassablement de faire des ravages à tous les niveaux, économique, social et autres, du fait qu'il se distingue par sa rapidité, son anonymat et son inter matérialité.

L'aide du conseil de l'Europe est vivement sollicitée.

English version

Justification for training strategy

Morocco, like other countries, suffers from digital crime attacks. A few examples of these serious acts are: flight of the intellectual and artistic property, identity theft, invasion of privacy, manipulation of images for publication in social networks, pédophilographie problems (visitors in Morocco during their vacation that create image banks highlighting the sexual relations with minors), paralysis of information systems and information networks of some Public bodies, infiltration boxes E-mail private. These are the main infringements through the illegal use of new technology in IT.

Objectives of the training strategy

The objective is to provide specific training for Magistrates on cybercrime and electronic evidence.

The Moroccan Higher Institute of the Judiciary has among its missions, the completion of the Initial Training for future Judges and Magistrates of the Continuing Education office. Regarding Initial Formation, the training lasts 24 months with alternating the Institute training and internships in various courts. The issue of cybercrime is taught in the module with a Criminal Law courses lasting only three hours. There is not, to date, a **module devoted exclusively to cybercrime.**

As for continuing and specialized education, it revolves around: Study Sessions, Seminars and Workshops in Morocco and abroad. In this context, it is proposed the establishment of a group of trained judges on e-crime and, by updating and strengthening their skills to become "Magistrates Referrers" capable of ensuring in turn academic courses on Cybercrime is the benefit of future judges in training at the Institute or for the benefit of judges of the Courts.

Training requirements (needs analysis)

The first expectation is for training on electronic crime are also to achieve the realization of basic training which includes the following elements:

- The nature related to network threats;
- The legal devices against cybercrime;
- The digital investigative techniques and procedures for establishing proof;
- Questions and answers to legal set up and the case law in this area, whether national or international.

Training capabilities and resources

Les futurs Formateurs Magistrats doivent être sélectionnés parmi les magistrats du parquet et les
The future trainers for judges must be selected from prosecutors and judges with experience in criminal matters, with legal background and know-how, and to benefit from a training technique that involves in a first stage in introductory courses basic skills taught by local or foreign jurisdiction.

In a second stage or the advanced stage, they will need outside expertise to provide courses on the most sophisticated threats. These advanced courses may require significant hardware and software.
Alongside this technical training legal content is essential by mentioning a number of real trial with all legal aspects that surround it.

The content of legal education requires whether at Level 1 or Level 2 training on legal issues. The Council of Europe has sought to help the Institute to develop a training plan with a well-defined

content, and also the knowledge of experts on cybercrime and electronic evidence. and in order to form a number of "Referrers Magistrates' who will take over providing training for judges as at central level or at regional level and within the framework of cooperation, we would have to deliver training to countries in the region who seek.

We would also launch a certification program that will ensure the quality of training provided, which allows a network of national experts trained according to international standards. This certification can be prepared with the participation of the Council of Europe.

Other considerations

Based on the documents and materials provided by the Council of Europe and based on the experience and expertise of its specialists, we can in the near future, consider the introduction of a first training, after have determined the following:

- The duration;
- Targeted category;
- The availability of magistrates (frequency).

Some materials will be provided by local stakeholders, others will be provided by experts proposed by the Council of Europe; the program will be finalized and validated.

Finally, the Institute is aware of the magnitude and severity of this phenomenon of cybercrime; this scourge that continues tirelessly to wreak havoc at all levels, economic, social and other, because it is characterized by its speed, anonymity and inter materiality.

The assistance of the Council of Europe is highly solicited.

3.7 Philippines

3.7.1 Justification for training strategy

The widespread use of Information Communication Technology (ICT) systems in commerce, trade and practically most other day to day private and public transactions has also brought along its pervasive abuse and misuse (cybercrime).

Areas affected by cybercrime cover electronic commercial and non-commercial transactions, issuance and use of access devices, photo and video voyeurism, child pornography, trafficking in persons especially women and children, privacy of communications, intellectual and property rights, individual personal information in ICT systems in both government and private sector.

3.7.2 Objectives of the training strategy

The essential elements in the criminal justice system that will need cybercrime and digital evidence training would be those in law enforcement (police and criminal investigators, to include those in customs, immigration and quarantine), prosecution, and those in the judiciary.

In the judiciary, the critical elements would be the:

- Judges of the 2nd level courts (Regional Trial Courts Judges) because jurisdiction over cybercrimes are by law lodged in them;
- Branch Clerks of Court (BCOCs) of the 2nd level courts because they closely assist the RTC judges in the performance of their judicial and administrative duties.

Not so critical elements in the judiciary that may also need focused exposure on the subject would be:

- Justices of the national appellate court which is the Court of Appeals as well as justices of the special collegiate trial courts which are the Sandiganbayan (Anti-Graft Court) and Court of Tax Appeals;
- Court Attorneys assigned to the Justices.

In the prosecution, the critical elements would be the:

- State, Regional, Provincial and City Prosecutors and their Assistants, all of the Department of Justice (DOJ);
- Ombudsman Investigators and Special Prosecutors, both of the Office of the Ombudsman.

Note: By specific provision of the recently enacted cybercrime law (RA 10175), there shall be designated special cybercrime courts to be manned by specially trained judges to handle cybercrime cases.

3.7.3 Training requirements (needs analysis)

RTCJs need to be exposed to the speedily evolving environment of ICT systems, the special field of cybercrime; the new law and allied statutes; the Budapest convention on cybercrime and its subsequent guidelines. They also need to get better acquainted with the rules on electronic evidence.

BCOCs must likewise be trained on the same subjects and additionally on the storage and safekeeping of all pieces of evidence concerning cybercrime cases that are formally turned over to the courts.

Prosecutors need training on the same subjects, as above. They also need to undergo the kind of training given to law enforcers and police investigators on the technical aspects of cybercrime

detection, investigation and interdiction; marking, handling and preservation of evidence with emphasis on the chain of evidence custody principle. Such an exposure to ground level police anti-cybercrime work will better equip them with the know-how of prosecuting a cyber-offense.

Specific law enforcement groups should be targeted and given special training on the subject with the end-in-view of developing a pool of training specialists on the technical aspect of police anti-cybercrime work.

3.7.4 Training capabilities and resources

The Philippine Judicial Academy (PHILJA), which is a specialized entity under the Supreme Court tasked with the training of judges and lawyers desirous of being appointed to the bench, is in a position to handle and implement a training strategy that will expose RTCJs and BCOCs to cybercrime and electronic evidence. As a matter of fact, PHILJA has recently commenced in 2013, a three-day seminar amongst RTCJs in the countryside (in batches of 35 to 40 judges per Region) on the very subject of cybercrime and electronic evidence. About four such 3-day seminars have been conducted with the assistance of either USAID or the US DOJ-OPDAT (US Department of Justice, Overseas Prosecutorial Development and Training). The training has been carried out with specialists on the sub-topics outlined in the seminar who come from the academia, the NBI (National Bureau of Investigation, Cybercrime Unit) and from the PHILJA's Corps of Professors.

The sufficiency of specialists-trainers on the very technical aspects of cybercrime detection and investigation may be an issue as specialists on the matter who can be trainers may be in short supply. There are quite a number of specialists, but whether or not they can be trainers is another matter. Perhaps, this is an area where PHILJA may have to coordinate with the National Bureau of Investigation of the DOJ and the Criminal Investigation and Detection Group of the Philippine National Police – DILG, to inventory their specialists who can act as trainers. This is also an area where foreign assistance may be considered.

There are at least three options by which cybercrime and electronic evidence training may be delivered in the Judiciary:

First. PHILJA can continue with its Regional approach in conducting 3-day seminars until it is able to cover all the RTCJs in the regions. This option will be resource-guzzling and will certainly take a long period considering the total number of RTCJs (bet. 800 & 900).

Second. PHILJA can marshal its resources and resume the special training after the special cybercrime RTCs have been designated. It is estimated that the total number will not exceed 100. Focusing the training on these specially designated branches of the RTCs will be economical.

Third. PHILJA can mainstream cybercrime and electronic evidence training via incorporation of an appropriate module in the regular Pre-Judicature Training Program (PJTP), Orientation Seminar-Workshop for Newly Appointed Judges, as well as in the periodic Regional Judicial Career Enhancement Program (RJCEP).

As a training institution established initially via Supreme Court resolution in 1996 and later by law, in 1998, PHILJA has acquired sufficient expertise in the conduct of training programs as may be required by developments in the legal environment. It can package an appropriate training program and hold it in its training centre situated in the suburbs of Metropolitan Manila. Thus, facilities-wise, carrying out a training activity will not be a problem. It can also assemble the necessary team of instructors/trainers who can handle the actual training. It is in the area of financial logistics that PHILJA is somewhat handicapped.

As a matter of protocol, all training activities are documented and culminate with the issuance of an appropriate certificate to those who satisfactorily complete the training program. Thus far, no diploma program on the very specialized filed of cybercrime is available from any academic

institution in the country. In the College of Law of the University of the Philippines, cybercrime and electronic evidence are treated merely as ordinary components of the much larger field of criminal law, criminal procedure and evidence.

