WORKSHOP REPORT ON EFFECTIVE CYBERCRIME LEGISLATION IN EASTERN AFRICA
DAR ES SALAAM, TANZANIA, 22-24 AUGUST 2013

Executive summary

Cyber criminals in East Africa take advantage of weaknesses in cybercrime legislation and the nascent systems of law enforcement leading to a proliferation of illicit activities. Like the rest of the African continent, these illicit activities have afflicted the East African region (Burundi, Kenya, Rwanda, Tanzania and Uganda) necessitating the development of international collaborative networks aimed to facilitate proactive crime prevention programmes and the promulgation of effective cybercrime legislation.

The workshop built on the commitment of Eastern Africa states to fight cybercrime and was a collaborative project between the African Centre for Cyberlaw and Cybercrime Prevention (ACCP); the Council of Europe (CoE) and the United Nations African Institute for the Prevention of Crime and the Treatment of Offenders (UNAFRI). With funding from the CoE the workshop was hosted by the United Republic of Tanzania from 22-24 August 2013 at the Peacock Hotel in Dar-es-Salaam.

Identification of the resource persons (Dr Maureen Owor- lead consultant), Mr Sizwe Snail (international co-ordinator) and Mr. Saidi Mashaka Kalunde (national co-ordinator) was undertaken by UNAFRI and ACCP. Dr. Alexander Seger, the Secretary, Cybercrime Convention Committee and also Head of Data Protection and Cybercrime Division in the Directorate General of Human Rights and Rule of Law, represented the CoE.

Participants to the workshop were drawn from middle level civil servants in the police, prosecutions, prisons, judiciary, legislative drafting and other government departments from the East African countries of Burundi, Kenya, Rwanda, Tanzania and Uganda. The choice of participants reflected their influence in developing the framework for effective strategies on cybercrime legislation and enforcement in their countries.

Based on topics that were relevant to the work of the participants, the workshop used knowledge exchange through case studies of domestic legal frameworks to give primacy to local perspectives; analysis of local and regional jurisprudence; the sharing of good practice at the national, regional and international level; and interactive participatory sessions to encourage debate.

The deliberations were candid and exposed the strengths and challenges of developing effective legislation on cybercrime in each state. Delegates noted the varying stages of legislative development in each country, with Kenya and Uganda having a number of laws in place, while Rwanda, Burundi and Tanzania were at early stages in the development of legislation. Each delegation indicated the desire to improve the capacity of their human resources, strengthen collaboration within the national and international frontiers, consolidate the available prospects for modernity and the efficacy of the digital age; and integrate human rights safeguards into procedural and substantive law.

Based on its relevance to Eastern African legislative regime, the Budapest Convention and the work of the Council of Europe formed the background reference materials providing guidance on a range of topics from definitions of cybercrime and electronic evidence to the practicalities of implementing legislation. Participants acknowledged that cybercrime, being 'borderless' and cross territorial by nature, required collective efforts to detect, apprehend, investigate, try and punish offenders. As such, international treaties such as the Budapest Convention offer a good base on which to frame laws that deal with the challenges posed by cybercrime.

The spirit of the Budapest Convention seen in emerging legislation and draft legislation (bills) in Eastern Africa as well as in other sub-regions, and in part of the Draft African Union Conventions on cybercrime, raises the possibility of increased accession to the Budapest Convention by African countries. This predicted accession has meant that Eastern Africa and indeed the entire African continent, is fundamentally geared towards further cooperation within the continent and with the Council of Europe. The workshop called for Member States to take up the call for ratification of the Budapest Convention and domestication of its provisions into local legislation. In this regard, and consistent with their mandates, UNAFRI and ACCP offered to suppport the demands of the Member States in cybercrime prevention and the development of criminal justice strategies.

The resolve of the participants to cooperate with each other to fight cybercrime pointed to their belief in themselves, as the primary resource to take the knowledge on cybercrime and the fight against it to their respective countries. The participants appreciated the value of procedural law and substantive law to facilitate successful prosecution of cybercriminals but also identified the challenges they face within their own national context. Against this background, the workshop participants made the following resolutions:

- ICT technocrats should be invited to future workshops;
- East African states should increase collaboration with the Council of Europe with a view to promote intervention to meet the needs of all African legislative jurisdictions in the matter of cybercrime legislation;
- States should be encouraged to ratify the Budapest Convention and domesticate its provisions;

- Law enforcement agencies should enhance transborder cooperation to promote faster responses to cybercrime through the sharing of information, experience and good practices;
- The United Nations Convention against Transnational Organised Crime, 2000, could be used by states that have domesticated it in the absence of specific legislation against cybercrime;
- States should ratify other relevant regional and international conventions and domesticate their provisions;
- The organisers should increase the frequency of training sessions with longer sessions;
- To promote continuity of participation, participants could form a core East African cyber police;
- States should initiate extradition and mutual legal assistance frameworks;
- States should initiate schemes for compensating victims of cybercrime in criminal justice administration;
- ACCP should conduct research into the status and impact of existing initiatives in cybercrime legislation;
- States should amend their procedural laws to include electronic or other intangible evidence of cybercrime, as opposed to tangible evidence of traditional crimes. It is possible that new forms of cybercrime will often emerge with evolving technology; therefore new cyber laws should be introduced to respond to these rapid changes;
- ACCP should facilitate awareness-raising programmes in the region;
- The organisers and the delegates should ensure prompt implementation of recommendations of the workshop.

Background

The Eastern African region is vulnerable to the emerging challenges of cyber criminal activity as the East African states are at various stages in the development of their cybercrime legislation; sometimes lagging behind other African states in their legislative responses to cybercrime. For example Kenya and Uganda have enacted some laws on cybercrime while Tanzania has a draft Bill for consideration. Rwanda and Burundi still apply their Penal Codes but have no specific law to deal with cybercrime. Yet elsewhere on the continent, there are on-going initiatives at the sub-regional and regional level. For instance the Economic Community of West African States (ECOWAS) has adapted *Directive CIDIR. 1/08/11 on Fighting Cybercrime;* the Southern African Development Community (SADC) has developed model laws on e-commerce and cybercrime. At the East African Community level (EAC) there was a EAC *Legal framework for Cyberlaws EAC 1 and EAC 2*. These initiatives are mirrored at the regional level where the African Union (AU) is in the final stages of preparing a draft Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.

The AU draft Convention, the sub regional initiatives and the legislation of the East African countries (where it exists) are based largely on the Council of Europe's Convention on Cybercrime 2001[1] (herafter 'the Budapest Convention'). The Convention is also a model for cybercrime legislation in European states, the United States of America, Australia, Canada, and Japan. UNAFRI and ACCP support African states in their efforts to develop cybercrime legislation that are harmonised with the Budapest Convention as well as other international and regional legal frameworks.

The relevance of the Budapest Convention to the formulation of effective legislation in Eastern Africa is significant and the workshop was formulated with this fact in mind. The workshop objectives aimed to address the development of effective cybercrime legislation and offer guidance on policy and related responses to the challenges of dealing with cybercrime in the Eastern African region. While being sensitive to state sovereignty, the workshop was intended to help inform state processes that influence the development of legislation that deals with cybercrime. The workshop used knowledge exchange through case studies from each country to give primacy to local perspectives; analysis of local and regional jurisprudence; the sharing of good practice and interactive participatory sessions to encourage debate.

To facilitate the workshop were: Dr Maureen Owor (the lead consultant), Mr Sizwe Snail (international co-ordinator of ACCP); Dr. Alhas Maicibi (representative of ACCP; Mr. Saidi Mashaka Kalunde- ACCP national co-ordinator for Tanzania); and Dr. Alexander Seger, the Head of Data Protection and Cybercrime Division of the Council of Europe.

Participants to the workshop were drawn from middle level civil servants in the police, prosecutions, prisons, judiciary, legislative drafting and other government departments from the five East African countries. The choice of participants reflected their influence in promoting the benefits of the training workshop as trainers and creating the desired multiplier effect in their countries. A list of the participants and their contact email addresses is attached to this report.

The rest of the report sets out a summary of each of the sessions in the order of appearance.

SESSION 1: Opening Formalities

Chair: Mr. Said Mashaka Kalunde (ACCP National Coordinator, Tanzania).

This session covered welcome remarks, the introduction of delegates (participants), the formal opening of the workshop and a presentation of the status of legal and policy responses at the national level by country delegations.

[1] The treaty seeks to address computer crime and internet crimes. It was adopted by the Committee of Ministers of the Council of Europe at its 109th Session on 8 November 2001, opened for signature in Budapest on 23 November 2001 and entered into force on 1 July 2004.

