# GLACY Special

## GLOBAL ACTION ON CYBERCRIME

The Global Action on Cybercrime (GLACY) Project is funded by the European Union and the Council of Europe. The implementation of the project is carried out by the Council of Europe. Within the framework of the GLACY Project, an international workshop on mainstreaming judicial training on cybercrime and electronic evidence was hosted by the National Institute of Magistrates in Bucharest, Romania from 2nd to 3rd June 2014. The aim of the workshop was to prepare elements of domestic judicial training strategies for each of the participating countries.

The IJLS was represented at the workshop by its Chairperson who delivered the Judicial Training Country Strategy. At the workshop, the Chairperson stressed the fact that the IJLS has the statutory mandate of delivering training to all the stakeholders in the administration of justice and of providing Continuing Professional Development (CPD) courses to all law practitioners. She also advocated for a Training Of Trainers (TOT) programme whereby a contingent of trainers from the police prosecutors, state prosecutors, law practitioners and judges will be constituted and trained to deliver courses in cybercrime and electronic evidence at the Institute. The Chairperson also requested assistance from the Council of Europe for the TOT programme, which was readily granted.

The first session of the TOT programme took place at the IJLS from 26th to 30th January 2015.

## Opening Ceremony of the Training of Trainers (TOT) Programme


In her speech at the opening ceremony of the TOT programme, the Chairperson of the IJLS, Justice Mrs A F Chui Yew Cheong pointed out that cybercrime has already paved its way in the criminal landscape and therefore it is important that all parties dealing with cybercrime, whether at investigation level or adjudication level be given adequate training on cybercrime and electronic evidence issues. She highlighted the relevance of the TOT programme as having capacity building ends at the IJLS. She thanked the trainers from the Council of Europe for the preparation of a very comprehensive programme ranging from relevant theoretical and technical aspects of electronic evidence as well as sessions aimed at the development of communicative aptitudes of potential trainers. She concluded her speech on a note of anticipation that the TOT will bear fruition with the advent of a pool of competent trainers in the near future. The potential trainers will be called upon to impart basic knowledge about cybercrime and electronic evidence issues to the members of the judiciary and the legal profession.

On behalf of the European Union and the EU Delegation to Mauritius, Mr. Aldo Dell'Ariccia, Ag. Ambassador, Head of the European Union delegate to Mauritius, thanked the IJLS for hosting and providing a platform for the training prepared with the invaluable support of the Council of Europe.


In his speech, he underlined that there is a growing evidence of the strong link between connectivity and social and economic progress; and the reliance on Information and Communication Technologies has never been greater. He also emphasised that opportunities offered by cyberspace in terms of social and economic development also contribute to the growing vulnerability to cybercrime threats. As a result, law enforcement authorities and the judiciary are confronted with numerous obstacles in the efficient performance of their duties. In this light, the EU has also recognised its responsibility to deepen and expand the cooperation with other countries to improve the prevention and prosecution of cybercrimes outside the EU.

Further, he mentioned that the Budapest Convention on Cybercrime provides an excellent model that includes all necessary safeguards and conditions for successful cybercrime investigation. He explained the rationale behind the EU's active contribution in the endeavour of fostering the Budapest Convention. This has culminated in the EU's partnership with the Council of Europe for some years already in implementing projects in the EU's neighbouring countries aiming at strengthening the capacities of criminal justice authorities to co-operate effectively against cybercrime, in line with the provisions of the Budapest Convention.

Both speeches underlined the instrumental role of the training and were hopeful that judicial and law enforcement training institutions will incorporate cybercrime modules in their curriculum.