In the case of the National Prosecution Service of the DOJ and the Ombudsman Investigators and Special Prosecutors of the Office of the Ombudsman, training of their prosecutors and personnel can be handled by PHILJA via an appropriate agreement in the meantime that neither one has an adjunct training arm.

With respect to the matter of training specialized groups of law enforcement agencies under either the DOJ (e.g. NBI, BID, etc.) or the DILG (e.g. PNP CIDG, etc.) , any training, for purposes of standardization, economic use of resources and mutual cooperation, may be undertaken through PHILJA. Financial logistics, standardized training materials will be imperatives in this activity as PHILJA's annual budget does not sufficiently account for non-judicial training activities.

3.7.5 Other considerations

On top of the PHILJA, another national training institution that is equipped to carry out area-wide training is the Institute of Judicial Administration (IJA), which is a component of the much larger University of the Philippines Law Center (UPLC), an entity embedded in the state university. IJA, an academic entity, however, now has greatly reduced functions in view of PHILJA. It is still available as a vehicle for delivering legal training, although now limited to the conduct of mandatory continuing legal education (MCLE) for lawyers in general.

In the area of maximizing use of resources from an international perspective, the Philippines through PHILJA can be the regional centre for delivering internationally assisted training programs on cybercrime, ICT systems and electronic evidence.

3.8 Senegal

3.8.1 Justification for training strategy

L'impact de la technologie sur la criminalité est une réalité au Sénégal. Plusieurs cas de jurisprudence ont été relevés ces dernières années au niveau des juridictions.

Le Contentieux récurrent porte essentiellement sur les procédures relatives a l'accès et au maintien frauduleux a un système informatique, l'interception de données liées au transfert d'argent, conversions de communications internationales en communications locales portant atteinte aux opérateurs, escroquerie de type ingénierie sociale pour soustraction de fonds, fishing, la suppression de données informatiques d'ex employés, violation des données personnelles atteinte a la vie privée, a l'image, infiltration de boîtes email etc.

Une décision du tribunal des flagrants délits de Dakar du 18 septembre 2009 constitue une des premières applications de la loi sénégalaise du 25 janvier 2008 portant sur la cybercriminalité. Dans cette espèce, les juges ont qualifié d'accès frauduleux à un système informatique, le fait pour un collaborateur d'une société spécialisée dans la vente et la distribution de pneumatiques, d'accéder sans autorisation aux données de l'ordinateur du directeur commercial de ladite société.

Dans une autre affaire dite « *Fulgence BAHI* » jugée par la deuxième chambre correctionnelle du tribunal régional Hors Classe de Dakar le 21 janvier 2010, le tribunal a condamné une personne pour le délit prévu par l'article 431-8 du Code pénal pour avoir fait usage d'une carte de paiement falsifié et effectué frauduleusement des achats dans les terminaux de paiement électronique (TPE) de la Société Générale de Banques au Sénégal (SGBS) installés dans une bijouterie. Le jugement d'instance a été confirmé sur ce point par un arrêt de la chambre correctionnelle de la Cour d'Appel de Dakar du 13 décembre 2010.

Dans une troisième affaire, « *Kouakou KOUADIO »,* le tribunal régional Hors Classe de Dakar a le 2 mai 2012 condamné, Kouakou KOUADIO qui a effectué un paiement à une boutique sise à un centre commercial pour y acquérir des films, une console de jeu et un jeu vidéo avec une fausse carte de crédit qu'il a déclaré avoir acquis en Russie via internet.

Très récemment, la première chambre correctionnelle du tribunal régional hors classe de Dakar a rejeté la prévention d'accès frauduleux à un système en tirant argument de la qualité d'associés des prévenus qui disposaient légalement de code d'accès au site au même titre que le plaignant .Le simple fait de modifier le code d'accès du site ne consomme pas le délit d'accès frauduleux à un système.

Cette nouvelle forme de délinquance transnationale de par sa technicité, sa complexité, sa volatilité, son développement fulgurant a nécessité un encadrement textuel spécifique tant au plan national qu'international.

The impact of technology on crime is a reality in Senegal. Several court cases have been identified in recent years in the courts.

Recurring litigation focuses on the procedures relating to access and to maintaining a fraudulent computer system, interception of data related to money transfers, conversions international communications affecting the local communications operators, engineering-type scam, subtracting social fund, fishing, suppressing computer data of ex-employees, violation of personal data breach and privacy, of pictures, infiltration of mailboxes etc.

A court decision flagrante delicto in Dakar on 18 September 2009 was one of the first applications of the Senegalese law of 25 January 2008 on cybercrime. In this case, the judges described as unauthorized access to a computer system, the fact that an employee of a company specializing in

the sale and distribution of tires, gained unauthorized access to computer data Trade Manager of the company.

In another case called "Fulgence BAHI" judged by the second Criminal Chamber of the Regional Court of Dakar Out January 21, 2010, the court sentenced a person for the offense provided for in Article 431-8 of the Penal Code for making use of a payment card forged and fraudulently made purchases in electronic payment terminals (TPE) Societe Generale de Banques au Senegal (SGBS) installed in a jewelry shop. Instance judgment was confirmed on this point by a judgment of the Criminal Chamber of the Court of Appeal of Dakar 13 December 2010.

In a third case, "Kouakou KOUADIO", Hors Classe Regional Court of Dakar on 2 May 2012 sentenced Kouakou KOUADIO who has made a payment to a store located in a shopping center to acquire films, a game console and a video game with a fake credit card he said he had acquired in Russia via internet.

Very recently, the first Criminal Chamber of the Regional Court of Dakar Officer rejected the prevention of unauthorized access to a system by pulling argument of quality associated defendants legally had access code to the site as well as the complainant. By simply changing the access code of the site does not mean an offense under unauthorized access to a system.

This new form of transnational crime by its technical expertise, its complexity, volatility, its rapid development has required a specific text frame both nationally and internationally.

3.8.2 Objectives of the training strategy

Du point de vue des cibles, trois catégories de personnels sollicitent la formation au plan judiciaire:

- les futurs formateurs;
- les magistrats;
- le personnel d'appui.

Ils seront sélectionnés pour la formation initiale auprès des auditeurs de justice et des élèves greffiers et en formation continue auprès des magistrats et des greffiers des juridictions en fonction de leur profil et de leur motivation.

Pour les magistrats, on peut retenir trois niveaux en fonction des profils :
- niveau 1 : Sessions destinées à tous les magistrats de la chaîne pénale au niveau de la première instance (instruction, parquet de la république et siège) et au niveau des cours d'appel (parquet général, chambres correctionnelles et chambres d'accusation des cours d'appel) . L'organisation de la formation se fera au sein du Centre de formation judiciaire (CFJ), ou à distance.
- niveau 2 : sessions destinées a tous les membres du dispositif (magistrats du pool anti criminalité organisée et points focaux des TGI et des chambres criminelles représentant toutes les fonctions (instruction, parquet et siège) ; organisation au sein du CFJ en présentiel et a distance.
- niveau 3 : magistrats de la future section de lutte contre la cybercriminalité du pool- anti criminalité organisée dans toutes les fonctions (instruction, parquet et siège), une formation juridique et technique très avancée et une mise à niveau permanente.

Pour le personnel d'appui (les greffiers):

- Niveau vulgarisation: appropriation du dispositif national et international,
- formalisation des procédures (dimension nationale et internationale) suivi et gestion des procédures

From the point of view of the target, three categories of staff seeking training in the courts:

- Future trainers;

- Magistrates;
- Support staff.

They will be selected for the initial training for trainee judges and clerks and students training to judges and court clerks according to their profile and their motivation.

For judges, it can be three levels based on profiles:
- Level 1: Sessions for all judges of the criminal justice system at the trial (investigation, prosecutor of the republic and seat) and at the courts of appeal (Prosecutor General, Corrections rooms, and charges of courts of appeal). The organization of the training will be in the Judicial Training Centre (JTC), or remotely.
- Level 2: sessions for all members of the device (magistrates organized and focal points of TGI and criminal chambers representing all functions (education, flooring and seat) anti crime pool; organization within the CFJ-face and distance.
- Level 3: Judges of the future section of the fight against cybercrime pool anti-organized crime in all functions (education, flooring and seat), a very advanced legal and technical training and continuous upgrading.

For support staff (clerks)
- Level extension: ownership of national and international device,
- Formalization of procedures (national and international dimension) monitoring and management procedures

3.8.3 Training requirements (needs analysis)

Le contenu de la formation des formateurs et des magistrats portera sur:
- une formation sur la compréhension des menaces liées au réseau informatique ;
- les techniques de collecte, d'analyse de préservation et de présentation des preuves électroniques ;
- les dispositifs juridiques mis en place au plan national, régional et international.

Pour les formateurs, ils bénéficieront d'une formation en pédagogie.

The content of the training of trainers and judges will include:
- Training on understanding the threats related to computer network;
- Techniques for collecting, analysing preservation and presentation of electronic evidence;
- Legal arrangements put in place at national, regional and international levels.

For trainers, they should receive training in pedagogy.

3.8.4 Training capabilities and resources

Les ressources existantes au Sénégal sont très limites : les formateurs seront choisis dans deux domaines spécifiques.