Representing the host country, Mr. Said Kalunde welcomed participants to Tanzania and emphasized the need for working together as a region because of the transnational nature of cybercrime. He thanked the Council of Europe, UNAFRI, ACCP, and Government of Tanzania for organising and facilitating the workshop. He then introduced the facilitators, paid tribute to them for supporting the East African states in their development of cybercrime legislation and called upon the participants to use the available technical support provided by the facilitators during the workshop. Mr Kalunde then called upon Dr. Seger, Mr Kisembo and Dr. Maicibi to make their opening remarks.

A. Dr. Alexander Seger (Council of Europe www.coe.int/cybercrime)

Dr. Seger pointed out that much work had been done towards the development of cybercrime legislation in the other regions except Eastern Africa. There was now a new focus on the utilisation of African institutions like the UNAFRI and ACCP to build capacity in the training of personnel in law enforcement and criminal justice. He stressed that crimes today have some form of electronic evidence –related not only to computer but in many other electronic devices which called for specialized knowledge of a special group of people to focus on complications involved in committing crime electronically. Examples include the specialisation in forensic data protection. He expressed hope that at the end of the workshop, participants would have identified their national and regional needs for technical assistance available from institutions and experts specifically from Council of Europe whose links have been extended to cover Japan and USA.

Dr. Seger explained that ICT facilitates economic development and rule of law. However, economic development must follow a legal framework as a safeguard from misuse and abuse. Therefore it was important to develop legal frameworks and in this regard the Council of Europe was willing to assist states.

B. Mr. John Kisembo- Acting Director, UNAFRI

Mr. Kisembo paid tribute to Mr. Saidi Kalunde and the Government of Tanzania for facilitating and hosting the workshop, the CoE for funding the workshop and the facilitators and participants for their commitment. He gave a background to the establishment of UNAFRI as a regional mechanism to assist African states in their response to unique problems of crime and the impact that crime poses on socio-economic development. He explained that as part of its mandate, UNAFRI collaborated with individual experts and institutions as a result of which the ACCP was established. He emphasised the value of collaboration among institutions and individuals to help develop the capacity to respond to common threats and challenges of cybercrime. Mr Kisembo assured participants of the commitment of UNAFRI and ACCP to the provision of technical support to African countries and institutions. He assured participants that the workshop was the beginning of the long consultative process to harness the knowledge and expertise needed to spur the growth of systems and mechanisms that will help make the Africa region safe from cybercrime.

Dr. Alhas Nok Maicibi- representative, ACCP

Dr. Maicibi described the significance of the electronic devices in the economic development of countries by way of helping states exploit their abilities and resources for growth. However, such devices, he cautioned may also be used by criminals to perpetuate illicit activities. He gave a background to the formation of ACCP including details of its management and administrative structures. He expressed the apologies of Dr. Chawki Mohammed a co-director of ACCP who could not attend the workshop due to other pressing professional commitments. Introducing the ACCP officials present, Dr. Maicibi called upon all participants to seek professional expertise and utilise ACCP to the maximum. He invited participants to publish their articles with the African Journal of Crime and Criminal Justice as a platform for the dissemination of scholarship on cybercrime. He urged participants to beseech their countries to become signatories to regional and international conventions on cybercrime. He hoped that the next round of workshops will focus on enforcement of cyber law, noting that exogenous cyber crime can easily be tamed and dressed in African fashion to enable its content to be understood by those least knowledgeable in Africa.

Session 2: The state of cybercrime legislation in Eastern Africa- an overview

Chaired by Dr. Alhas Maicibi

In this session, the delegations from each country presented a report on the development of cybercrime legislation, the policy and regulatory framework; the criminal justice system and any challenges faced in the development and enforcement of laws on cybercrime. Some delegations also made reference to the status of cybersecurity in their countries. Proposals on reform are covered in Session 8.

1. BURUNDI

Cybercrime is relatively new in Burundi. Although there is no specific legislation to criminalise unlawful cyber crimes, the Penal Code has provisions on electronic transactions. On 29 April 2009, Burundi adopted a new Penal Code which took into account the new criminal phenomenon of cybercrime.

The development of information technology has had consequences which are exemplified in a new kind of crime - cybercrime. Previously, the Criminal Code of 1981 did not punish intrusive behaviors in computer systems and data such as cases of forgery and use of forged material through computer including the modification or destruction of stored data, treated or transmitted by a computer system, and the unauthorised access to a computer system (hacking).

Presently, there is a draft bill on electronic signatures and its authentication, consumer protection, privacy, data protection, computer crime, banking and taxation and information security elements. The Bill is now being scrutinised by the Ministry for Justice to assess its compliance with existing laws. Burundi's criminal law was amended in 2010 by this Bill in areas such as cybercrime (computer-related crimes). Cybercrime includes common law offenses to which IT (information technology) is a simple tool. However, although the Criminal Code does not provide for offences that may be committed using the internet such as theft, fraud, slander, blackmail and harassment, racial aversion, sabotage, and the dissemination of child pornography, the general principles of criminal law are applied.

For instance, under the Burundian Penal Code:

> "Whoever commits forgery, introducing a computer system, modifying or deleting data that is stored, treated or transmitted by a computer system, or changing by any technological means possible use of data in a computer system and thereby alters the legal implications of such data, shall be punished by imprisonment of five to twenty years and a fine of fifty thousand to one hundred thousand francs. Whoever makes use of data obtained, knowing that it is false shall be punished as if he were the author of the falsity".

Challenges:
As cybercrime legislation is new in Burundi, it has unique challenges. Suspects for instance, frequently act anonymously and cover their tracks, and new criminal activities are spreading rapidly and widely through the online avenues of crime. Other challenges posed by the cybercrime legislation and its prosecution are specifically linked to the establishment of evidence of cybercrimes. The collection of evidence is complicated by the intangible nature of cyberspace and the degree of sophistication required of investigators in the detection and observation of criminal acts by agents. The transnational nature of cybercrime adds to the difficulties involving the need for legislative harmonization and cooperation of international investigation services.

Burundi is considering specific interventions with a focus to address the challenges imposed on their country by cybercrime.

2. KENYA

The government of Kenya formed a committee in June 2013 to spearhead efforts against cyber crime under the **Communications Act of Kenya**. By this Act, war was declared on cyber criminals with stiff penalties prescribed for unlawful acts like cyber hacking, and cyber bullying. The Act aims to protect the government within the overall system of ICT as the engine for e-commerce and e- governance to safeguard development.

Technically, **Kenya Information and Communications Act** hosts the electronics and transactions law. This legislation also provides for cyber crime in Kenya and has provisions on mobile money transactions. The Act complies with the regional convention-the AU Draft Convention on Cybercrime. The provisions under the part of the Act on electronic transactions include—

- Unauthorized access to computer data;
- Access with intent to commit offences;
- Unauthorized access to and interception of computer service;
- Unauthorized modification of computer material;
- Damaging or denying access to computer system;
- Unauthorized disclosure of password;
- Unlawful possession of devices and data;
- Electronic fraud;
- Tampering with computer source documents;
- Publishing of obscene information in electronic form;
- Publication for fraudulent purposes; and
- Unauthorized access to protected systems.

Significantly, the **Evidence Act** also introduced amendments which allow for admissibility of electronic evidence and the conditions for storing, preservation and presentation of electronic evidence. Therefore, the question of primary or secondary evidence does not arise; rather the emphasis is on the weight or the relevance of the electronic evidence. There are also other laws that deal with cyber crime such as the Central Depositories Act, and the Penal Code among others.

With regard to prosecution, Kenya still relied on physical evidence but not electronic evidence. Developments reflect the problems regarding electronic evidence and the focus on police and prosecutions. The delegation made other suggestions regarding the challenges faced in handling cybercrime as well as strategies for their realisation.

3. RWANDA

Cyber law is included in Rwanda's Organic law. Under the Penal Code, section 5 refers to computer related crimes. The penalties include the payment of fines of between 5 to 7 million Rwandese Francs. Recidivists are also punished with the same penalties. There are no specific legislations to deal with cyber crimes, but these will be developed in due course.

Rwanda hopes to benefit from the workshop through collaboration at the local, regional and international levels on how to streamline legislation on cybercrime in Rwanda. Rwanda expects that the workshop will help participants analyse current and draft legislation of participating countries in terms of their consistency with the Budapest convention on cybercrime; the rule of law; and elements of cybercrime enforcement strategies. It hopes the workshop can outline further activities and assistance to be provided in the period 2014 - 2016.

Rwanda is looking for ways in which the challenges of cyberlegislation deficiency can be addressed.