## GLACY
## Cybercrime and Electronic Evidence Training of Trainers (TOT)
## Port Louis, 26 – 30 January 2015

The Cybercrime and Electronic Evidence Training of Trainers (TOT) was held at the seat of IJLS in January 2015. The training was delivered by delegates from the Council of Europe namely Mr. Zahid Jamil (Barrister-at-Law), Mr. Nigel Jones (Cybercrime and Electronic Evidence Specialist) and Mrs. Victoria Catliff (Project Manager of the TOT). The participants at the training consisted of law practitioners, Magistrates and police officers. The course itself had been designed to provide law enforcement officers, Prosecutors, Magistrates and Judges with an overview of the practical skills to aid them in their respective responsibilities regarding cybercrime investigation, prosecution and adjudication.

The five days' training course comprised of substantive parts on cybercrime, mainly understanding the criminal law provision whilst identifying the key factors used to describe the offences based on the Budapest Convention, as well as training skills on presentation delivery techniques.

The substantive part laid emphasis on the theory of cybercrime and how this practice is becoming part of nearly all crimes committed worldwide, especially white collar crimes. Various cases were discussed where local people have been victims of cybercrime, especially where financi -al institutions' websites were forged to commit fraud. Further, it was also pointed out that it is crucial to determine a cybercrime case in the light of specific characteristics.

The sessions on training skills laid focus on areas namely the identification and understanding of the characteristics of good and poor presenters; earmarking appropriate ways of giving and receiving feedback ("feedback sandwich"), verbal and non-verbal communication, preparation and planning, training and delivery mechanisms, audience engagement and the art of listening and questioning while delivering a presentation.

At the end of the five days' training course, the delegates made individual presentations on different topics related to cybercrime. Upon delivery of their presentations, the delegates received feedback from the audience as part of a self-evaluation mechanism.

The training course, on a global note, shed light on interesting facets of cybercrime; not only through the informative sessions carried out by the trainers of the Council of Europe but also through presenta-

tions made by the trainee delegates. The trainers highlighted that the sessions lived up to the expectations in as much as the team of trainees consisted of professionals from various fields of the criminal justice hierarchy and the various activities and interactions in which they participated were fuelled with ease and motivation.

# INTERVIEWS

**Mrs Victoria CATLIFF**

Project Manager, Council of Europe

**Being a project manager at the Council of Europe entails a lot of work and responsibilities. Could you tell us more?**

I am new to the Council of Europe which I joined in October 2014. Prior to that, I worked for the UNODC where I managed a regional $ 1.5 million in a legal technical assistance project on counter-terrorism in 5 countries of Central Asia. Before that, I worked for 13 years, managing protection and prevention programs for the International Committee of the Red Cross (ICRC) in favour of victims of armed conflict (including security detainees) in conflict zones of Africa, Asia and Europe. I am legally trained and have long experience in managing projects for international organisations.

The project manager is basically responsible for the implementation of the project document, a matrix which is presented to a donor for funding. A project may be started with partial funding and/or complete funding. Progress assessment is an ongoing process and funds are often released in relation with results obtained. In this particular case, it is funded by the government. This project, GLACY (Global Action on Cybercrime) in which Mauritius is a partner, is fully funded (Euro 3.35 million), by the European Union and the Council of Europe and implemented by the latter. Fully funded projects take a bit of pressure off as there is no need to hunt for fund raising mechanisms. As a project manager, one may be involved in the drafting of the project presented for funding or one may be recruited to launch or manage an ongoing specific project, dealing with a particular thematic area like this one on cybercrime or say, the prevention of terrorism. The position may be allocated depending upon the knowledge and expertise of the candidate. I applied for this position based on my interest in international co-operation. The project manager is also responsible for the budget and expenditures have to be accounted for: The donor has to be kept informed and briefed about the way in which the money is being spent. The project manager is responsible for ensuring the proper implementation of the project activities.

There are two programme managers under the GLACY project and their tasks are divided by countries and we work together in reporting and dividing the work plan. Since I speak French and I have worked in French-speaking countries such as Chad, Rwanda, Morocco and Senegal, I took up this assignment in Mauritius. I also have responsibilities for another project in Eastern partnership region in 6 countries of the former Soviet Union. There is another project called ‘Octopus’ which is an online community of around 300 experts, who meet in a conference in Strasbourg every year or two in thematic working groups on areas such as standard operating procedures, law reform, online radicalisa-

tion, women and cybercrime, online child protection etc.