Les formateurs en droit :
On peut identifier parmi les formateurs existants :
- un magistrat spécialisé : Dr Pape Assane Toure
- un lieutenant de police : Pape Gueye

Ils seront complétés par les formateurs de la chaîne pénale du Centre de formation judiciaire: les formateurs en Instruction, au Parquet et au siège correctionnel

Les formateurs au plan technique :

Cette formation technique qui portera sur une initiation de base sera assurés par des ingénieurs de l'Agence de l'Informatique de l'Etat (ADIE).

Le Sénégal aura besoin de l'appui de ressources humaines internationales notamment en Formation technique avancée. Il aura besoin d'un appui logistique et pédagogique notamment pour l'acquisition de logiciels et d'applications.

La formation sera délivrée a court terme dans le cadre de la formation continue et à moyen terme dans le cadre de la formation initiale.

- En formation continue : Elle sera modulée à trois niveaux ci-dessus visés.
- En formation initiale: il sera procédé a l'introduction dans le curriculum de formation des magistrats du module cybercriminalité (cours trimestriel). La cybercriminalité pourra être choisie comme dominante.

A cet effet l'intéressé respectera :
la proposition de sujet de mémoire sur la thématique le stage pratique auprès des services d'enquête de la police (brigade de lutte contre la cybercriminalité) et des autres structures impliquées telle que la commission des données personnelles, la section spécialisée du pool anti criminalité organisée.

Existing resources in Senegal are very limited: trainers will be selected in two specific areas.

Trainers in law that can be identified from existing trainers:
- A specialized judge: Dr. Pape Assane Toure
- A police lieutenant: Pape Gueye

They will be complemented by the trainers of the criminal chain Judicial Training Centre: trainers in Education, Prosecution and Correctional center.

Trainers on the technical area: This technical training will cover a basic introduction will be provided by engineers Information Technology State Agency (ADIE).

Senegal will need the support of international human resources including Advanced Technical Training. There will be also needed logistical and pedagogical support for the acquisition of software and applications.

The training will be delivered in the short term as part of the continuous training and in the medium term as part of the initial training.
- Continuous education: It will be modulated at three levels mentioned above.
- Initial training, there shall be an introduction into the curriculum of the training of judges cybercrime module (quarterly progress). Cybercrime can be chosen as dominant.

For the interested person observed:
- The proposed dissertation topic on the theme
- The practical training for both police investigation services (the brigade on fighting cybercrime) and other structures involved such as the commission of personal data, the Section of organized crime anti pool.

3.8.5 Other considerations

Pour la mise en œuvre de la Stratégie nationale de formation, il convient de tenir compte du dispositif envisagé:

Au plan national:

Une section de lutte contre la cybercriminalité sera créée au sein du pool anti criminalité organisée à compétence nationale basée à Dakar

Des points focaux régionaux seront désignés et formés au niveau de chaque TGI dans les trois différentes fonctions (instruction, parquet et siège) au niveau des trois ressorts des cours d'appel.

La mise en place d'une plateforme interdisciplinaire pour favoriser la coordination entre enquêteurs, poursuivants et juges le tout sous la coordination du Centre. National de Cyber sécurité

Au plan régional:

- En raison de sa position stratégique et son rayonnement régional, il sera important de constituer le CFJ Centre de formation judiciaire, en Centre régional (ouest africain) de cybercriminalité.

- Pour développer la coopération régionale en matière de formation judiciaire, il pourra être utilisé les leviers existants:
- Réseau Africain Francophone de Formation judiciaire (10 pays)
- École régionale supérieure de la magistrature (en droit des affaires: droit pénal des affaires)

DEMANDE APPUI INSTITUTIONNEL DU CONSEIL DE L'EUROPE

- Appui à l'élaboration d'un programme de formation adapte et la mise a disposition des outils pédagogiques (a court terme dans 6 mois)

- Appui a la formation des formateurs en cybercriminalité et en gestion des preuves électroniques (a court terme dans les 6 mois)

- Appui a l'organisation des sessions de restitutions à l'intention des magistrats, des greffiers, des OPJ, des avocats et des membres de la commission nationale des données personnelles; (moyen terme)

NB : démarrage de la formation initiale (a la prochaine promotion)

- Appui à l'érection du CFJ en Centre régional d'excellence en cybercriminalité;

- Appui à l'organisation de sessions régionales de renforcement capacités des chefs d'institut de formation, des formateurs des écoles et acteurs judiciaires de terrain (information, formation et spécialisation) ; délivrance de certification professionnelle.

- Appui au développement et à la formation aux outils de coopération internationale;

- Appui à la mise en place d'une plateforme régionale de renforcement des capacités des acteurs de la chaîne de prévention, de détection, d'investigation et de poursuite (la chaîne pénale -enquêteurs (officiers de police judiciaire OPJ- police gendarmerie-; magistrats (procureurs et juges)

- Appui à la collecte et à la publication de la jurisprudence nationale et régionale;

- Appui a la mise en place d'une certification puis d'un Master en cybercriminalité en relation entre le CFJ et les universités de Dakar et St. Louis.

- Appui pour le suivi du projet.

The implementation of the National Strategy training should reflect the proposed scheme:

At the National level:

A section of the fight against cybercrime will be created in the organized crime anti pool with national jurisdiction based in Dakar

Regional focal points will be designated and trained at each TGI in three different functions (Education, Public Prosecutors department and seat) at three courts of appeal.

The establishment of an interdisciplinary platform should be created, to promote coordination between investigators, prosecutors and judges all under the coordination of the National Centre on Cyber Security.

At the regional level:

Due to its strategic position and its regional influence, it will be important to establish the CFJ Judicial Training Centre, a regional center on cybercrime (West Africa).

To develop regional cooperation in judicial training, it can be used existing levers:
- Francophone African Network of Judicial Training (10 countries)
- Regional High School for the Judiciary (Business Law: Criminal Business Law)

REQUEST INSTITUTIONAL SUPPORT OF THE COUNCIL OF EUROPE

- Support the development of a adapted training program and make available educational tools (short term 6 months)

- Support for the training of trainers in cybercrime and electronic evidence management (short term 6 months)

- Support the organization of meetings for the re-establishment for judges, clerks, OPJ, lawyers and members of the National Commission of personal data; (Medium term)

NB: Starting initial training (at the next generation)

- Support for the creation of CFJ in regional Centre of Excellence in cybercrime;

- Support for the organization of regional capacity building sessions leaders training institute, trainers schools and judicial operators (information, training and specialization); issuance of professional certification.

- Support for the development and training tools for international cooperation;

- Support for the establishment of a regional platform for capacity building of actors in the chain of prevention, detection, investigation and prosecution (criminal investigators-chain (judicial police officers OPJ-Police-gendarmerie; magistrates (prosecutors and judges)

- Support for the collection and publication of national and regional jurisprudence;

- Support for the establishment of a certification and a Master of cybercrime relationship between CFJ and Universities of Dakar and St. Louis.

- Support for project monitoring

English version

Justification for training strategy

The impact of technology on crime is a reality in Senegal. Several court cases have been identified in recent years in the courts.

Recurring litigation focuses on the procedures relating to access and to maintaining a fraudulent computer system, interception of data related to money transfers, conversions international communications affecting the local communications operators, engineering-type scam, subtracting social fund, fishing, suppressing computer data of ex-employees, violation of personal data breach and privacy, of pictures, infiltration of mailboxes etc.

A court decision flagrante delicto in Dakar on 18 September 2009 was one of the first applications of the Senegalese law of 25 January 2008 on cybercrime. In this case, the judges described as unauthorized access to a computer system, the fact that an employee of a company specializing in the sale and distribution of tires, gained unauthorized access to computer data Trade Manager of the company.

In another case called "Fulgence BAHI" judged by the second Criminal Chamber of the Regional Court of Dakar Out January 21, 2010, the court sentenced a person for the offense provided for in Article 431-8 of the Penal Code for making use of a payment card forged and fraudulently made purchases in electronic payment terminals (TPE) Societe Generale de Banques au Senegal (SGBS) installed in a jewelry shop. Instance judgment was confirmed on this point by a judgment of the Criminal Chamber of the Court of Appeal of Dakar 13 December 2010.

In a third case, "Kouakou KOUADIO", Hors Classe Regional Court of Dakar on 2 May 2012 sentenced Kouakou KOUADIO who has made a payment to a store located in a shopping center to acquire films, a game console and a video game with a fake credit card he said he had acquired in Russia via internet.

Very recently, the first Criminal Chamber of the Regional Court of Dakar Officer rejected the prevention of unauthorized access to a system by pulling argument of quality associated defendants legally had access code to the site as well as the complainant. By simply changing the access code of the site does not mean an offense under unauthorized access to a system.

This new form of transnational crime by its technical expertise, its complexity, volatility, its rapid development has required a specific text frame both nationally and internationally.

Objectives of the training strategy

From the point of view of the target, three categories of staff seeking training in the courts:
- Future trainers;
- Magistrates;
- Support staff.

They will be selected for the initial training for trainee judges and clerks and students training to judges and court clerks according to their profile and their motivation.

For judges, it can be three levels based on profiles:
- Level 1: Sessions for all judges of the criminal justice system at the trial (investigation, prosecutor of the republic and seat) and at the courts of appeal (Prosecutor General, Corrections rooms, and charges of courts of appeal). The organization of the training will be in the Judicial Training Centre (JTC), or remotely.