4. TANZANIA

There is no specific law on e-commerce in Tanzania as yet. However, there is a draft bill on cybercrime control which is being discussed by a variety of stakeholders. At the same time, a wide consultative framework has been opened to discuss ways of guiding and informing the process of legislation. The legislation is expected to be comprehensive and effective. This presentation is in respect of Tanzania's position on cybercrimes. In this report we will address various aspect of cybercrimes laws in Tanzania as hereunder indicated.

Background

Tanzania like many other countries has been operating its business of affairs manually for quite a long time. However due to advancement of science and technology the world has moved to electronic means of conducting affairs such as bank transactions, communication, record keeping etc. Despite these developments, there has not been a matching change in the legal framework. Even electronic evidence was not admissible in court until fairly recently when the High Court in an unprecendented move, admitted electronic evidence for the first time in the case of *Trust Bank Tanzania Ltd V Le Marsh and Others*[2]. This move subsequently triggered the amendment of our evidence Act (TEA) to permit admissibility of electronic evidence.[3]

Organizational interest

From an organisational perspective, it is inevitable for an organisation to embark on the fight against cybercrime and in the process to layout relevant infrastructure to curb the scourge. The basis of this assertion is built on two main reasons among others which are economic and security reasons. Without a legal framework to prevent cybercrimes even the normal living expenses will escalate. The investors will not be at ease to invest here. However if they do, they will operate at a high cost due to the risks involved as long as they transact electronically, something which is a way of life nowadays, but conspicuously missing supportive cyber-legislation. The price will be paid by Tanzanians in one way or the other if they invest here or otherwise.

On the other hand, virtually all communication and most of the issues dealing with collaboration and transacting business are happening and being handled electronically through the internet. The government needs to be in full control so as to take measures for safeguarding transactions of the cyber-community for the sake of security. If the law does not mandate the authority to the government on steps to be taken on certain issues of criminal nature and since we are keen to observe the rule of law, the country might be

[2] Commercial Case No 4 of 2000.
[3] Section 40A of Tanzania Evidence Act Chapter 6 of Tanzanian Laws.

in chaos. The government has an inalienable duty to keep pace with the emerging technological advancements.

Legislation: presently, Tanzania is in the process of enacting three laws in line with Cybercrimes. The draft Bills are: **the Computer Crimes and Cyber Crimes Bill, the Data Protection and Privacy Bill and the Electronic Transactions and Communications Bill**. The Computer Crimes bill has twenty one (21) cyber offences under part II. The offences range from illegal access, pornography to computer related forgery, etc. Further the Bill has procedural aspects which define search and seizure, assistance in investigation under part V as well as making all offences under it extraditable under part III. **The Data Protection and Privacy Bill** has provisions on the weight and admissibility of electronic evidence. In the interim, there is the **Electronic and Postal Communication Act No 3 of 2010 (EPOCA)** which has elements of cyber offences including illegal interception. The act is meant for regulation of mobile communications (mostly mobile phones).

Challenges: Tanzania is desirous of embracing current trends in the fight against cybercrime, but the country still face a number of challenges, as specified below:
-No specific laws on cybercrime which complicates the process of prosecution;
- Insufficient capacity in investigation, enforcement and legislation;
- Lack of a joint platform for legislature mechanisms, national enforcement and criminal justice systems;
- The police do not have skills to conduct electronic investigations – as a result of which electronic evidence gets contaminated;
- Absence of a definition of electronic evidence for application in courts;
- Lack of awareness among the general public about cybercrime;
-The general cyber community is not sensitized to the nature of infiltration by criminals.

Tanzania shared their roadmap to cyberlegislation whose component aspects included, strategies, steps to be taken, areas of need to technical support and proposals.

5. UGANDA

Cyber security is a relatively new field as its study is directly related to the rise of digital technologies. This also means that cyber security has evolved apart from most other concepts of security. This notion of security includes protection from disruptions in confidentiality, integrity, availability and often non repudiation of digital technologies and information.

Uganda has recently passed three laws related to the EAC Legal Framework: the **Computer Misuse Act, 2011, the Electronic Transactions Act, 2011 and the Electronic Signatures Act, 2011.**

The Computer Misuse Act is the principal legislation covering cyber crime. It provides for the safety and security of electronic transactions and information systems, the prevention of unlawful access, abuse or misuse of information systems including

computers and for securing the conduct of electronic transactions in a trustworthy environment. The act creates offences with respect to the unauthorised use, access, abuse of computers or data. It also has provisions on electronic fraud, child pornography, cyber harassment, cyber-stalking.

The Electronic Transactions Act provides for the use, security, facilitation and regulation of electronic communications and transactions as a functional equivalent to the already existing forms of communication. The Act gives legal certainty in respect of validity, legal effect and enforceability of information in electronic form with respect to relations between parties especially establishing contractual obligations. In 2007, prior to the enactment of this Act, the High Court in *Hansa, Emmanuel Onyango vs Aya Investments Ltd, Mohammed Hamid* relied on the exchange of emails between the parties to determine the contractual relations.

The Electronic Signatures Act 2011 provides for the use of electronic signatures and their regulation. All the three laws have been published and are now in force.

The principal player agencies are: the Ministry of Information Communcation Technology, the Uganda Communications Commission, the National Information Technology Act-Uganda (NITA-U), the Uganda Police Force; and the Judiciary.

As a country, we have gone further to set up a Computer Emergency Response Team (CERT) with all the aforementioned Government agencies being represented on the committee. The Uganda Communications Commission (UCC) has set up its own CERT to compliment the national team and this was set up on the 6th of June 2013.

This CERT prowls the Internet to monitor and report hi-tech crime including cyber terrorism, computer intrusion,online sexual exploitation and cyber fraud. The team also coordinates all other multi sectoral agencies in this fight against cyber crime; liaises with other law enforcement agencies in the prosecution of cyber related crimes and collaborates with other regional and international agencies with similar remits.

Overview of statistics on cybercrime (Uganda Police Crime Report 2012)

Cyber crime has increased by 14.9% from the previous year. The report indicates that cyber crime focuses on mobile money and Automated Teller Machines (ATM) fraud. MTN alone has transacted through its Mobile Money service a total of US$245 million. Cyber crime targeting Mobile money and ATMs accounted for a loss of over $1million country wide. Around $100,000 was transferred without the knowledge or authority of telecom service providers between August and November of 2012. Despite the challenges attributed to crime statistics, the figures reported above are a pointer towards the seriousness of the problem of cybercrime and the danger posed to electronic transactions.

Challenges:

Despite the colossal amounts involved in the Mobile Money transfer service, there is no statutory framework governing the transactions. The mobile network operators have no

obligations to report or disclose info on mobile money services to Bank of Uganda (BOU) as a regulator.

There is a general lack of capacity among the police and other law enforcement agencies to detect,investigate and assist in prosecution under the Computer Misuse Act 2011. This has been a challenge in the prosecution of some high profile cases in the country like *Uganda Vs Kato Kajubi* and *Uganda Vs Dr. Aggrey Kiyingi* cases that relied on electornic evidence. In *Kato Kajubi* following a retrial, the accused was convicted. Following the terrorist attack on Kampala on 11th July 2010, the police with the help of the FBI were able to uncover emails linking the bombings to the suspects.

There is lack of capacity and funding to enable special skills training required to counter the ever evolving and increasing cyber crime nationally and globally. Uganda does not have adequate data protection laws. Across the East African sub region and the African contintent, there is a lack of a harmonized legislative regime to tackle cybercrime. Finally, there is insufficient knowledge about the law and inadeqauate sensitization of the public and other potential victims of cybercrime.

SESSION 2: International perspectives- Budapest Convention 2001

Facilitator: Dr. Alexander Seger (CoE)

Dr Alexander Seger set out the background to the CoE including its corporate identity and the details of its governance structure and the 12 signatories to the Convention. The CoE has a current membership of 39 parties (35 in Europe, and includes Australia, Japan and the USA). Despite its appearance as a European treaty, the scope of the CoE is global given the inter-territorial nature of its vision to fight cyber crime. As such, the treaty is open for accession by any state. Any country requiring entry should write through its Ministry of Foreign Affairs to the CoE expressing interest. This is followed by consultations and initiation to accede. For instance, Mexico's application 6 (six) years ago is still being processed. The first phase involves a political process requiring an assessment of the country's status. To date, some 39 countries have ratified the Budapest Convention including some African countries.

The Convention aims principally at:

1. harmonising the domestic criminal substantive law elements of offences and connected provisions in the area of cyber-crime.
2. providing for domestic criminal procedural law powers necessary for the investigation and prosecution of such offences as well as other offences committed by means of a computer system or evidence in relation to which is in electronic form.
3. setting up a fast and effective regime of international co-operation.