The concept of this judicial training course was developed during a previous course in Southern Europe. My responsibility also lies at the level of contracting out the right consultant to do a particular job.

This project, as most other projects, has seven priority result areas:

1. Engaging with political authorities,
2. Harmonisation of legislation,
3. Law enforcement training,
4. Judicial training,
5. Inter-agency and public-private co-operation,
6. International co-operation and
7. Assessment of progress.

There are overall, global objectives and targeted/specific objectives in those priority thematic areas. The seven privileged countries benefitting from technical assistance under this project have been chosen on the basis of their commitment to implementing the Budapest Convention and of the seven, Mauritius is the only country to have adopted the Convention thus. As such, Mauritius is involved in policy-making and the priorities for assistance have thus a different focus to other countries.

We have a team of thematic experts and as seen in Mauritius, there are two external consultants with different profiles; one is from a legal background whereas the other one has law enforcement, pedagogical experience. The project began by a country visit by a multi-disciplinary team: a legal expert, a law enforcement expert, technical, project manager etc. The number of experts involved might reach up to five. They develop an initial situation report, based on a visit for two weeks of all the relevant agencies in the country, and from that, a work plan is developed and sent to the authorities for their comments. Following this, the work plan is transposed into activities. Some activities, such as the judicial training of trainers introductory and advanced course on cybercrime and, electronic evidence are carried out in every country. Other activities can be designed specifically according to country needs. For example, there can be requests for tailor-made activities, such as a workshop to mobilise political support for the creation of a cyber security centre of excellence or a workshop on legislative amendments to harmonise with the Budapest Convention. Different countries use different languages of instruction for delivering this course and then it is adapted according to local needs. Mauritania, for instance, made a request for a team of Council of Europe to review its cybercrime legislation and produce a one-off report. As such, I would contact one of our legal experts and ask whether they are available to do a gap analysis report comparing domestic legislation in compliance with international requirements.

**How important it is for the Council of Europe to train the signatory members of the Budapest Convention in the light of emerging issues of cybercrime?**

The Convention Committee (T-CY) regroups countries parties to the Budapest Convention and Mauritius is one of

them. 45 States have ratified to the Convention and other States have adapted their domestic legislation with reference to the Budapest Convention without being party to it. The parties meet in Strasbourg twice a year and sessions are devoted to areas such as implementing provisions of the Convention and, producing guidance notes (link to webpage: http://www.coe.int/dghl/cooperation/economiccrime/cybercrime/T-CY/Default_TCY_en.asp). One such guidance notes on trans-border access to data was adopted in December 2014 (see link on http://www.coe.int/t/hghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY (2013)7REV_GN3_transborder_V12adopted.pdf) and they also established a working group on cloud evidence. All the 45 States were not convened to that thematic working group, which will discuss the challenges regarding evidence in the cloud (Mauritius is represented). By being a party to the Convention, Mauritius is also contributing to policy making and developing legislation. Membership thus goes beyond capacity-building projects, such as GLACY. Not only the input of signatory members is invited but all those who can make a valuable contribution to the emerging and challenging issues of cloud evidence. All countries need capacity-building.

Cybercrime Program office (CPROC: http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/C-PROC/c-proc_about_CPROC_V4_EN_RO.pdf) based in Bucharest, dedicated to capacity-building programmes on cybercrime. The Romanian government has offered rent-free offices, which allows us to spend more money on project activities.