- Level 2: sessions for all members of the device (magistrates organized and focal points of TGI and criminal chambers representing all functions (education, flooring and seat) anti crime pool; organization within the CFJ-face and distance.
- Level 3: Judges of the future section of the fight against cybercrime pool anti-organized crime in all functions (education, flooring and seat), a very advanced legal and technical training and continuous upgrading.

For support staff (clerks)
- Level extension: ownership of national and international device,
- Formalization of procedures (national and international dimension) monitoring and management procedures

Training requirements (needs analysis)

The content of the training of trainers and judges will include:
- Training on understanding the threats related to computer network;
- Techniques for collecting, analysing preservation and presentation of electronic evidence;
- Legal arrangements put in place at national, regional and international levels.

For trainers, they should receive training in pedagogy.

Training capabilities and resources

Existing resources in Senegal are very limited: trainers will be selected in two specific areas.

Trainers in law that can be identified from existing trainers:
- A specialized judge: Dr. Pape Assane Toure
- A police lieutenant: Pape Gueye

They will be complemented by the trainers of the criminal chain Judicial Training Centre: trainers in Education, Prosecution and Correctional center.

Trainers on the technical area: This technical training will cover a basic introduction will be provided by engineers Information Technology State Agency (ADIE).

Senegal will need the support of international human resources including Advanced Technical Training. There will be also needed logistical and pedagogical support for the acquisition of software and applications.

The training will be delivered in the short term as part of the continuous training and in the medium term as part of the initial training.
- Continuous education: It will be modulated at three levels mentioned above.
- Initial training, there shall be an introduction into the curriculum of the training of judges cybercrime module (quarterly progress). Cybercrime can be chosen as dominant.

For the interested person observed:
- The proposed dissertation topic on the theme
- The practical training for both police investigation services (the brigade on fighting cybercrime) and other structures involved such as the commission of personal data, the Section of organized crime anti pool.

Other considerations

The implementation of the National Strategy training should reflect the proposed scheme:

At the National level:

A section of the fight against cybercrime will be created in the organized crime anti pool with national jurisdiction based in Dakar

Regional focal points will be designated and trained at each TGI in three different functions (Education, Public Prosecutors department and seat) at three courts of appeal.

The establishment of an interdisciplinary platform should be created, to promote coordination between investigators, prosecutors and judges all under the coordination of the National Centre on Cyber Security.

At the regional level:

Due to its strategic position and its regional influence, it will be important to establish the CFJ Judicial Training Centre, a regional center on cybercrime (West Africa).

To develop regional cooperation in judicial training, it can be used existing levers:
- Francophone African Network of Judicial Training (10 countries)
- Regional High School for the Judiciary (Business Law: Criminal Business Law)

REQUEST INSTITUTIONAL SUPPORT OF THE COUNCIL OF EUROPE

- Support the development of a adapted training program and make available educational tools (short term 6 months)
- Support for the training of trainers in cybercrime and electronic evidence management (short term 6 months)
- Support the organization of meetings for the re-establishment for judges, clerks, OPJ, lawyers and members of the National Commission of personal data; (Medium term)

NB: Starting initial training (at the next generation)

- Support for the creation of CFJ in regional Centre of Excellence in cybercrime;
- Support for the organization of regional capacity building sessions leaders training institute, trainers schools and judicial operators (information, training and specialization); issuance of professional certification.
- Support for the development and training tools for international cooperation;
- Support for the establishment of a regional platform for capacity building of actors in the chain of prevention, detection, investigation and prosecution (criminal investigators-chain (judicial police officers OPJ-Police-gendarmerie; magistrates (prosecutors and judges)
- Support for the collection and publication of national and regional jurisprudence;
- Support for the establishment of a certification and a Master of cybercrime relationship between CFJ and Universities of Dakar and St. Louis.
- Support for project monitoring

3.9 South Africa

3.9.1 Justification for training strategy

South Africa is a signatory to the Budapest Convention on Cybercrime.

Cybercrime has an impact economically, socially and politically, as well as on security and human rights. The actual and potential risks associated with cybercrimes justify training of all judicial officers in order to ensure that they have the necessary skills, knowledge and understanding to adjudicate these offences.

Since cybercrime encompasses a variety of offences including those involving attacks against computer data and systems as well as offences that are committed by means of computer systems, such as forgery, fraud, theft, child pornography, Intellectual Property Right – offences etc. SA has a high number of sexual offences which include cybercrimes such as child pornography, sex tourism and cyber grooming. SA has a high rate of serious violent and organized crimes and in most instances technology plays a role in the commission of the offences and/or solving thereof.

Judicial officers in dealing with cybercrimes need to have a basic understanding of the electrical and digital means used to commit the offences and have to understand the terminology used and the concepts related thereto. For example, if the fraud was committed through phishing or skimming, the judicial officer needs to know what the act is this term is referring to.

Electronic and digital evidence can and is presented increasingly in all courts and can be present in any kind of offence. In order to be able to adjudicate on the admissibility of the evidence as well as to evaluate and adjudicate this evidence, a basic understanding of the technology and terminology is necessary. For example, even the basic legal concept as to when a document is an original or a copy is influenced by electronic and digital technology.

In order to be able to evaluate whether a witness called as an expert is indeed an expert, judicial officers need to understand what type of experience and qualifications is necessary for a person to actually be an expert in respect of the type of expert evidence to be given as well what questions in this regard should be asked. When search and seizure warrants must be granted that relates to electronic and digital evidence, problems are being experienced in respect of the scope and extent of the search. With a better understanding of the technology, this can be addressed as well. Being trained on cybercrime and electronic evidence will also ensure that any of the orders that are made by the judicial officers will be executable orders.

Though the focus is on cybercrime, the need to understand the cyberspace environment and electronic and digital evidence is also necessary within civil and family law litigation. For example, contracts are being concluded electronically through email, on the internet etc. Harassment and/or defamation may be done electronically through Facebook, twitter or email. Understanding the technology will assist judicial officers to better understand and assess the impact of these actions and the judicial officers will be in a better position to assess whether orders prayed for will be executable. Judicial officers will further be in a better position to understand the extent and impact of infringements on the right to privacy through electronic or digital means.

3.9.2 Objectives of the training strategy

Judicial Officers

Though some district court magistrates had attended training dealing with the ECT Act at Justice College when still trained there, they had not had any training on cybercrimes or electronic evidence to the extent they need. Regional magistrates in conjunction with Justice College had arranged their own training around 2006 in each provincial division, which were attend by most regional magistrates in the country at the time on commercial crimes which included cybercrimes,

counterfeiting and the most common schemes and scams. The ECT Act, RICA, POCA, legislation dealing with corruption, copyright, intellectual property, counterfeits and related aspects, electronic evidence, admissibility, etc. were dealt with together with case law discussions, procedures, best practices and practical group work with case studies.

The training on commercial crimes had been included in the training for all newly appointed regional magistrates.

No judges had received any training in respect of cybercrime and electronic evidence.

SAJEI is only responsible for the training of judicial officers.

Other stakeholders:

Prosecutors
Justice College is responsible for their training and they had been receiving basic training in cybercrimes and electronic evidence for a number of years now – it is institutionalized courses. An advanced course must be developed as a need for such a course had been identified.

Interpreters
Interpreters are used in all courts and it is important that interpreters receive the necessary training to understand the technology and terminology in order to be able to interpret it to the accused and witnesses. It is recommended that Justice College should develop a module / course for interpreters dealing with concepts, technology and terminology used in cybercrime matters and electronic and digital evidence. Interpreters also need to be able to interpreter expert witness testimony in this regard and need a basic understanding of these concepts and terminology in order to be able to interpret correctly.

They would require expert assistance to develop training material and/or to adapt available cybercrime material and trainers should be trained for interpreters to train all interpreters.

The available glossary should be developed further as necessary for the needs of interpreters, including the terms and explanations of concepts in the official languages to ensure that there will be uniformity in the terms and explanations used in interpreting the concepts by al language practitioners countrywide. The standardized multilingual 'interpreters dictionary' should be made available to all court interpreters.

Defense lawyers
Courts are experiencing a lot of challenges if either or both the prosecution and/or the lawyer for the accused do not have knowledge of cybercrimes or electronic evidence. It also impacts on the Accused right to a fair trial if his lawyer is not able to challenge evidence due to a lack of knowledge.

Through the education arm of the Law Society of SA, LEAD, attorneys receive both practical training when they are doing articles (6 months course at law schools across the country) and continued education programs. Cybercrime and electronic evidence should be included both in the basic legal training as well as part of the continued education programs.

If the available material can be adapted by them and trainers of LEAD can attend a trainer's course, they can present the necessary training for attorneys countrywide. Attorneys normally would pay for attendance of courses.

3.9.3 Training requirements (needs analysis)

The main identified need is for a centralized course of trainers to attend trainers workshop held by Cybercrime project office, preferably to be done by November 2014.

For the efficient implementation of the workshops, the following elements have to be provided for each training: course and material workshop (5 days), together with experts to develop training material for each course, facilitators' material, workbooks, resource guides for each course and practice manual. This workshop should be one workshop for all three levels of judicial officers to ensure uniformity of material.

It is desirable that the materials to be done by end of Feb 2015 (to be included in the training material for courses for newly appointed regional and district court magistrates – 2015 large number to be trained).

Trainers course for district court facilitators
This training should be a centralized course, with a 3 days length and it should be done by May 2015.