The following offences are defined in the Convention: illegal access, illegal interception, data interference, system interference, misuse of devices, computer-related

forgery, computer-related fraud, offences related to child pornography and offences related to copyright and neighbouring rights. The Convention also sets out procedural law issues such as expedited preservation of stored data, expedited preservation and partial disclosure of traffic data, production order, search and seizure of computer data, real-time collection of traffic data, and interception of content data. The procedural issues refer to:

i) Criminalising conduct, by which process crimes targeted include; illegal access, illegal interception, data interference, system interference, misuse of devices, fraud and forgery and child pornography
ii) procedural tools for litigation include expedited preservation, search and seizure and interception of computer data
iii) international cooperation among the signatories to the treaty to facilitate extradition of suspects, mutual legal assistance in apprehension and management of identified cases, spontaneous information to facilitate judicious action on cases, expedited preservation to get the evidence at required time with the promptness necessary; mutual assistance for interception and accessing computer data.

Functioning of the Budapest Convention

1. Standards: Budapest Convention and related instruments are a measure of global standards in the fight against cybercrime;
2. Capacity building / technical cooperation programs are available on request to assist countries that are signatory to the convention;
3. Follow up. The convention acts as a checklist to its signatories and other countries that would like to make legislation consistent with its provisions as they compare with the local legislations. It offers a guideline which some countries have followed in their legislation. These include Uganda, the Computer Misuse Act of 2011 which relates to Article 5 of the Convention.The process is a dynamic mechanism of relationship between countries.

Every word in the convention has a purpose. The convention has corresponding aspects for relating to specific laws in countries. It can therefore assist countries as a check list for inclusion of the significant elements of existing laws and upcoming laws. Facilitation to countries includes technical assistance in capacity building in the development of cybercrime strategies in legislation and safeguards, financial investigation, private-public partnership, judicial training international cooperation, and the protection of children. Capacity building tools include electronic evidence guide, first responder training pack, and judicial training covering introductory and advanced courses. CoE supports the training of trainers across the world.

Impact of the Convention

The Budapest Convention is known as a tool for stronger and more harmonized legislation with the under mentioned influences:
-More efficient international cooperation between parties.
-better cyber security performance

-Council of Europe is a catalyst to capacity building efforts
- A tool for better investigation, prosecution and adjudication of cyber crime and e-evidence cases.
- develop trusted partnerships and public/private cooperation
-contribute to human rights/rule of law in cyber space

Dr. Seger noted that the political considerations often determine the momentum of cooperation. The adoption of the convention takes into account the sovereignty concerns of countries and requires that each party is at liberty and has the ultimate discretion on the matter of cooperation. No country is coerced nor rushed into cooperation.

Benefits of the ratifying the Convention

- Trusted and efficient cooperation with other parties
- Participation in the Cybercrime Convention Committee
- Participation in future standards setting (Guidance Notes, Protocols and other additions to Budapest Convention)
- Enhanced trust by the private sector
- Availability of technical assistance and capacity building

Dr Seger added further that the only envisaged "cost" paid in acceding the convention is 'commitment to cooperate'.

Plenary discussion:

Tanzania sought to know the balance between human rights and cyber crime control measures. In response, Dr. Seger referred to Art 15 of the Convention which responds to these concerns, emphasising that governments have a positive obligation to protect their populations against cyber crime. He cited a case of pornography in Finland as a case study. He stressed that The Budapest Convection applies to criminal investigations and not national intelligence operations from a point of view of rule of law, human rights and politics.

Kenya observed that the drafting of laws can also provide for relevant safeguards to protect but also limit rights contained in the relevant sections of the Constitution.

SESSION 3: Cybercrime and electronic evidence –definitions, trends and threats

Facilitator- Dr. Maureen Owor (ACCP)

Dr. Owor set out the objectives of the sessions namely: to develop an understanding of the contested notion of cybercrime and electronic evidence; appreciate current trends and the threats of cybercrime at the national and regional level. She then gave an overview of the impact of cybercrime following the growing use of electronic devices in

Africa's hinterland. Referring to recent figures on cybercrime Dr. Owor pointed out that in Uganda alone, cybercrime was responsible for the loss of about 1.5 billion Uganda shillings in mobile money fraud. News paper reports from the UK show that old computers are being sold to companies that ship them off to Africa where the data stored on the computer is used for illegal activities (Josie Ensor and Richard Gray "How your old computer may be on its way to Africa's online fraud capital" *The Telegraph* 25 Nov 2012). Africa is facing an escalation in cybercrime. Although the term (cybercrime) is gradually entering formal legal terminology due to the harmonising influence of the 2001 COE Cybercrime Convention to describe computer misuse legislation (Wall, 2008, 863) some questions remain: how do African states define cybercrime and electronic evidence?

The participants broke out into three groups to discuss the definition of cyber crime and electronic evidence, as well as the trends and threats. Here are the results of the group discussions.

Group I:
Cybercrime is an unlawful act committed by an individual using an electronic device. The important elements to be considered in the definition of cybercrime include the facts that show an unlawful act takes place, the unlawful act is defined in law and the act should involve use of an electronic device or a computer.
Electronic Evidence: refers to non- physical or non-tangible evidence and includes data available in cameras, computers, Sim cards and other electronic data.
Trends: Africa has recorded an increase in crime attributed to electronically related threats for instance in Kenya and Uganda in M-pesa and other mobile money tansactions. This problem is widespread in the other East African countries as well.
Threats: include cyber fraud, copyright infringements, bullying and pornography.
***Sources*:** ACCP reports, CoE Electronic Evidence guide

Group II
Definition of cybercrime: there was a visible lack of consensus on the definition of cybercrime. The range of opinions covered cybercrime as a state in which there is a deliberate compromise of reasonable safety to cybercrime as any crime committed using electric device.
Electronic evidence: citing the example of the Kenyan law, electronic evidence was described as any record attributed to electronic devices
Threats: cybercrime is multiplying with high levels of proliferation that exceeds the capacity of individual states to tackle effectively.
Trends- the growth in the use of electronic devices has led to increasing vulnerability of people.
Sources: Budapest Convention, Kenyan laws, websites.

Group III
Definition of cybercrime: there are several definitions each being context specific. Generally the definition relates to offences committed with the use of a computer, a phone and internet networks.

Electronic evidence: electronic evidence originates from the drives of electronic devices or computers and may be volatile (retrievable) and non- volatile forms of electronic evidence.
Threats: threats include: cyber crime attackers committing economic crimes which affect the population. There is also a potential for the commission of political crimes with serious governance consequences. Cybercrime can cause damage to computer systems through virus attacks (sabotage).
Trends: there is a growing trend towards the criminalisation of cybercrime through legislative processes. Equally there is a growing need for the harmonisation of laws that are based on the Budapest Convention.
Sources include works by Professor Eugene, works by Professor Muchome (University of Dar Es Salaam) and *The Daily News* of Tanzania**.**

Plenary discussion
Dr. Owor appreciated the input and passionate involvement of all participants in their various groups which had contributed to their exposure to the subject. She pointed out that although the definition of cybercrime is still contested, cybercrime is used today to describe the crimes or harms that are committed using networked technologies (Walls 2008). As a functional definition it identifies general offence categories to be enacted in domestic penal legislation (Weisman, 2005, UN 1995). The CoE convention for instance uses the term 'cybercrime' to refer to an assortment of criminal activity including offences against computer data and systems, computer-related offences; content offences and copyright offences. Participants observed that the challenges of a legal definition limit the ability to identify crime which in turn leads to the problem of creating clear guidance or benchmarks to guide law enforcement agencies on how to identify cybercrime. It was pointed out by Kenya that one could use a General Interpretation Act to assist in interpretation of terms.

The discussion turned to the reliability of statistics. Dr. Owor pointed out the problems of relying on a legal definition of cybercrime that may cover a limited number of acts like computer misuse. There was also the issue of under reporting of cybercrime and over reliance on police-recorded statistics that have disparate methods of counting cybercrime. Participants noted that despite these shortcomings statistics are the basis of compiling crime trends. Admittedly, a lot of crime is not reported to police for various reasons. The need for a data bank was highlighted because without it, crime data will remain fragmented making the process of information sharing difficult.

Based on practices from Germany and the UK, participants noted the need for wide consultations to help identify the trends of cybercrime. The digital divide has also added a new dimension to the difficulties of identifying trends of cybercrime. For some people who do not use computers, cybercrime and electronic evidence may seem to be an abstract phenomenon.