**How enriching/helpful is it to the Council of Europe to assess the ways in which various signatories are implementing the Budapest Convention?**

By becoming a party to the Convention, commitment to its implementation is entailed. This is precisely what the Convention Committee reviews in terms of challenges at the level of implementation. Since cybercrime and electronic evidence are extremely fast evolving areas, it is important to assess whether the provisions of the Convention respond to the emerging challenges and whether the parties can properly respond to them.

**Can you share with us your views about your experience in Mauritius with the IJLS?**

I must say that it has been an extremely positive experience indeed. IJLS has a very powerful ally in its Chairperson. Each country is different but the legal mandate of the IJLS to provide Continuous Professional Development (CPD) to the criminal justice system at large and the very active participation of the law enforcement agencies in this training is very valuable. It is perhaps due to the powerful leadership of the IJLS that the parties of the criminal justice system are co-ordinating in their judicial training strategy.

In some countries, we witness a more fragmented approach. It is a very important aspect of the continuous judicial training to have such integrated forums. Ideally, training should not be separated and confined to individual institutions. There should be an umbrella of training centres. In most countries, for some time, law enforcement agencies

benefitted from more external assistance in training. This project seeks to redress the balance and prioritises training of the criminal justice system. The project is flexible to local needs and in Mauritius, there is a need for a more integrated approach as observed during the initial assessment of February last year when we visited all institutions (The Data Protection Commission, The Revenue Authority, The Competition Commission) because they also have investigators. The rationale of the introductory course is to train a corps of national trainers and within a structure like the IJLS, I believe they can disseminate the basic knowledge acquired to other institutions of the criminal justice system. The next step is to deliver the advanced course on electronic evidence.

The Chairperson talked about the familiarisation of higher judicial orders (i.e Senior Supreme Court Judges) with such training programs. These are the kinds of needs that we can consider and adapt the national work plan accordingly. It is a two and a half year project which actually started in November 2013 but the project managers were recruited in October 2014, so we will have to work hard to implement everything in time!

---

**Mr Zahid Jamil**

Barrister-at-Law, Gray's Inn, London, UK

Legal and policy consultant in cybercrime and cyber security

Consultant and expert for the Council of Europe on Conventions on Cybercrime

**The fact that only 45 countries have ratified to the Convention, is it not problematic when the need for international co-operation arises?**

At present, 45 countries have ratified to the Convention whereas a couple of years ago only 30 had done so. There is a rapidly growing number of countries which are asking for ratification. Regardless of that, the key element to bear in mind is the relevance of joining. The fact that the United States is a member is in itself a fact and a matter of high significance. As a result, developing countries will naturally be prone to emulate. The efficacy and utility of the Convention coupled with the stature of key signatories as mentioned, irrespective of the number, remains the main motivation and guiding reason which motivates other countries to ratify to the Convention. It is to be noted that ratification to the Convention is open and any country can send a request for accession. It is a process which naturally takes time to be accomplished.

**According to you, to what extent has Mauritius been successful at implementing/adapting to the Budapest Convention?**

I am of the opinion that Mauritius is being extremely forward looking in its approach. The Computer Misuse legislation and the Mutual Legal Assistance legislation bear ample proof to my belief. There is room for improvement and the areas of the legislations which need to be subjected to improvement have been identified over the last few days during the conference sessions. The best thing about the Mauritian legislation is that it is correctly oriented. The mode-

ls on which it is based, that is, the Singaporean and the UK legislations are indeed the right models. Not only is the Mauritian legislation headed in the right direction but Mauritius is far more advanced than many other countries in the region in this subject matter. Quoting the names of countries where the legal framework with regards to the cybercrime issue is not of good standard would be improper. Without any doubt, I can affirm that the Mauritian legislation is a decent and good piece of legislation from a comparative perspective. Amendments are required concerning the Computer Misuse Act, the ICT Act, the Mutual Assistance in Criminal Matters Act and possibly the Copyright Act.