Considering the issue of who may train judicial officers, training material such as DVD that deals with relevant technical aspects, can show how work should be done. Moreover, the DVD should be made to be used by trainers at courses as well.

Training of Trainers for district court courses (30 district court magistrates)

For district court magistrates:
Electronic evidence: 2 days, decentralized courses in each cluster, should be institutionalized
The course should be included in training for newly appointed magistrates

- Overview of sources of electronic evidence
- Relevant legislative provisions (ECT Act, CPA etc) and relevant case law
- Search and Seizure
- Admissibility
- Third party data and privacy rights
- Evaluation of expertise of expert and of evidence
- Practical work: case studies – should preferably also include case record of expert witness testimony to be evaluated as part of practical work

Basic cybercrime course: 3 days decentralized courses – to be ongoing and should be institutionalized
- Introduction to cybercrime risks and threats
- International framework: Budapest Convention
- Introduction to technology
- Relevant legislation and case law
- Applicable procedural aspects
- Electronic and digital evidence including procedure, admissibility, evaluation
- Jurisdictional aspects
- Sentencing in cybercrimes including ancillary orders
- Asset forfeiture applications
- Practical work: Different case studies for group work

For Regional Magistrates
Electronic evidence and aspects of cybercrime are already included in training of newly appointed regional magistrates
Conference for all other regional magistrates (centralized) – 3 days

Course on cybercrimes and electronic evidence should
- Introduction to cybercrime risks and threats

- International framework: Budapest Convention
- Introduction to technology
- Relevant legislation and case law
- Applicable procedural aspects
- Electronic and digital evidence including sources, procedure, admissibility, evaluation
- Jurisdictional aspects
- Sentencing in cybercrimes including ancillary orders
- Asset forfeiture applications
- Practical work: Different case studies for group work

Judges

Conference – centralized, 3 days

- Introduction to cybercrime risks and threats
- International framework: Budapest Convention
- Introduction to technology
- Relevant legislation and case law
- Applicable procedural aspects
- Electronic and digital evidence including procedure, admissibility, evaluation
- Jurisdictional aspects
- Sentencing in cybercrimes including ancillary orders
- Asset forfeiture applications
- Impact of technology on civil litigation

3.9.4 Training capabilities and resources

There are currently regional court magistrates that had done training on cybercrime and electronic evidence. It has been proposed that they be trained as trainers, who can train district court magistrates as trainers for the courses for district court magistrates. Guest lecturers from academia can be used as well. On the other hand, people that potentially might be witness or party in court cannot be used as trainers.

Manuals for trainers with resource material should be compiled

The South African Judicial Education Institute (SAJEI) will organize and arrange all workshops, as it has event coordinators. Certification and accreditation are not done at SAJEI.

Trained trainers will do training for district court magistrate with academics as is needed.

Conference for Regional magistrates:

- Trainers will conduct training together with invited guest speakers, mainly academics
- Can use international experts to present
- Material for workshop DVD should be shop and finalized by end of Jan 2015

Conference for Judges

- Mainly academics
- Should also use international experts to present
- 3 day centralized – must be held during High court recess (April 2015?)
- Would need assistance with funding for conference, international experts, material development

Conference for regional magistrates

- 3 day centralized, to be held next financial year
- Would need assistance with funding for conference, international experts, material development

Courses for district court magistrates

- to be institutionalized
- Electronic evidence courses, 2 days
- At least 10 courses per year should be scheduled – must have at least one per province

Cybercrime courses

- To be scheduled from 2016
- Decentralized, 3 day course
- At least 5 per year

3.9.5 Other considerations

SAJEI and Justice College will assist Cybercrime Project Office to start and maintain SA legislative and case information on suggested Wikipedia site. The above mentioned institutions will forward all relevant legislation and case law currently available as soon as possible to Cybercrime Project Office, thereafter to forward new cases when available to Cybercrime Project Office as well as any new legislation. Useful articles published should also be forwarded to Cybercrime Project Office

It needs to be further discussed the opportunity to develop of Regional Centre in SA for southern Africa region to assist neighboring countries such as Namibia, Botswana, Lesotho, Swaziland. Also, it is needed to improve regional cooperation with the above mentioned countries and should also include study visit to other regional centres.

3.10 Sri Lanka

3.10.1 Justification for training strategy

Usage of the internet had seen a dramatic increase over the past decade and is rapidly on the increase. What were 65,000 internet subscribers in 2001 has grown to 2.1 million in 2013. Commensurate to this increase, it is observed a considerable growth in cyber related crimes. One reason for this is the rapid growth in the use of computers by the private sector in particular in commercial sector impacting on the activities of the average citizen. On top of this e-governance policy had made drastic changes to the manner in which the government attends to the needs of the people. This had also led to a surge in computer related crimes, in particular: Bank frauds, credit card frauds, computer hacking, money laundering, publishing of defamatory and obscene materials on social networks, child pornography etc.

In the recent past a country wide extortion racket was detected using mobile phones and the existing formal banking systems. Further, obtaining remittances (donations) using stolen and or "cloned" credit cards issued outside Sri Lanka through the internet payment gateway to the credit of bogus NPO set up in the receive these remittances was also detected. Investigations revealed the cards had been issued in the US and operated by a person based in France who operated a terrorist cell related to a terrorist group based in Sri Lanka.

Peoples trafficking syndicates operating between Sri Lanka and Australia came to light a few years back and this required attention of law enforcement authorities of other jurisdictions. Interpreting and admitting evidence of the 'logs' of the GPS of these vessels' was held imperative for successful prosecution. These are a few specific instances in which technology impacts on the country in general and the criminal justice system in particular.

Considering the above, there appears to be a greater need now than ever, not only to prevent such incidents but also to ensure that wrongdoers are adequately punished to deter others engaging in such conduct.

Towards this end its imperative all three sectors of the criminal justice system that is the law enforcement, prosecution and the judiciary equip itself with the skills necessary to deal with the violations effectively.

It's important that the personnel who handle this area keep abreast of new development in technology to make an effective contribution towards investigation.

It's in this context requests are made for specialized training in cybercrimes and electronic evidence as the level of expertise available at present is grossly insufficient to deal with these aspects.

3.10.2 Objectives of the training strategy

General comment - Given the fact Sri Lanka is a small jurisdiction and has a very limited number of prosecutors and judicial officers, and as such it's not feasible to have "specialized" judicial officers or prosecutors to handle cybercrimes.

Stakeholders - Sri Lanka being a common law country, the system of criminal justice is adversarial in character and the stakeholders of the system include: High Court Judges, Magistrates, Prosecutors and Investigators.

High Court Judges – Cybercrimes are embodied in the Computer Crimes Act (24 of 2007) and crimes can exclusively be trialed by High Courts. As such training High Court Judges is of

paramount importance. In addition most of the serious crimes end up in High Courts by way of indictments. Thus sound knowledge of electronic evidence is equally important.

Magistrates - Generally Magistrates exercise jurisdiction over large number of crimes and electronic and digital evidence play a vital part in trials. In addition magistrates give directions to the investigators to conduct further investigations when certain aspects are either not covered or in instances where the investigators had failed to carry out vital aspects of the investigation. It's significant to give them an in-depth training on these aspects as magistrates are eventually getting promoted as High Court judges.

Prosecutors - All cybercrimes indictments are drafted by prosecutors, in addition to conduct of prosecutions before High Courts. A sound knowledge relating to cybercrimes /electronic evidence is essential for successful prosecutions. (Supervision of institution of criminal proceedings for Cybercrimes and Credit Card frauds is under a designated officer at the Attorney-General's Dept).

Investigators - A dedicated Unit (Cyber Crime Investigations Unit) has been establishment within the Criminal Investigations Department consisting of 200 odd officers. Without an in-depth knowledge of the subject on the part of the officers concerned, it would be difficult to combat cybercrimes successfully. To complement the Cybercrime Investigation Unit, a Digital Forensic Lab has been established at the Sri Lanka Information and Communication Technology Agency (ICTA). It is important that the personnel who handle this area keep abreast of new developments in technology to make an effective contribution towards investigations.

3.10.3 Training requirements (needs analysis)

The requirement of securing the device and electronic evidence is statutorily dealt under the applicable law (e.g. Evidence special Provisions Act no 14 of 1996).

Judges – Some of the issues that need to be treated are:

- Fundamentals in Information Technology basic concepts in Cybercrimes and content of international instruments relating to cybercrimes/electronic evidence.
- Domestic legislation applicable.
- Challenges encountered in other jurisdictions (case studies) and overcoming them.
- Applicable evidentiary provisions with regard to admissibility,
- Responding to mutual legal assistance requests on timely and fruitful basis.
- Evaluation of electronic /digital evidence of an Expert.
- In particular international standards and practical application of the applicable legal provisions. Safeguards that are needed to be adhered to, when permitting evidence to prevent infringing rights of 3rd parties, human rights etc.

Prosecutors - Basically the same as above and in addition Rules relating to collection, preservation of digital /electronic evidence, issues that can arise out of chain of custody relating in such material, presenting evidence of "experts".

Investigators - Analysis of electronic evidence , including collection of such evidence in a manner presentable as evidence, methods of securing such evidence and chain of custody issues.