The issue of electronic evidence led to technical questions from Tanzania on the status of computer or email print outs- whether courts should treat them as primary or secondary evidence. Participants were reminded by Dr Seger to include all sources of

electronic evidence like computer data, traffic data, internet data and subscriber data. The latter must be singled out. Other technical issues raised by Rwanda and Burundi were related to situations where the retrieval of subscriber data is blocked by a state and where it is impracticable to locate the offender.

Participants discussed the following threats to electronic evidence which include the careless handling of e-evidence which compromises its authenticity; inappropriate procedures for searching, securing, locating electronic evidence may lead to an infringement of a suspect or any third party's rights; lack of appropriate storage facilities and transportation may cause loss of evidence; poor storage practices due to low technical capacity; and routine deletion of data as well as deletion that is intended to destroy evidence.

Other threats to electronic evidence identified include: the ad-hoc reform of evidence laws which may not map onto the reality of the changing nature of electronic evidence; the stringent evidential rules on admissibility, reliability, evidential weight of evidence, its relevance and the hearsay rule. Other threats include defences like the Trojan horse defence (cybercrime was committed by a malware worm or virus or other programme but is not attributed to individual criminal liability. A restrictive approach of judges in their admission of electronic evidence may make it hard to prove cybercrime (Murungi 2011).

SESSION 4: Cybercrime legislation – substantive criminal law

Facilitator: Mr. Sizwe Snail (ACCP)

Mr. Snail began his session with a discussion of specific articles of the Budapest Convention and illustrated their relevance to the cyber crime legislation in African countries. He discussed those provisions of the convention relating to computer generated offences that could be of use in the cybercrime laws in Africa. These include provisions on content-related offences, infringement of copyright and related rights/intellectual property, patents, trademarks and domain name. Some sections like Article II on aiding, abetting and attempting to commit a crime refers to the liability which attracts a sanction. He also pointed out the relevance of Article 12 on corporate liability to African states.

Computer crime is a new type of criminal activity which started in the early 90's as the Internet became a common place for online users worldwide. Defining Cyber crime as any criminal activity that involves a computer he categorised the crime as one which deals with crimes that can only be committed which were previously not possible before the advent of the computer such as hacking, cracking, sniffing and the production and decimation of malicious code. The other category of computer crimes is much wider and have been in existence for centuries but is now committed in the cyber environment such as internet fraud, possession and distribution of child pornography.

The next part of his discussion looked at the response by African countries to cyber law and cybercrime followed by a discussion of the ongoing legislative process in Tanzania as an example of legislation that is largely consistent with the provisions of the Budapest Convention. Mr Snail described several initiatives in the various sub regions of Africa that respond to cybercrime. For example, in East Africa, the EAC had a legal framework for the legislation on cybercrime for Eastern Africa. In 2009, ECOWAS adopted Directive CIDIR 1/08/11 on Fighting cybercrime. Elsewhere, the SADC countries had developed model laws on ecommerce and cybercrime.

Mr Snail examined the provisions of the Draft AU convention which proposes amendment to existing laws and draws on the salient features in the Budapest Convention though it gives an African dimension. The AU draft convention covers the following aspects: attack on computer systems; content-related offences; communication technologies; offences related to electronic messages; security measures and offences specific to IC Technologies. The rest of Mr Snail's presentation examined Tanzania' draft Computer Crime and Cybercrime Bill 2013 and gave an overview of its substantive provisions with a highlight of unique provisions like that on Territorial Jurisdiction.

SESSION 5: Procedural law – Part I: investigative powers, safeguards and adducing electronic evidence

Facilitators: Mr. Said M. Kalunde and Dr. Alexander Seger

Mr Saidi Kalunde started with an overview of the procedural law on cybercrime defining these as rules that prescribe the steps to be followed in investigative and prosecutorial duties that are judiciously enforced, and the methods for enforcing rights and duties as a set of established forms for conducting a trial and regulating the events that precede and follow it. He detailed the legislative measures necessary to establish powers and procedures on specific criminal investigations or proceedings. The procedural laws include legislative measures which are necessary to establish the powers and procedures relating to: offences established in accordance with the cybercrime legislation; other criminal offences committed by means of a computer system, and the collection of evidence in electronic form of a criminal offence.

With specific reference to relevant provisions of the Budapest Convention, Mr Kalunde outlined the intersection of specified practices consistent with the procedural law provisions as recommended by the Task Force of East African Cyberlaw Framework - the body of law that prescribed formal steps to be taken in enforcing legal rights in the Eastern Africa region. He detailed the sections which gave legitimacy to the development of effective but balanced procedural Instruments which enable competent authorities to order for the lawful collection of traffic data and the lawful interception of content data; assist law enforcement to use sophisticated investigation instruments such as key-loggers and remote forensic software, to collect passwords used by suspect, or to

identify connection used by a suspect; Limit use of sophisticated instruments to serious crime cases. No procedural instrument should interfere with a suspect's internationally or regionally accepted fundamental rights.

Mr Kalunde discussed the measures that have been recommended by the EAC Cyberlaw task force. The measures address the need for capacity of law enforcement agencies to obtain/access forensic data in investigation. The task force also recommended that the ICT impact on crimes in the region be given due consideration and that partner states should undertake reforms of substantive and procedural law which the East African Community Secretariat considers necessary. The five partner states should consider the role of the East African Court of Justice in addressing the multi-jurisdictional nature of computer crime and the adoption of common criminal procedures within the eastern African region. States should pay special attention to the wording and provisions of the Council of Europe Convention on Cybercrime (2001) and consider the possibility of acceding to the Convention.

Dr Alexander Seger gave an overview of the procedural provisions of the Budapest Convention (Articles 15-22). He discussed provisions of the Uganda Computer Misuse Act and the Tanzania draft Bill to show ways in which the provisions adhere to or differ from the Convention and the areas of procedural innovation. With reference to the relevant provisions of the Budapest convention on search and seizure, Dr. Seger emphasised the development of effective but balance procedural instruments which enable authorities to facilitate evidence gathering, investigation, order expedited, preservation, regulate seizure and search, order for lawful collection of traffic data, assist law enforcement to use sophisticated investigation instrument, limit use of sophisticated instruments within the parameters of the rule of law and human rights of the parties.

Session 5 Procedural law – part II

Facilitator: Mr Sizwe Snail

Mr Snail gave a broad overview of how South African law dealt with cyber crime from a common law perspective. He also outlined the consolidating effect of the new cyber crime provisions contained in South Africa's Electronic Communications Transactions Act, Act 25 of 2002 in the prosecution of cybercrime. The presentation focused on the statutorily defined crimes and the provisions on the value and evidential weight of electronic data during criminal proceedings. The presentation also covered the powers of 'Cyber inspectors'. The ECT has given South African Court's broad jurisdiction when adjudicating cybercrimes due to its borderless nature.

Mr Snail stressed that ICT crime has to be tackled with a more sophisticated multi-disciplinary including a focus on protecting both the 'container' of valuables (the computer is merely the modern equivalent of a bank vault), as well as the value - money or gold it contains data). On appropriate laws to be applied in a prosecution he described the relevance of **c**ommon law position which (prior to the ECT Act) could be

extended as widely as possible so as to cater for the arrest and successful prosecution of online offenders. In illustration, he gave a number of cases judged in South Africa relating to identified aspects such child pornography. The applicability of the common law however has its own limitations particularly when dealing with online crimes involving assault, theft, extortion, spamming, phishing, treason, murder, breaking and entering into premises with the intent to steal and malicious damage to property.

In conclusion, he observed that most of the cyber crime provisions in the ECTA seemed to cover the known types of cyber crime. His view was that the legislature did not make cyber crimes an abstract concept of legal writing, creating crimes after the advent of the computer, but also before the advent of the computer, stressing that a mere attempt to commit these crimes is a criminal transgression. South Africa, Nigeria and Egypt have developed legislation to deal with these new crimes whose enforceability is still being tested in courts of law. As such some legal practitioners and adjudicators (magistrates and judges) need to be educated and conditioned to embrace the cyber crime provisions of the ECTA. Given the borderless nature of the internet and the challenges it poses in terms of jurisdictional questions, international co-operation and uniformity, it is of the utmost importance that states learn from each other's efforts to deal with cybercrime and create an international cyber crime code to be applied universally if any major success is to be achieved in combating cyber crime. This is vital to Eastern Africa where efforts to formulate effective cybercrime legislation are in advanced stages.

SESSION 6: Developing an effective criminal justice strategy on cybercrime and electronic evidence

Facilitator: Dr Maureen Owor

Dr Owor recapitulated the learning points of the previous sessions before setting out the objectives for session 6. The objectives were to enable participants understand the justification for an effective cybercrime strategy on cybercrime and electronic evidence, appreciate the elements of an effective criminal justice strategy and evaluate case studies on criminal justice responses.