**What, in your views, is the importance of the Budapest Convention?**

- It is the only Convention
- It is truly multilateral
- The technology-neutral language used in the Convention means that there is no expiry date on it.
- It is really global
- The groups who have exclusive access to the data are signatories to the Convention
- It is open to participation from developing countries
- It provides the right structural framework in matters pertaining to:
  (1) offences committed
  (2) procedural provisions
  (3) international co-operation elements
- If there had been a treaty or model law, it would have contained only part 1 and part 2; other aspects would not have been included at all. Taking into consideration these reasons, regardless from the facts related to its substance and quality, the relationships accruing from it render it an excellent piece of Convention.

**Do you think that there will come a time when the level of cybercrimes will exceed that of other crimes?**

I have no idea whether cybercrimes will be on the increase or not but I can say that other crimes will be perpetrated with the continual use of the computer and the internet. In this connection, it is important to make three distinctions namely:

(1) Network-related crimes: crimes against the confidentiality of networks and the availability of networks

(2) Computer-related crimes: computer-related forgery and fraud

(3) Content-related crimes: offline and online crimes

The most important thing to remember is that regardless of these distinctions, most crimes these days will have electronic evidence as an element of investigation or an evidence that needs to be collected with respect to investigation and prosecution of that crime. The Convention, in its procedural powers, does not apply to cybercrime only; it applies to 3 other areas as well namely:

(1) Crimes which are criminalised under the Convention

(2) Computer-related crimes

(3) Any collection of electronic evidence with respect to investigation and prosecution

Therefore, it does not really matter for our purposes whether one type of crime will overtake other crimes. Since our lives are now irreversibly interconnected to technology, the Budapest Convention turns out to be highly relevant and significant in this connection.

---

**Mr Nigel JONES**

Former police officer

Visiting Professor at Canterbury Christ Church University

Independent cybercrime and electronic evidence specialist

**In your views, how often should trainers themselves receive refreshing training sessions?**

A distinction should first and foremost be made between training skills elements and substantive practice. The minimum training expected of somebody to begin as a trainer would be approximately 4 weeks' training. The fact that the Council of Europe is here to deliver training for this limited period is owing to budgetary restrictions and time-related constraints. The 2 days of introductory training sessions were merely an induction meant to introduce delegates to the soft skills of training such as 'good' and 'bad' presentation skills. It is highly important that a more detailed training course is undertaken and if the intention to do so, is felt by individuals, then more formal education and qualification in training will be required.

To come back to the question, once delegates have been subjected to the introductory level of training, the need to refresh themselves will be needed and this is often accomplished by self-teaching. This is carried out with a view to keeping up-to-date with latest materials and information as part of the teaching mechanism in those long-term courses. In terms of their training skills, once individuals have become and are qualified as trainers, there is little need for them to go back and follow remedial training.

In relation to the substantive issues, it depends whether the training they are expected to deliver belongs to their own subject area or not. In the particular context of training over here, a mixed group of trainers was present. If only a specific group, for instance lawyers would have been subjected to training, they would not have benefitted from the experience of the police officers. Likewise, if only police officers would have undergone training, they would not have taken advantage of the knowledge of lawyers. The frequency of following training sessions has a direct co-relational link with the level of familiarity with the subject matter of the course. This course has been incorporated in the IJLS training structure with a view to assembling these individuals coming from different fields as a group and it is indeed an excellent idea. Their skills of delivering a presentation with the input of other trainers have been enhanced. This is

potentially the start of developing a series of training activities that would be progressive. May be future courses on legal issues will be directed only to lawyers. Police officers will be targeted to follow courses based primarily on technical issues.

Trainers who need to be fully conversant with the materials they are going to deliver will have their training pack prepared and geared in such a way that the materials are continually kept up-to-date in the light of latest changes and innovations. However, they cannot be continually trained themselves with regards to their training skills. The important thing to do is to identify people who are capable of delivering the training themselves; the issue of being retrained themselves does not really come up. Trainers should have at least 3 months for enabling them to prepare their training pack because they may need to individualise it and embark on updating exercises. The time to refresh their memory about the subject and in a specific manner is part of their self-training process.