3.10.4 Training capabilities and resources

The lack of trainers had badly hampered the training programs and this is a critical need. There are no dedicated trainers; Training thus far had been conducted on an ad hoc basis making use of experts available in the field of IT and electronics. Most of them do not possess a legal background, thus the effectiveness of the training programs is diminished to an extent. Nor is there training modules available on the subject.

There is an urgent need of trainers and towards this and, trainer of trainers programme is a dire need at present.

Sri Lanka would appreciate if it could be facilitated to train a set of trainers in the three categories (Judicial, Prosecutorial and Investigatory). This is the only way Sri Lanka can obtain trainers. As a short term measure, placement in training programs for judicial officers and prosecutors is desirable.

Its suggested training to be delivered by using the following ideas:

- Conduct of workshops within the country
- Facilitating participation in workshops outside the jurisdiction in particular international seminars.
- Visits to regional Training Institutes.
- Placing a training modules in the curricular (judges training) thereby institutionalising Cybercrime training.

Same is the case with prosecutors and investigators, with necessary adjustments.

No cybercrime training centre is available at present but does not seem to be in need of one at this point.

Experts in the field of IT/ electronics from the Universities/ICTA can be made use of for training. Even presently it's happening. All training should be delivered in the English language.

Resources Available

For the training of the judges, the Judges Training Institute is available plus it has its own training budget which very limited for continuing training. There is no training institute for prosecutors but training sessions are conducted on ad hoc basis. Resources available for workshops are very limited. However, logistical requirements are available within the A.G's Department for the conduct of workshops.

3.10.5 Other considerations

The urgent need is to have a set of Trainers trained (for each stake holder referred to):

- Development of Training Module is another requirement; this again has to be separate training modules for sectors.

- Preferably training programme should be confined to 3 days.

Assistance of the Council of Europe is sought to achieve the above objectives.

3.11 Tonga

3.11.1 Justification for training strategy

In August 2013, Tonga became connected to high speed internet. This was made possible through fibre optic cable from its neighbouring country of Fiji. Therefore internet has become readily available for Tonga through telephones and other mobile devices. Even though it has proven to be a beneficiary move it also has come with its challenges.

The high speed internet has seen reports of cyber bullying, abuse of social networks, distribution of pornography (adult & minor) and the commission of traditional crimes with the use of the internet or telephone to name a few. However prior to the high speed internet Tonga has seen an increase in the number of bank fraud cases involving the manipulation of bank computer systems. There have also been cases of similar nature involving private companies as well.

Tonga has also seen the challenges in handling digital evidence. Law enforcement are not efficiently equipped to handle, store and present digital evidence. Relevant authorities are also not aware of the proper procedures involved when extracting and storing digital evidence.

3.11.2 Objectives of the training strategy

A proper needs analysis will have to be conducted on each of these stakeholders so that actual needs are identified. However, listed below are the basic needs, as follows:

1) Judges and Magistrates
- Assessing electronic evidence;
- Ruling on the reliability and admissibility of electronic evidence;
- Understanding the way in which the crime was committed;
- Gathering of evidence process for the issuing of court orders for instance search warrants etc.

2) Prosecutors (mid to senior level)
- Investigating procedures of cybercrime;
- Extracting, processing and proper storage of electronic evidence;
- Assessing and presenting the evidence in court; and
- Understanding the admissibility and reliability of electronic evidence.

3) Legal Drafters (are also Prosecutors)
- Understand the technical terms;
- Understand the process of investigation and procedures involved;
- Understanding the ways the crimes are being committing;
- Understanding the development of cybercrime and electronic specific policies and its development into law.

4) Court translators
- Technical terms;
- Technical evidence.

3.11.3 Training requirements (needs analysis)

A proper needs analysis will have to be conducted on each of these stakeholders so that actual needs are identified. However, listed below are the basic needs, as follows:

1) Judges and Magistrates

- Assessing electronic evidence;
- Ruling on the reliability and admissibility of electronic evidence;
- Understanding the way in which the crime was committed;
- Gathering of evidence process for the issuing of court orders for instance search warrants etc.

2) Prosecutors (mid to senior level)
- Investigating procedures of cybercrime;
- Extracting, processing and proper storage of electronic evidence;
- Assessing and presenting the evidence in court; and
- Understanding the admissibility and reliability of electronic evidence.

3) Legal Drafters (are also Prosecutors)
- Understand the technical terms;
- Understand the process of investigation and procedures involved;
- Understanding the ways the crimes are being committing;
- Understanding the development of cybercrime and electronic specific policies and its development into law.

4) Court translators
- Technical terms;
- Technical evidence.

3.11.4 Training capabilities and resources

There are currently no trainers in Tonga to implement a training strategy. However we have identified one representative from the Attorney General's Office intended to train the prosecutors and one representative from the Ministry of Justice intended to train the judges and magistrates.

The following is a short to long term strategy that Tonga would like to see being implemented:

1) Basic Train the Trainer's Course

As these two representatives are not trained to train at the moment, Tonga would appreciate any assistance from the Council of Europe for them to attend the basic train the trainer's course as a start. The provision of basic training material would be required as well.

2) Local In-house Training

The returning trainers would be able to conduct in-house trainings three separate trainings for judges, magistrates and the prosecutors. The justification for separating the judges and the magistrates is that there is only one legally trained magistrate amongst the six of them and the remaining are law practitioners. Therefore the course would have to be delivered to them in the Tongan language. The two judges and the prosecutors can have their individual sessions.

Taking into consideration the small number of judges, magistrates and prosecutors, it would be practicable to conduct the sessions during the lunch hour once a week depending on the duration of the course.

3) Regional Approach Training

The regional approach would be to have the Council of Europe and other donor partners for example the World Bank that would want to fund a regional training on cybercrime as was previously done in 2011. The support through the current Pacific Judiciary Development Programme could also be another avenue that the Council of Europe and other donor partners could use to train the judges and the magistrates.

4) International Approach Training

International approach would see more trainers benefitting from the Council of Europe programs. Practically the judges could be sent one at a time to take part in these trainings to assist in advancing their skills in cybercrime and electronic evidence. Also the attending of the trainers of the advance course as well.

5) Delivery of Training

The most effective way of delivering the training in Tonga would be through face to face. As mentioned it would be practicable to have the training during the lunch hour so that court sittings are not interrupted. As there are currently no materials in Tonga, any sort of assistance in providing this would be appreciated.

6) Cybercrime Training Centre

As for a cybercrime training centre, the best approach with this would be at a regional level so that the resources both technical and logistical would be maximised.

7) Type of training

Trainings both on the technical and legal aspects of cybercrime and electronic evidence should be taught at both the national and regional level.

8) Language

With regards to languages, if the training is delivered on a regional level it would be best delivered in English. However as previously mentioned local trainings would be delivered in Tongan and English.

3.11.5 Other considerations

- Developing a "off-the-shelf" basic training course that can be used by any successor to the nominees intended to be trained. It is required that the Council of Europe to assist in the development of this curriculum.

- The use of the newly established Cyber Challenges Task Force and their working groups. This could be an expert group both on a technical and legal level as it consists of law enforcements, ICT personnel's and other relevant stakeholders.

3.12 Romania

3.12.1 Justification for training strategy

Information technology affects different aspects of the crime spectrum and both national legislation, Romanian distinguishes between computer enabled crimes and computer dependent crime and therefore traditional crimes committed with the use of information technology will be dealt properly if the judiciary and law enforcement will be trained to understand the role played by the technology in the commission of a crime. In Romania, there is a large variety of crimes with which the prosecutors and judges are confronting.

In Romania, because of the specialised prosecutors unit, their activity can be measured as well the impact of the computer dependent crimes. As a fact, technology affects most economic crimes (credit card fraud, bank frauds, forgery, embezzlement but also pornography, different types of participation in crimes such as recruitment in trafficking in human beings, drug trafficking over the internet and many others).

Electronic evidence, even if not defined in the Romanian criminal procedural code, is accepted as a factual element revealed in the cyberspace. The encounter of the electronic evidence and the need of its understanding have been stressed by the Romanian delegation.

Computer data as defined by the CCC can be seen in fact as a definition of the electronic evidence with this add: this computer data has the force to prove or ability to prove the existence or not of a crime, the guilt or innocence of a suspect.

Seen as a factual element, computer data/electronic evidence is not obvious for the human eye and therefore translation is needed, education is needed.

3.12.2 Objectives of the training strategy

In Romania there is a clear distinguish between:
- police officers mandated with the investigation and gathering the evidence
- prosecutors supervising or being involved in the investigation as it is in Romania
- judges (natural judge principle)

Moreover, there are no specialized courts for cybercrime but there are specialized units for prosecutors and law enforcement (limited jurisdiction in investigating cybercrime – computer depended crimes and a few from the computer enabled crimes such as computer related fraud, computer related forgery, organized crime linked to credit card fraud etc. The other computer enabled crimes are investigated and prosecuted by the regular units.

In conclusion, training is needed at all levels even though there is some knowledge.

3.12.3 Training requirements (needs analysis)

The information above is specific to law enforcement power and procedure however in Romania the prosecutor is the leader of the investigation either supervising the investigation either being involved directly and therefore such information is needed.

It was indicated that securing evidence is crucial for the prosecution and proper working methodologies are needed to be disseminated throughout the judiciary.

Knowing and following procedures make the evidence legal, predictable, traceable, reliable, completed etc. These are considered working methods.