The criminal justice system was defined as the system of law enforcement involved in apprehending, prosecuting, defending, sentencing and punishing suspects or those convicted of a crime (Oxford dictionary). Participants indentified the core institutions of the criminal justice system as the police, the prosecution, the judiciary, prison service, probation office, communities, community development officers and defence lawyers. Other important bodies include the legislative draftsman, human resource administrators and ICT personnel among others.

Dr Owor described the models for responding to cybercrime as part of cyber security strategies and the justifications for such a strategy- because criminal justice authorities do not have a prominent role in developing cyber security strategies despite their work

in the detection, investigation, prosecution, defence, sentencing and punishment of offenders. An effective system would among other things, ensure the confidentiality, integrity and availability of the computer data and the computer systems, punish attacks on the systems while adhering to the rule of law.

For this session, the components of a criminal justice response that participants discussed were:

- **Regulatory framework**: covers measures like those on effective reporting and prevention mechanisms. For instance the South Africa *Electronic Communications and Transactions Act* 2002 provides for cyber inspectors to monitor and inspect any web site or activity on an information system in the public domain. There are also policies for instance on the handling of cybercrime cases and electronic evidence- an example is the *Cybercrime and Digital Evidence Policy* (Sussex Police ref 1134/2013). A third aspect is the enactment of legislation (Primary, secondary, tertiary).
- **Human resources** like specialised cybercrime units. Two main issues for consideration arise. The first are the legal powers granted to law enforcement officials and the limits on those powers (Owor, 2011 on the absence of provisions on proportionality and adequate judicial oversight in Uganda's Computer Misuse Act 2011). The second are ethical and professional considerations.
- **Training** of law enforcement personnel should start with identification of training needs in cybercrime and electronic evidence. The training should be linked to national policies. Examples like judicial training (Owor, Musoke, forthcoming 2013)
- **Co-operation:** Due to networked technology, cybercrime can overcome geographical constraints, thereby raising global and inter-jurisdictional challenges (Jang and Lim, 2013). There is need for co-operation at the public, private, regional and international level through arrangements in the form of Treaties (e.g. Mutual Legal Assistance Treaties) or reciprocal legislation.
- **Search & confiscation of crime proceeds on Internet:** could cover cross/trans-border investigations; process of search and seizure; confiscation; dealing with jurisdictional disparities and the ubiquity doctrine (CoE report, 70-71, para 250).
- **Protection of personal data:** caution against intrusive means of search and seizure which may lead to possible invasion of privacy rights. On the limitation of the right to privacy within the context of Article 24(3) Kenya constitution see *Dyer & Blair Bank Ltd v Equity Bank Ltd & another [2012] KLR (High Court at Nairobi, Civil Case 26 of 2009).*
- **Rights based approaches-** consider the rights of parties (offender, victim, others), the right to access information, and protection against self-incrimination. Will your state extend the bill of rights to foreigners extradited to your country to stand trial on criminal charges?

SESSION 7: CHALLENGES AND SOLUTIONS

This session comprised of four break-out groups in which participants developed elements of an effective criminal justice strategy on cybercrime and electronic evidence using case studies. The four areas were:

- How to develop a robust, regulatory framework (measures, policies and laws)
- Human resources and development of a training strategy that integrates legal and ethical considerations
- Establish effective systems for national, regional and international co-operation, search and confiscation of proceeds
- Facilitate a rights based approach that contributes to protection of personal data and upholds the Rule of Law?

Group I – Regulatory framework

The group gave an update on the measures, policies and processes of law reform in Tanzania and Uganda. In Uganda, relevant laws protecting users against cybercrime were outlined. It was noted that there was significant response to this initiative through Computer Emergency Response Teams (CERT), specialised units at Uganda Communication Commission (UCC), the Police Force all of which have a cybercrime prevention unit, and policy to this effect. There is the amendment to the Tanzanian Evidence Act on electronic evidence admissibility and Mahalu's case.

Group II – Human resources- Training

On Human Resources, the group outlined guidelines for personnel in enforcing the law:

i) Training:- The aim is capacity building, benchmarking and utilizing good practices from abroad e.g. from South Africa. The use of Training of Trainers as a cost- saving strategy to maximize capacity was emphasised. The group noted that monitoring and evaluation of staff was sometimes missing. Effective training means there has to be updated equipment because obsolete equipment or its unavailability makes personnel redundant. Lack of cybercrime knowledge is dysfunctional to cybercrime control.

Concerns were raised regarding the limited exposure to skills training, sometimes limited to staff in a specific Ministry or Attorney General's Chambers. Some of the people trained are not those members of staff who deal with cybercrime on a day to day basis. As such, the knowledge acquired may not be disseminated to others who need it.

ii) Human Resources – The law enforcement personnel should have the power to use the law in their routine work. There should however be limits to this power, recognising the rights of parties as required and regulated by the code of ethics.

iii) Training needs should be clearly identified. For example, it is important to know whether the training is to focus on national policies, or whether refresher courses will be necessary and whether they will achieve the desired goal. The training should have measures for staff retention in order to retain skills obtained in training by avoiding brain-drain which afflicts most African countries.

Group III – Regional and international co-operation

Cybercrime is a sub regional and multi-disciplinary problem calling for international cooperation - states with states, agents with cooperates and between key partners of the

criminal justice for a successful fight against cybercrime. This cooperation can be stipulated through Memoranda of Understanding, Agreements and Conventions.

Cooperation is through extradition and mutual legal assistance to assist the enforcement the law for recovery of proceeds of illicit wealth acquired through cybercrime. There is need for focal persons (consistent with) Budapest Convention Art 35). Cybercrime involves huge amounts of proceeds and confiscation is vital for recovery of ill gotten proceeds.

In Tanzania the Proceeds of Crime Act focuses on the computer used as well as the proceeds. The computer will also be confiscated. Other legislation can also be used, for instance, the Anti money laundering Act. Such laws should set out measures for the seizure and confiscation of proceeds of crime; search and confiscation of crime proceeds on internet and facilitating cross border investigations using established processes of search and seizure, confiscation and dealing with jurisdictional disparities.

Group IV – Right of Individuals

This group examined the rights of individuals, including offenders/criminals and victims. The rights of individuals are enshrined in the Constitution. Rights are not absolute; there are limits on certain rights, depending on circumstances. A suspect is also liable for protection within the confines of the law e.g. data protection law where the law exists. The sources of individual rights and procedural safeguards can be found in national constitutions, the EAC Bill of rights, the African Charter on Human Rights.

Group V – The rights-based approach

This group examined the application of the rights during law enforcement. The group noted that law enforcement requires respect for local sensitivities. There may be limitations since the means of search and seizure may lead to invasion of privacy of individuals if not carefully carried out. It was emphasised that procedural process of law enforcement must be exercised within the context of human rights and judicial oversight. In this regard, the group pointed out that the defence has a right to obtain electronic evidence. This could be arranged through letters rogatory through which defence lawyers can request for pertinent information.

Plenary discussion

Regulatory frameworks include reporting and prevention and there are relevant cases studies from South Africa. Where there are no policies regarding on cybercrime or handling electronic evidence there may be laws instead. It is crucial that there are standards for assessing the effectiveness of a law. Laws ought to follow principles of rule of law; be effective and clear. Dr Owor pointed out that legislative drafters should consider what the aim of the law is and whether it (law) is clear on what it requires people to do? Above all, law should be clear on why a restriction is imposed. Participants discussed the need for harmonisation of legal regimes at sub-regional, regional level and international level.

The following points were discussed in turn by the participants: issues of the pluralistic systems, use of technology neutral language; dominant official language versus unofficial local languages; and being mindful of the issues surrounding gender identity. Dr Owor flagged up a final question for consideration- whether cybercrime legislation can resonate with African normative frameworks? In countries like Uganda, laws have to reflect African values in order for them to be relevant (Uganda Law Reform Commission Act). Given the nature of cybercrime, integrating African values requires conceptualisation at a more theoretical level and involving communities in the drafting of law.

SESSION 8: RECOMMENDATIONS BY COUNTRY
Facilitators: Dr Maureen Owor and Dr. Alexander Seger

The participants in the training workshop appreciated the strengths and challenges available in each country's presentation. The delegations indicated the desire to improve their legislation, develop their human resource, engage in capacity building, collaborate within the national and international frontiers, and consolidate the available prospects for modernity and the efficacy of the electronic age.