Research has established that 95% of the content of the training is retained by the trainers while they deliver the training to others and the frequency of delivering training to others impacts upon their own skills as trainers. Becoming a good trainer entails a high level of commitment. Bearing in mind the fact that people's interests change over time, we can understand the reason behind a gradual reduction in the number of people actively involved in training.

The important thing about training is not to learn how to train for a fixed period of time but to ascribe to the process an ongoing basis with a view to enabling the detection and assessment/evaluation of the best trainers. The ability to bring changes to one's own presentation in the light of new events and information should be enhanced. The objective of training is to make sure that the delegates obtain the right amount of information and training and thus the overall learning and enrichment of those at the receiving end should be prioritised.

**Do you think that the umbrella of trainers should broaden to other professionals as well? For instance, academics?**

What needs to be done is to look into the training needs to be delivered and identify potential trainers to deliver it. At this level of training, it is not technically complicated. The need to move on towards the creation of more progressive training which might take on more legally technical dimensions as well as the need to bring in outside support (that possesses the required level of knowledge) is indeed felt.

Broadening it to academics and industry as well will indeed be very beneficial and relevant. I used to run the National High Tech Crime Training Centre for the UK police service where I had a mixture of trainers with people from all walks of life. It depends on the deliverables and set targets.

**What are the limitations/constraints that a police officer would face during an enquiry on cases related to digital evidence, taking into account the highly volatile nature of this type of evidence?**

There are 4 main barriers to efficient investigation namely:

(1) Lack of resources

(2) Lack of equipment

(3) Lack of financial resources

(4) Lack of technical knowledge

The problem with policing is the tendency to have a small number of people who have actual mastery and understanding of the issues in cybercrime. The lack of strategic position particularly on cybercrime underscores efficient investigation. Very often, the senior management lacks technical knowledge regarding digital forensics since it is a fairly new issue in comparison with traditional issues involved in police investigation.

This particular lack of knowledge leads in turn to an insufficiency in terms of resources allocation. Coupled with the problem of insufficient and cybercrime-conversant staff is the lack of the right amount of specialised equipment to perform the task correctly. The training required to keep the staff involved up-to-date is also inadequate. Since the training required for forensic examiners is very specific and needs to be done on a regular basis to keep them up-to-date, it is important to invest and allocate sufficient amount of resources to training. Lack of understanding about different softwares (with different requirements and specific purposes individually) leads to an overall lack of efficiency in police investigation with regards to cybercrime cases.

In terms of equipment, the forensic tools are highly expensive and different software packages are required for specific and different purposes. The budget to cater for an increase in staff and equipment should be mapped out over a period of 5 years, for example in the UK. However, in Mauritius, it seems that such a mechanism has not yet been instituted.

Also there is lack of knowledge about cybercrime issues among the general police at grassroots level itself. We must fully recognise the relevance of first responders in cybercrime-related issues at the level of police stations and in this regard, it is important that police officers at all levels are given training about the ways to preserve the evidence collected for further examination. If they fail to preserve the evidence correctly, the consequences will be three-fold namely:

(1) Firstly, evidence that could be potentially beneficial will not be seized due to failure in recognising its relevance to an investigation.

(2) Evidence is seized in the wrong way, therefore leading to a negation of its potential value.

(3) Thirdly, public safety issue might arise owing to failure of seizing potentially dangerous elements that could prove dangerous to the public. The risk level of having public safety issues can be kept in check if there is proper handling of

evidence stemming from adequate knowledge of cybercrime issues. Thus, there is an absolute need to incorporate training on identification and seizure of digital electronic evidence into mainstream training for all new police recruits with a view to enhancing their capacity in looking at events from different angles. Remedial training programmes with regards to digital forensics do not really turn out to be beneficial compared to the implementation of training programmes on the same issues for new recruits.