Special investigative powers are considered important and critical in obtaining evidence. The legal and the technical aspects of such proceedings are either important (real time data collection, real time traffic data collection, computer searches seizure, computer data analysis, other type of expertise on viruses, programming etc.

However, the investigation methodology is also considered important:

- where to find the evidence and how to obtain it in different practical cybercrime cases
- how to investigate a botnet, an intrusion etc
- how to correctly bring charges and sustain charges with the proper evidence package
- what it is to be proven in different types of crime
- collection of case studies, working books
- glossary of terms, definitions, common understating

3.12.4 Training capabilities and resources

In Romania, there is a lack of trainers for both initial and continuous training. A way to get more trainers is to train the trainers, to recruit practitioners and train them to teach where possible. Practitioners have to be encouraged to train and to disseminate knowledge.

In Romania, there is a project called Cyberex-ro which is planned to be functional in 2016. With this project 8 trainers will be educated in the University College of Dublin in order to get skills in computer investigation, computer forensic. The obligation of the project is to produce different training materials that can be used at different levels of knowledge for judiciary as well as for the law enforcement.

There have been conducted training conferences with all the actors involved in the proceedings.

Simplified materials related to computer investigation/forensic can be and should be embedded in the initial training curriculum of the National Institute of Magistracy (NIM) as well as for continuous training for judiciary.

For Romania, Cyberex-ro project and NIM should plan by the end of the project a way to maximize the dissemination of the teaching materials as well as to constitute a working group to identify possible updating of the materials.

Romania is exploring the possibility to attract academia and private sector into the training programs. For continuous training, it is possible and already done. It was indicated the existence of training rooms within the National Institutes equipped with computers and technology specific for training.

In Romania, at the Institute level there is a kit used to give information to the students but not practical information on how the kit is really used in practical cases.

A computer investigation module is to be developed by Cyberex-ro and then, upon a subsequent memorandum of understanding delivered to the students and in office judiciary.

E-learning is to be considered.

Identifying resources from academia and private sector that can be involved in judiciary training is to be explored at least for very specific areas such as programming, virus analysis or else.

3.12.5 Other considerations

Help in identify a profile for trainers (practitioners) – train the trainers, working methodologies, investigative methodologies, collection of case law studies, exercises.

4 CONCLUSIONS AND RECOMMENDATIONS TO THE PROJECT AREAS

4.1 Conclusions

Divided into groups, participants discussed possible elements of judicial training strategies to ensure broadest possible training of judges and prosecutors on cybercrime and electronic evidence:

- Group 1: Morocco and Senegal (Facilitators: Estelle de Marco and Adel Jomni)
- Group 2: Armenia, Azerbaijan, Georgia (Facilitator: Nigel Jones and Kornelija Ivanusic)
- Group 3: Mauritius, Philippines, Sri Lanka, South Africa, Tonga (Facilitator: Esther George and Pedro Verdelho)
- Group 4: Moldova and Romania (Facilitator: Ioana Albani)

The groups presented the current situation in each country and then further discussed how to set up the judicial training strategy specific on each country needs.

Several countries have introduced some elements of cybercrime training within their wider education and training programmes delivered; however these do not appear to be introduced as a result of any specific subject related needs analysis being conducted.

Notable activities among the countries are:

- Even if Morocco has a Judicial Training Institution specialised in training for judges and prosecutors, there is no specific modules dedicated exclusively to Cybercrime and Electronic Evidence integrated in the mainstream training curricula.

- The Philippines has provided information regarding the Philippine Judicial Academy (PHILJA), which is a specialized entity under the Supreme Court tasked with the training of judges and lawyers that has recently commenced a three-day seminar on the very subject of cybercrime and electronic evidence. From this perspective, the Philippines through PHILJA can be the regional centre for delivering internationally assisted training programs on cybercrime, ICT systems and electronic evidence.

- Due to its strategic position and its regional influence, Senegal proposed the establishment of the Judicial Training Centre for West Africa (CFJ), a regional Center of Excellence on Cybercrime.

- In South Africa, there are currently regional court magistrates that had done training on cybercrime and electronic evidence and it has been proposed that they be trained as trainers, who can train district court magistrates as trainers for the courses for district court magistrates. The South African Judicial Education Institute (SAJEI) has the capacity to organize and arrange all workshops, but they cannot arrange certification and accreditation.

- The representatives from South Africa proposed to be further discussed the opportunity to develop of Regional Centre in SA for southern Africa region to assist neighbouring countries such as Namibia, Botswana, Lesotho, Swaziland.

- Tonga has taken part into a regional intervention on cybercrime designed by World Bank, which funded a regional training on cybercrime in 2011.

4.2 Recommendations

The recommendations that follow should be read in conjunction with the individual project area information that appears above.

Having in mind that cybercrime has a transnational nature, it is necessary to promote **international cooperation** in the fight against cybercrime on the basis of common rules. Every country has its own rules, but the universal moral norms are the same everywhere, therefore there should be common understanding on cybercrime related issues. The common understanding and the substantial law is the Budapest Convention on Cybercrime.

The Judicial Training Strategy should include how to organize the training courses in an effective manner and also how **to integrate the training courses in the curricula of the training institutions (centres)**. Training in cybercrime and electronic evidence should also be developed into mainstream training systems for judges and prosecutors.

Due to the identified lack of trainers at the national level, the Council of Europe should provide foreign experts (consultants) who will be involved in the process of developing curriculum on cybercrime in the respective Judicial Training Institutions (Centres) and get involved in **Training of Trainers programmes**.

The **adaptation of training materials** to country specific needs and national legislation should be one of the stepping stones of training development curricula. Moreover, the training workshops and materials should be specialised for different stakeholders, according to their identified needs. Length of the trainings should vary between 3-5 days, depending on the needs identified for each stakeholder.

For the effectiveness of trainings delivered to priority countries within the GLACY project and also for the efficient use of resources, **a pool of international trainers** should be set up in order to put in place a ToT strategy that is implemented consistently to all project countries. The need for international expertise of trainers was stressed by all participating countries throughout the workshop.

The creation of an online platform (CyberWiki) for **sharing case studies and best practices** on cybercrime related cases should be an opportunity to transfer the knowledge from the more advanced countries to the ones that are starting to develop national strategies. The online platform can also be used and an efficient tool for e-learning and sharing training materials.

Regional hubs for training should be established in areas as West Africa, Central Africa or the East Pacific islands, in order to provide technical assistance and share good practices in areas with similar cybercrime related cases. This endeavour would have a multiplicative effect on the region and would enable regional cooperation for neighbouring countries

5 Annexes

5.1 Annex 1 Agenda of the Judicial Training Workshop

CyberCrime@EAP
Joint project on cybercrime in the Eastern Partnership region

GLACY
Joint project on Global Action on Cybercrime

Draft version 20 May 2014

Mainstreaming judicial training on cybercrime and electronic evidence

International workshop under the CyberCrime@EAP and GLACY projects
Hosted by the Romanian National Institute of Magistracy
Bucharest, Romania, 2 – 3 June 2014

Agenda (draft)

Background

Given the threat of cybercrime and the increasing relevance of electronic evidence in criminal proceedings it is essential that judges and prosecutors have access to training addressing these matters and providing at least basic skills. In 2009, therefore, the Council of Europe adopted a concept recommending that modules on cybercrime and electronic evidence be integrated into the curricula of judicial training institutions. The concept has been tested successfully in South-eastern Europe and training materials (Basic course, advanced course, Electronic Evidence Guide) have been developed. The implementation of this concept is now supported through the CyberCrime@EAP and GLACY projects also in other regions.

Objective

The aim of the workshop is:

- To prepare elements of domestic judicial training concepts for each of the participating countries.

Participants

The workshop is primarily for representatives of training institutions for judges and prosecutors in management positions or responsible for curriculum development. The CyberCrime@EAP and GLACY projects will fund travel and per diem expenses for:

- 2 representatives of judicial training institutions from each Eastern Partnership country: Armenia, Azerbaijan, Belarus, Georgia, Moldova and Ukraine;
- 2 representatives of judicial training institutions from each of the following GLACY priority countries: Mauritius, Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga.

Working languages will be English, French and Romanian.