The participants appreciated that the Budapest Convention, and works by the Council of Europe, formed the background information in the learning process, providing essential guidelines and a promise of continued cooperation and technical assistance, to sustain the interest that has been generated at this inaugural intervention in the region.

Against this background, each country's delegation made specific country proposals/recommendations as detailed hereunder:

1. BURUNDI
The Burundi delegation cited regional cooperation as a remedy to offer possible solutions to the challenges posed by ineffective cybercrime legislation

a) *Collaboration*

No country in the world can effectively fight against cybercrime individually. The nature of the phenomenon and especially the highly technical realization suggests that all states of the world have to work together to deal with the challenge. The problem of cybercrime is that it is an almost imperceptible offense. The location of the cyber offender is unknown and impractical.

b) *Regional/International legislative mechanisms*

Often transnational litigation is complicated by the fact that often international cooperation is not in itself sufficient. Under the principle of territoriality of criminal law, it is difficult to prosecute a cybercriminal who is outside the country. In addition, there is no jurisdiction which can track down this kind of criminal.

c) Mutual legal assistance/extradition

The Burundian delegation proposes the negotiation of some sort of cross border regional and international jurisdiction to prosecute cybercrime. As in international criminal law, it is necessary to examine the possibility of introducing the principle to extradite or prosecute to ensure that dangerous cyber criminals are identified wherever they are, whoever they are and whatever time of the commission of the offence.

d) Technical capacity of the criminal justice system

Africa must be particularly careful and sustained efforts must be made. Locally, the criminal justice system must have the specialized knowledge to deal with this global scourge. More specifically, Burundi proposes that its police, prosecutors and judges are first made aware of the problem; are very well trained and have the means to cope effectively.

2. KENYA

a) Proposed Strategies on Cyber Crime and Electronic Evidence

- Improve procedural law to cater for cyber crime;
- The CID cyber crime unit be empowered in terms of trained personnel in cyber crime, ensure sufficient work tools are provided to curb cyber crime;
- Ensure law enforcement officers (police, prosecutors, judiciary, probation, CBOs and NGOs) are continuously trained in the area of cyber crime and electronic evidence so as to aptly fight cyber crime. The training needs should be identified for cybercrime and electronic evidence;
- The Kenya Information Communication and Technology Policy should be amended to provide for procedural law on cyber crime and electronic evidence;
- Establish a cyber crime laboratory similar to one that Rwanda is developing.

b) Steps to be taken (recommendations)

1. Amend or enact procedural laws to provide for—

- Expedited preservation and disclosure;
- Production orders and provide for the following categories of electronic data: traffic data; content data; and subscriber data;
- Search and seizure of stored computer data and to apply to extended computer network;
- Interception of data;
- Real time collection of traffic data;
- Conditions and safeguards of procedural provisions;
- The scope of procedural provisions in respect to specific criminal investigations and proceedings;
- Forensic tools.

2. Provide for more civil remedies, compensation etc in cybercrime legislation.

3. Ensure that within the eastern Africa community, the laws are harmonized so as to avoid dual criminality.

4. Enact the Data Protection Bill, currently at the second stage in Parliament.
5. Ensure international cooperation on the fight against cyber crime.
6. Develop policies on electronic evidence and handling of chain of electronic evidence.
7. Provide for a reporting and feedback mechanism such as collection of data via data banks which could act as a monitoring and evaluation mechanism.
8. Strengthen inter-agency collaboration thus enhancing national cooperation in the fight against cyber crime.
9. Ensure robust public awareness programmes on key aspects of cyber crime and how it affects the citizenry at large.

All relevant laws have been passed, but there are outstanding provisions that need revision. The commencement of the establishment of the Kenyan CERT (Computer Emergency Response Team) is a significant milestone in combating cybercrimes. The set-up is still at the initial stages hence the need for awareness raising among critical stakeholders has been identified. Hopefully the workshop will provide ample substance and technical assistance to inform the processes of reviewing (amendments) the law to address the inter-territorial aspects of legislation within the framework of a wider Eastern African context.

Kenya is somehow ahead of the other countries in the East African region regarding the development of cyber crime legislation. Its legislation is aimed to be in compliance with the East African Community Taskforce Recommendations on Cyber Laws, the Budapest Convention and the Draft Africa Union Convention on the Establishment of a Credible Legal Framework for Cyber Security in Africa.

3. RWANDA

Recommendations

- Strengthen specialized law enforcement units (Prosecution, Police, etc)
- Organize trainings of law enforcement agencies (judges , prosecutors police, lawyers) on cybercrime and electronic evidence;
- Conduct awareness campaigns and sensitize the population /victims about cybercrimes;
- Finalise the law governing information and communication technologies;
- Consider ratification of the Budapest convention on cybercrime;
- Speed up the availability of tools to facilitate the collection and preservation of electronic evidence (e.g. computer forensic laboratory);
- Develop cybercrime data recording system and ensure that information is shared between concerned entities.

4. TANZANIA

Efforts are made to make comprehensive legislation against cybercrime in Tanzania and these measures take into account the need for integration of best practice based on international and regional perspectives. In the interim, the delegation makes the following proposals to strengthen capacity to deal with challenges of enforcing cybercrime legislation.

Steps to be taken

- Establish a forensic laboratory;
- Develop the capacity of investigators, prosecutors, magistrates, judges and prisons officers;
- Promote international cooperation which will be of much help on different matters, including cybercrime prevention;
- Amend legislation to avoid double criminality and consolidate existing laws through law revision to avoid scattered provisions of law.

Areas of need for technical assistance

I) Capacity building on: the collection and analysis of electronic evidence, the drafting of cybercrime legislations and the presentation of electronic evidence in court.
II) To facilitate the regulatory authorities with equipment and skills on the means to regulate providers.

Recommendations

- Ammend penal provisions of the laws on cybercrime to include compensation orders;
- Consider minimum mandatory sentences to avoid leaving sentencing discretion to the courts;
- Amend laws to include provisions on admissibility of electronic evidence;
- To amend EPOCA to avoid double criminality eg section 120 of EPOCA provides for illegal interception while the same provision is in the draft Cybercrime bill- section 7.

5. UGANDA

1.0 Introduction

In Uganda, the advent and development of ICT came with new crimes and this provided a platform for the commission of existing crimes such as fraud, terrorism, money laundering, murder and theft. Although these crimes could be prosecuted under the Penal code Act, ICT related crimes such as hacking and theft of computer programmes or software poised a challenge to the legal system, hence the need to enhance cyber security.

Cyber security in Uganda is a relatively new field which is related to the rise of digital technology. This also means that cyber security has evolved separately from other concepts of security. In order to give protection from disruptions in confidentiality, integrity, availability of computer s and often non repudiation of digital technologies and information hence the need to combat cyber crime in Uganda.

2.0 Statement of the problem

The existence of cyber laws notwithstanding, cyber crime continues to rise. The lack of capacity among law enforcement units of government coupled with the lack of

awareness on the part of the community and the fact that our virtual borders are open raises questions regarding Uganda's capability to combat cyber crime.

3.0 Justification

The need to protect the current population of about 37 million Ugandans from threats like terrorism and economic crime most especially now as the crime rate associated to computers is at 14.8%, cannot be over stated. It is imperative therefore that a concerted joint effort, both nationally and internationally is taken to ensure that compromise to ICT is either eliminated or reduced to the minimum levels in Uganda and that no country in East Africa is used as a hub to infringe the virtual borders of member states.

4.0 Advantages of the Strategy

The strategy will:

- Develop the capacity of relevant players with the knowledge and skills of combating cyber crime in the country;
- Help create a secure economic environment;
- Help eliminate threats to life and other social services; and
- Ensure that the admissibility of electronic evidence is no longer a debatable issue in Ugandan courts.

5.0 Disadvantages

Developing such a strategy is expensive and it would require expertise that Uganda does not have. Such a strateggy may compromises the right to privacy so this issue needs to be addressesd as well.

6.0 Recommendations on steps to be taken by Uganda

Having appreciated the current legal regime and the threat that cybercrime poses to Uganda as a nation, we recommend as follows:

Legislation: Substantive and Procedural law:

- Amend the Evidence Act to expressly provide for the admissibility of electronic evidence.
- Amend the Computer Misuse Act to impose an obligation on citizens/persons to report any incidents of cyber crime.
- Amend Section 9 Computer Misuse Act - on preservation orders, to fit within the confines of the relevant provisions in the Budapest Convention. The section should be broadened to cover content data as data that may be subject to preservation orders.
- Hasten the application to accede to the Budapest Convention.
- Consolidated into a single legislation, the laws that punish cyber crimes. These laws include the Computer Misuse Act, Electronic Signatures Act and the Electronic Transactions Act all of 2011. A good example is South African legislation.
- A component on cyber crime should be incorporated into the National Education curriculum i.e. from Form 1 and/or other higher institutions of learning.