**Has there been a difference in the training methodology adopted for the training sessions for Mauritius in comparison with those carried out in other countries? Have the sessions been tailor-made specifically for each country?**

The course was developed as a template course in order for countries to be able to adapt themselves. We did not bring specific section-wise changes for each and every country. A session from one of the delegates was incorporated as it was considered beneficial to have somebody from the local scene to address the concerned subject matter. Specific blank space designs were used in some slides so that a future trainer from here can slot information into those slides for training purposes. The objectives of the lesson that related both to the Convention and domestic legislation and the slides that were left blank were part of the template. It was instrumental as a guide for future users/trainers.

The only session that was subjected to real changes is the Electronic Evidence and the reason lies in the incorporation of the session conducted by the police officers. The purpose was to have an insight into the Mauritian situation with cybercrime issues and to increase the knowledge of the prosecutors, lawyers and magistrates attending the training.

The style of delivery was adapted to the interests and needs of the audience and the course appears to have been designed specifically for this particular group of delegates with different skills and backgrounds. The forthcoming advanced course in August will cater more for the interests pertaining to legal knowledge and practical application of the law in an investigative scenario situation.

The idea behind the training course is quintessentially to invite those trainers who actively and efficiently demonstrate their training skills to deliver training in countries that are receiving support from the Council of Europe and subsequently, they will be empowered to join the list of trainers of the Council of Europe, as well as to continue to deliver training as part of a structured programme in Mauritius.

**Mr Ammar Oozeer**
Barrister-At-Law

## The GLACY Project: Cybercrime and Electronic Evidence

Given the threat of cybercrime and the increasing relevance of electronic evidence in criminal proceedings, it is essential that judicial and law enforcement officers have access to relevant training on cybercrime and electronic evidence. In 2009, therefore, the Council of Europe recommended that modules on cybercrime and electronic evidence be integrated into the curricula of judicial training institutions. The GLACY Project is one of the few projects which give effect to the recommendation of the Council of Europe.

### The GLACY Project

GLACY stands for Global Action on Cybercrime. The GLACY Project is a joint project of the Council of Europe and the European Union on Global Action on Cybercrime aimed at supporting countries worldwide to implement the Budapest Convention on Cybercrime. The specific objective of GLACY is to enable criminal justice authorities to engage in international cooperation on cybercrime and electronic evidence on the basis of the Convention.

Mauritius is one of the 6 priority countries selected to benefit from the GLACY Project. The other countries are Morocco, Philippines, Senegal, South Africa, Sri Lanka and Tonga. The project will end in November 2016.

### The Council of Europe Convention on Cybercrime

The Council of Europe Convention on Cybercrime also known as the Budapest Convention on Cybercrime is the leading international convention on cybercrime. The Convention was signed in Budapest in 2001 and came into force in 2004.

Though the Convention was drafted under the aegis of the Council of Europe, it is open to signature by non-members. Four non-EU members participated in the negotiations of the treaty and signed it (the United States, Canada, Japan and South Africa) and as date 6 non-EU members have ratified the Convention. These countries are: Australia, Dominican Republic, Japan, Mauritius, Panama, South Africa and United States of America. Mauritius is the first country in Africa to have acceded to the Convention. It did so on 15 November 2013.

The Convention is not, therefore, strictly a regional agreement. The fact that it has been ratified by non-European countries from different parts of the world suggests that it can be described as a global treaty. As a matter of fact, there is no other international treaty specifically on cybercrime. The Convention is the only binding international instrument designed specifically to combat cybercrime. The Convention is useful as an international standard whether or not a country joins it.