Location

The workshop will take place at the Romanian National Institute of Magistracy (www.inm-lex.ro) in Bucharest: Bd. Regina Elisabeta, nr. 53, sector 5, Bucuresti

Programme

Monday, 2 June 2014	
8h30	**Registration**
9h00	**Opening session** Octavia Spineanu-Matei, Director, National Institute of Magistrates Simona-Maya Teodoroiu, State Secretary, Ministry of Justice George Muscalu, Prosecutor, Vice-president of the Superior Council of Magistracy Alexander Seger, Head of Cybercrime Programme Office, Council of Europe
9h45	**Training systems and institutions in participating countries** Moderator: Esther George, UK Introduction (moderator of the session) Presentations by participating countries
10h30	*Coffee break*
10h45	**The judicial training concept of the Council of Europe: Elements** Moderator: Pedro Verdelho, Portugal Introduction to the concept (Cristina Schulman, Romania) Experience in South-Eastern Europe (Kornelija Ivanušić, Croatia)
12h00	**Why? Explaining the need for training on cybercrime and electronic evidence** Moderator: Pedro Verdelho, Portugal Introductory comments (Nigel Jones, UK / Ioana Albani, Romania / Estelle De Marco, University of Montpellier) Comments by participants
12h30	*Lunch break*
14h00	**Group work: possible elements of a domestic training strategy** Divided into groups participants will discuss possible elements of judicial training strategies to ensure broadest possible training of judges and prosecutors on cybercrime and electronic evidence. Group 1: Morocco and Senegal (Facilitators: Estelle de Marco, Montpellier / Adel Jomni, Montpellier) Group 2: Armenia, Azerbaijan, Georgia (Facilitator: Nigel Jones / Kornelija Ivanusic) Group 3: Mauritius, Philippines, Sri Lanka, South Africa, Tonga (Facilitator: Esther George, UK / Pedro Verdelho, Portugal) Group 4: Moldova and Romania (Facilitator: Ioana Albani)
16h00	Transfer to Victoriei Palace
17h00	**Launching ceremony of the Cybercrime Programme Office** of the Council of Europe (C-PROC) in Bucharest followed by a cocktail
Tuesday, 3 June 2014	
9h00	**Elements of domestic training strategies: results from group work** Moderator: Esther George, UK

10h30	*Coffee break*
10h45	**Training materials available** Moderator: Esther George, UK Council of Europe materials (Pedro Verdelho / Nigel Jones) Basic course Advanced course Electronic Evidence Guide Training materials developed in France (Adel Jomni, University of Montpellier) Materials available in participating countries
12h30	*Lunch break*
13h30	**Preparation of elements of domestic training strategies and steps to be taken** Delegations from each participating country are invited to prepare an outline of a domestic judicial training strategy: integrating training on cybercrime and electronic evidence into the curricula of judicial training institutions. (Facilitators to assist)
15h30	**Presentation of elements of domestic training strategies by each country** Moderator: Estelle de Marco, France Delegations are invited to present a summary of the elements prepared.
17h30	**Conclusions** Octavia Spineanu-Matei, Director, National Institute of Magistrates Alexander Seger, Head of Cybercrime Programme Office, Council of Europe
18h00	*End of the workshop*

Contact

At the Council of Europe:

Polixenia Calagi
Project Officer
Cybercrime Programme Office of the
Council of Europe (C-PROC)
Bucharest, Romania
Email: Polixenia.CALAGI@coe.int

At the Romania National Institute of Magistracy:

Razvan Mihaila
Expert
Institutul National al Magistraturii
Tel: 021 407 62 51
Fax: 021 407 62 59
Email: razvan.mihaila@inm-lex.ro

5.2 Annex 2 List of Participants

CyberCrime@EAP
Joint project on cybercrime in the Eastern Partnership region

Funded by the European Union and the Council of Europe

Implemented by the Council of Europe

GLACY
Joint project on Global Action on Cybercrime

www.coe.int/cybercrime

Mainstreaming judicial training on cybercrime and electronic evidence

International workshop under the CyberCrime@EAP and GLACY projects
Hosted by the Romanian National Institute of Magistracy
Bucharest, Romania, 2 – 3 June 2014

LIST OF PARTICIPANTS

Version 30 May 2014

Country		Surname	First name(s)	Position	Institution
Armenia	Mr.	HAKOBYAN	Hayk	Prosecutor of the Prosecutor General Office's Department for Investigation by National Security Agencies and on Cyber Crimes	General Prosecutor's office of the Republic of Armenia
Armenia	Mr.	TIGRAN	Poghosyan	Specialist on Criminal Cases Scientific and Research Department	Justice Academy of Republic of Armenia
Azerbaijan	Mr.	ALIKHANOV	Erkin	Deputy head of International Relations Direction	Deputy Chief of the International Cooperation Department, Head of the Extradition and Legal Assistance Section, Office of the Prosecutor-General of the Republic of Azerbaijan
Georgia	Mr.	KUTALADZE	Davit	Senior Investigator of the Investigative Unit at Tbilisi Prosecutor's Office	Chief Prosecutor's Office of Georgia

Country		Surname	First name(s)	Position	Institution
Georgia	Ms.	PARJIANI	Aniko	Chief Consultant of Cooperation with International Organizations	The High School of Justice
Moldova	Mr.	TALPA	Boris	Trainer of the national institute of justice on IT, investigation and judging of cybercrimes , judge	National Institute of Justice of Republic of Moldova
Moldova	Ms.	PITIC	Mariana	Chief of Training and Research Direction	National Institute of Justice of Republic of Moldova
Mauritius	Mr.	MADHUB	Oomeshwarnath	Deputy Solicitor General for Solicitor General	Solicitor General, Mauritius
Mauritius	Ms.	CHUI YEW CHEONG	Ah Foon	Judge of the Supreme Court and Chairperson of the Institute for Legal Studies	Institute for Legal Studies, Mauritius
Morocco	Mr.	MOULOUDI	Lhoucine	Chef de la division de la formation des attachés de justice à l'ISM	Division de la formation des attachés de justice à l'Institut Supérieur de la Magistrature, Morocco
Philippines	Mr.	BRUSELAS	Apolinario D.	Associate Justice	Court of Appeals, Manila, Philippines
Senegal	Mr.	DIAKHAT	E. Mamadou	Directeur du Centre de formation Judiciaire	Centre de formation Judiciaire, Dakar, Senegal
Senegal	Mr.	SALL	Samba	Magistrat, Juge d'instruction en charge du 2e cabinet d'instruction au Tribunal de Dakar	Tribunal de Dakar, Senegal
South Africa	Ms.	WESSELS	Jacoba Hendrina	Regional Court President, Polokwane, South Africa	Regional Court, Polokwane, South Africa
South Africa	Ms.	ROUX	Wilhelmina Cecilia	Advocate	Prosecutorial Training, Justice College.
Sri Lanka	Mr.	BUWANEKA	Aluwihare	Judge of the Supreme Court	Supreme Court, Colombo, Sri Lanka
Sri Lanka	Mr.	WIMALASENA	Ranga	Magistrate / Additional District Judge	Judicial Service Commission,Colombo, Sri Lanka
Tonga	Ms.	MACOMBER	Leotrina	Assistant Crown Counsel	Attorney General's Office, Government of the Kingdom of Tonga

Country		Surname	First name(s)	Position	Institution
Tonga	Ms.	TALANAIVINI	Mafi Adi	Legal Officer/Sub-registrar/Information Officer	Ministry of Justice/ Registrar General's Office Nuku'alofa, Tonga

SPEAKERS/FACILITATORS

Country		Surname	First name(s)	Position and Institution
Romania	Ms.	ALBANI	Ioana	Chief Prosecutor, Head of the Cybercrime Unit Prosecutor's Office attached to the High Court of Cassation and Justice Directorate for the Investigation of Organised Crime and Terrorism offences
France	Ms.	De MARCO	Estelle	Managing Director, Inthemis
United Kingdom	Ms.	GEORGE	Esther	Lead Cybercrime Consultant, Global Prosecutors E-Crime Network (GPEN) part of the International Association of Prosecutors and Zyber Global Ltd
Croatia	Ms.	IVANUSIC	Kornelija	Judge of municipal Court in Velika Gorica, Judicial Academy of Croatia
France	Mr.	JOMNI	Adel	Enseignant-chercheur UFR Droit & Science politique, Université Montpellier1, Directeur diplôme d'Université : Cybercriminalité : Droit, Sécurité de l'information & Informatique légale
United Kingdom	Mr.	JONES	Nigel	Specialist, Cybercrime and Electronic Evidence
Romania	Ms.	SCHULMAN	Cristina	Legal Adviser, Treaties International Relations and Liaison Magistrates Unit, Department of International Law and Judicial Cooperation, Ministry of Justice
Portugal	Mr.	VERDELHO	Pedro	Public Prosecutor, Cybercrime Office – Prosecutor General's Office

ROMANIA

Country		Surname	First name(s)	Position and Institution
Romania	Ms.	TEODOROIU	Simona-Maya	State Secretary, Ministry of Justice
Romania	Ms.	SPINEANU-MATEI	Octavia	Director, National Institute of Magistrates
Romania	Mr.	MUSCALU	George	Prosecutor, Vice-president of the Superior Council of Magistracy
Romania	Mr.	NICULAE	Nicoleta	Chief Prosecutor – Center for Operational Applications
Romania	Mr.	BADEA	Viorel	Chief Prosecutor - The Prevention and Combating Cybercrime Service
Romania	Ms.	POPA	Silvia	Chief Prosecutor - The Prevention and Combating Cybercrime Service
Romania	Mr.	ENCESCU	Florin	President, Court of law, Gorj
Romania	Mr.	TRUSCA	MARIAN	Deputy Director, National Institute of Magistrates
Romania	Mr.	MIHAILA	Razvan	Expert, National Institute of Magistrates

COUNCIL OF EUROPE
CYBERCRIME PROGRAMME OFFICE (C-PROC)

Organization		Surname	First name(s)	Position
COUNCIL OF EUROPE	Mr.	SEGER	Alexander	Head of Cybercrime Programme Office Executive Secretary of the Cybercrime Convention Committee
COUNCIL OF EUROPE	Ms.	CALAGI	Polixenia Elena	GLACY project team- Project Officer
COUNCIL OF EUROPE	Ms.	HANGANU	Maria Sinziana	GLACY project team – Project Assistant