- Creating awareness at all levels of the social strata to enable them identify and report cyber crime.
- Have sensitisation programmes through partnership between the Government and other service providers in the ICT sector for instance by establishing nd contributing to a fund to support awareness and sensitization campaigns. Awareness could also be part of corporate social responsibility.
- Develop the infrastruce to facilitate cyber crime prevention e.g. high-tech ICT Laboratories. Procure equipment to facilitate the analysis and storage of electronic data.

6.1 Strategies on cyber crime and electronic evidence:

(a) Conclude Bi-lateral agreements with all partner States;
(b) Ensure capacity building of all law enforcement agencies like the police, prosecutors, and judges/magistrates through training and updated infrastructure.
(c) Harmonise the national laws with the regional and international laws on cyber crime.
(d) Design and put in place an elaborate procedural framework on evidence gathering and prosecution of cross border cyber crimes.

6.2 Areas for further technical assistance;

a) Training of enforcement agencies like the Police officers, Prosecutors, Judges/Magistrates, Prison Officers in Basic computer knowledge.
b) Advanced computer forensic training for the respective law enforcement personnel.
c) Subsequent refresher courses for the law enforcement personnel.
d) Build capacity of Trainers on cyber crimes.

Session 9: The way forward

Participants recognised initiatives at the sub regional level, namely the work done by the East African Community on its *Legal framework for Cyberlaws* and similar initiatives by ECOWAS, SADC, and the African Union. These legal frameworks provide support for the development of cybercrime legislation in individual countries.

Africa has a legitimate need for a safe cyber environment in order to encourage e-commerce and in this regard, participants recommended the establishment of an Eastern African coalition of law enforcement organs to combat cybercrime using effective yet sustainable home-grown strategies developed from good practice and regional initiatives. To this end, strategies could include, enhanced awareness programmes; improved capacity building; human resource training, motivation and retention; formulation of effective legislation that fits within the wider international and regional framework; ratification and domestication of international and regional conventions; strategic management of criminal justice systems to focus on victims of cybercrime

while punishing cybercriminals; improved collaboration at the sub regional level and international level; information sharing and enhanced research of an academic and practical nature.

The need for political good will was underscored. To develop political goodwill and a common understanding on how cybercrime can be handled, there is a need to work with officials in the Ministries of Foreign Affairs in all partner States as well as service providers, the judiciary, law enforcement agencies, lawyers (through the Law societies), the private and nongovernmental sector and the citizens. This action can be buoyed by the formation of local networks for wide consultations to create awareness about cybercrime and obtain views about the challenges arising from the proposed legislation and issues surrounding cybersecurity. Other measures that relate to the development of effective legislation included: the involvement of members of Parliament in the enactment of laws and improved interaction with relevant Parliamentary Committees.

Regarding collaboration with partner institutions, participants observed that the Council of Europe offered opportunities for collaboration, capacity building, technical assistance and information sharing especially to countries that acceded to the Budapest Convention. The Budapest Convention was acknowledged for its relevance to emerging cybercrime laws in Eastern Africa and as a possible framework for the harmonisation of legislation in Africa. The continental focus on the Budapest Convention in this regard gives credence to the possibility of increased accession to the Treaty by African countries.

In this regard, and consistent with its mandate, UNAFRI/ACCP offered to meet the demands of the Member States – as a focal point and window of international intervention for the expert responses to strengthen crime prevention and criminal justice systems in the region.

Session 10: Closing session

Mr John Kisembo, the Acting Director, UNAFRI and co-Director of ACCP.

Mr. Kisembo recognised the official link between the Council of Europe, Eastern Africa, UNAFRI and ACCP and hoped that this link would enhance the development of laws on cybercrime. Mr Kisembo thanked the Government and people of Tanzania for their generosity in hosting the workshop and the active participation of the Tanzanian delegation. He gave a vote of thanks to the Lead consultant (Dr.Maureen Owor) and to Dr.Alexander Seger, Mr Sizwe Snail, Mr Saidi Kalunde and Dr. Alhas Maicibi and the staff of UNAFRI and the ACCP for their role in facilitating the workshop.

Special tribute was paid to the participants for honouring the invitation and taking part in the workshop in an open and engaging manner. Mr Kisembo asked the participants to put the information and skills they had acquired to good use by sharing the resources with other organs and acting as facilitators in their own countries.

Mr Kisembo expressed his appreciation for funding provided by the Council of Europe to run the workshop and he reiterated the need for continued support to cater for the actititives identified by particiatipants at the inaugural workshop. He pledged the services of UNAFRI and ACCP to provide support to states to deal with the problem of crime in general and cybercrime in particular given its devastating consequences in Africa. In this regard, he invited the delegations to indicate their needs to UNAFRI and ACCP. Mr Kisembo wished all the participants a safe journey back home and he then officially closed the workshop.

Appendix 1 - List of Participants

COUNTRY		NAME	TITLE/ ORGANIZATION	EMAIL
BURUNDI	1	Marie Louise Uwimana	Magistrate/Adviser-Ministry of Justice	mlwimana84@yahoo.fr
	2	Leonard Gacuko	Director-National Legislation Services	gacukolo@yahoo.fr
KENYA	3	Gikui Wangui Gichuhi	Prosecutor-ODPP Kenya	gikui@yahoo.com
	4	Irene Warima Kabua	Advocate	irene.kabua@gmail.com
TANZANIA	5	A. Wambura	District Resident Magistrate	anniebunga@yahoo.com
	6	Elinkaila Winston Mirrudy	Police Office-Cybercrime	winstonelly@gmail.com
	7	Saidi Mashaka Kalunde	State Attorney-Attorney General Chambers	saidimj@gmail.com
	8	Mlangi Thabit	State Attorney – Parliamentary Drafter	mlangi.thabit@gmail.com
	9	Maziku Joseph Masere	Officer - Prison Department	josephmaziku@gmail.com
	10	Awamu Ahmada Mbagwa	State Attorney-Office of Public Prosecutions	awamumbagwa@yahoo.com
	11	Rose Joyce Chilongozi	Attorney General Chambers-Senior State Attorney	mboyap@yahoo.co.uk
	12	Juma Ismail Said	Police Officer	Juma.ismail@yahoo.com
	13	Mussa Goliama Mpandiko	Prisons Officer	mpandikomusag@gmail.com
	14	Ramadhan Kalinga	State Attorney-Attorney General Chambers	ramakalinga@gmail.com
	15	Josephat Mkizungo	Senior State Attorney-Cybercrime &Cyber Law – Coordinator for DPP	jmkizungo@agctz.go.tz; jmkizungo@hotmail.com
	16	Rehema Katuga	State Attorney-Attorney General Chambers	rkatuga@yahoo.com
	17	Frank Shame	Principal Computer Systems Analyst	frankshame@estabs.go.tz
	18	Honest Njau	CSA-Ministry of Communication Science & Technology.	sambomarajr@yahoo.com; honest.njau@mst.go.tz
	19	Aimar Mohammed	Secretariat	aimar.mohammed@gmail.com
	20	Stephen Magesa	Police Officer	magesas@yahoo.com
RWANDA	21	Gahamanyi Emmanuel	Prosecutor	Emmanuelgah12@yahoo.fr
	22	Kanyabuganza Eric	Director-Economic Crimes – CID	banyabussperic@gmail.com
	23	Ikiriza Ruth	Principal State Attoney	ikirizaruth16@gmail.com
UGANDA	24	Oliver Nantamu	State Attorney	noplivie@gmail.com
	25	Solomon Kirunda	Senior Legislative Counsel	skirunda@parliament.go.ug

	26	Omar Mohammed	Principal State - Attorney	mohamomar@yahoo.com
UNAFRI	27	Kisembo John	UNAFRI – Acting Director	jkisembo2005@yahoo.com
	28	Patrick Mwaita	UNAFRI – Research Training Assistant	mwaitapatrick@yahoo.com
	29	Sarah Musoke	UNAFRI – Finance and Admin Assistant	sarahemusoke@hotmail.com
COUNCIL of EUROPE	30	Alexander Seger	Secretary of the Cybercrime Convention Committee	Alexander.seger@coe.int
	31	Alhas Maicibi	Professor, Secretary General - ACCP	alhas202@yahoo.co.uk
	32	Snail Kamtuze Sizwe Lindelo	Attorney	ssnail@snailattoneys.com
	33	Maureen Owor	ACCP - Fellow	mhowor@gmail.com