**The expected results of the GLACY Project**

At the end of the project, the following results are expected:

- Decision-makers of project countries are aware of cybercrime threats and rule of law/human rights implications and have identified strategic priorities regarding cybercrime
- Amendments are made to bring domestic legislation fully in line with the Convention on Cybercrime and to improve legislation and regulations on data protection and child online protection
- Enhanced skills for judges and prosecutors regarding cases on cybercrime and electronic evidence
- Enhanced specialised skills and institutions for investigations on cybercrime and electronic evidence
- Enhanced international law enforcement and judicial cooperation against cybercrime based on Chapter III (International co-operation) of the Convention
- Increased public/private and interagency information sharing in line with data protection standards
- Governments are able to assess progress made in the investigation, prosecution, adjudication of cybercrime and cases involving electronic evidence, including international cooperation

**Training for judicial and law enforcement officers – why is it important?**

Electronic evidence may be encountered during the investigation of any offence and it is essential that law enforcement officers have the knowledge and expertise to recognise and handle such evidence, to ensure the effectiveness and fairness of investigations. To this end ,law enforcement officers must be equipped with the appropriate knowledge and skills.

It is essential that judicial officers receive detailed and diversified training and such training must take into account the social awareness and in-depth understanding of different subjects reflecting the complexity of society. The importance which ICTs play in the society today is such that judicial officers (and law enforcement officers) must have at least a basic knowledge of technologies and related issues. For example, in addition to the large number of offences against or through ICT media, an increasing number of other cases which end up in court involve electronic evidence stored on a computer or other electronic or other devices. Therefore, judicial officers must be prepared to deal with cybercrime and electronic evidence.

Following a request by Mauritius to the Council of Europe in 2014, a team of trainers from the Council of Europe conducted a '*Judicial Training Skills and Introductory Cybercrime and Electronic Evidence Course'* at the Institute of Judicial and Legal Studies (IJLS) from 26 to 30 January 2015. Judicial and law enforcement officers were trained to be trainers on cybercrime and electronic evidence. These trainers will in turn train other judicial and law enforcement officers and the first training is expected to be delivered under the aegis of the IJLS in August this year.

The training which focused on the provisions of the Convention is very important because the *Computer Misuses and Cybercrime Act* contains similar provisions as in the Convention. Training skills were also imparted to the partici-

pants. The participants who were not already knowledgeable in cybercrime and electronic evidence did not have any difficulties to follow the course which was conducted expertly by the trainers. Besides imparting a basic training on the different cybercrime offences, the Council of Europe trainers also provided the participants with training skills.

**Inspector H.K Balgobin**
Police I.T. Unit ( Forensic Lab)

**How far has the training by the Council of Europe added to your existing skills?**

We had a good exposure to the Budapest Convention. The training skills acquired will help us in investigating cases more efficiently. The interactions with members of the judiciary helped us to better understand the need to provide specific elements of information related to the digital evidence produced in court for enquiry purposes.

**Do you think that cybercrime training should be provided to the whole Mauritius Police Force to ensure effective handling of cybercrime issues?**

Cybercrime cases are reported at police stations/CCID and elements of evidence are collected at the crime scene by police officers. As such, training on cybercrime will be beneficial to the police department to improve knowledge on electronic evidence, search and seizure techniques. This will contribute to greater efficiency at the level of investigation and handling of digital evidence.

**How difficult is it to handle digital evidence taking into account its volatile nature?**

Digital evidence can be easily tampered if not properly handled. Some evidence are of volatile nature and they can be lost if not properly secured. To avoid tampering/ loss of digital evidence, it should be handled by trained personnel. In the police department, the staff of the IT Unit are trained and equipped to handle and secure digital evidence of volatile nature.

Institute for Judicial and Legal Studies

**Level 7, Happy World House**
**Sir William Newton Street**
**Port Louis**
**MAURITIUS**

+230 213 4710
+230 212 1812

Email: ijls@govmu.org

Find us on the Web:
http://www.ijls.mu/


**Editorial**
**IJLS Intern Team**

## Forthcoming Events

## April 2015

- Lincoln's Inn Workshop
- Conference in Conjunction with l'Association Henri Capitant