



Distr.: GENERAL

E/ECA/CODIST/1

**UNITED NATIONS
ECONOMIC AND SOCIAL COUNCIL**

Original: English

ECONOMIC COMMISSION FOR AFRICA

First Meeting of the Committee on
Development Information, Science & Technology (CODIST)

Addis Ababa, Ethiopia
28 April – 1 May 2009

Workshop on Legal and Regulatory Framework for the Knowledge Economy



28 April 2009

BACKGROUND

An appropriate legal and regulatory environment for the knowledge economy ensures that there are set rules and regulations which allow the ICT sector to be more competitive allowing the economy to grow. It has been noted that there is a core relationship between the level of attainment of knowledge economy and the inflow of financial investments. Countries that have advanced economies such as Japan, Germany, Australia, United Kingdom and United States of America have all embraced e-commerce activities, as a way of life and enacted cyber legislation to regulate e-commerce activities.

African countries aspire to attract financial investment to boost economic growth and should therefore embrace this trend (the creation of a knowledge economy). However, Africa is lagging behind and there is fear that Africa will be excluded from the digital revolution. Africa faces a number of challenges such as lack of technologically advanced telecommunications infrastructure, lack of legal and regulatory frameworks supportive of ICT developments and the high rate of illiteracy.

An enabling environment which allows / encourages creation of a knowledge economy is of paramount importance. Some components of an appropriate enabling environment include:

- Ensuring that the playing field allows for healthy competitions in the ICT sector.
- developing financial system to mobilize capital to its most productive uses,
- Adoption of an appropriate legal and regulatory framework through introduction of a whole legal system supportive and free from legal barriers for the development of knowledge economy.
- Creation of an environment which offers basic assurances such as security, integrity, authenticity, confidentiality and data protection /privacy.

In recognition of these challenges, the Economic Commission for Africa (ECA) launched African Information Society Initiative (AISI) in May 1996. ECA 's vision is to assist African countries in establishing a conducive environment in which knowledge is seen as a vital tool for economic growth and bridge the digital divide between Africa and the rest of the world. AISI provides the road map to guide African countries in addressing the challenges of emerging globalization and the information age by developing and implementing National Information and Communication Infrastructure (NICI) policies and plans.

Recognizing the important role that ICTs play in facilitating attainment of development goals and their multiplier effects on growth and economic and social development, ECA responded to the challenge and launched AISI in May 1996. This initiative was a common vision to bridge the digital divide between Africa and the rest of the world and more importantly, to create effective digital opportunities to be developed by Africans and their partners and speed the continent's entry into the information and knowledge-based global economy. The digital divide continues to pose a serious socio-economic development threat to African countries and AISI attempts to address this threat by recognizing the role that ICTs can play in accelerating the socio-economic development process and in the fight against global poverty.

AISI is the action framework that has been the basis for information and communication activities in Africa for the last ten years. It also represents a regional framework to support the implementation of the New Partnership for Africa's Development (NEPAD). Africa's commitment to ICT4D is also reflected through the NEPAD Action Plan, where ICT projects and initiatives have been initiated to speed up subregional/regional connectivity.

It is therefore in this context that a workshop on "Legal and regulatory frameworks for the knowledge economy" was organized on 28 April 2009 at the UN Conference Center in Addis Abba, Ethiopia. The workshop, which was organized with the support of the Organisation Internationale de la Francophonie (OIF), UNCTAD and ISOC analyzed the formulation and modalities for adoption of legal and regulatory frameworks which is one essential element towards the creation of an enabling environment for the knowledge economy.

Session I: Opening Session

1. Welcoming and introductory remarks

In opening the legal and regulatory framework workshop, the Director of ICT, Science and Technology Division (ISTD), Ms Aida Opoku-Mensah informed the participants about the significance of the workshop on creating a conducive environment for the knowledge economy. She stressed that "*the creation of an enabling legal and regulatory environment is critical to the effective implementation of national and sectoral e-strategies*". She informed the participants that the workshop is expected to come up with plans in capacity building programmes on legal and regulatory issues, creation of knowledge sharing and best practice networks on legal and regulatory issues, and mainstreaming cyberlaw formulation as a pillar for national and subregional strategy implementation.



On behalf of the Organisation Internationale de la Francophonie, Mr Pierre Ouedraogo, Director of Administration reminded participants that "the current financial crisis will have an impact on our national and regional economies, and the issue of knowledge economy becomes crucial because, by promoting innovation, it can be an important factor for the fight against poverty and to bring about peace and stability in our countries" He further stated that the OIF expects the workshop to be "an opportunity to share the best practices, and to be a cradle for future networks of ICT experts in the area of regulatory frameworks which enlightens the concept and implementation of innovative national and regional strategies. This would enhance the digital industrial capacities that need the basic raw material of the information society which is knowledge". Mr Ouedraogo concluded by assuring participants that the OIF General Secretary expects a lot from the meeting and that he will ensure that the implementation of the recommendations in the framework of OIF's 2010-2013 programme of work.

An opening statement was also read on behalf of UNCTAD and stated that "our common challenge is to achieve a harmonized framework that will support the development of e-commerce and e-government at the national, regional and global levels (...) Policy makers in all parts of the world are concerned about harnessing the potential of ICTs. They are also increasingly aware of the necessity to adapt their legislation to the Internet economy. The creation of an enabling legal and regulatory environment is critical to the effective implementation of e-government strategies and to the

development of e-commerce at national and regional levels.” According to UNCTAD, Cyberlaws should primarily help to ensure trust between commercial partners; be in compliance with other countries’ legislation; ease the conduct of domestic and international trade; and offer legal protection for users and providers of e-commerce/e-government services.

On behalf of ISOC, Mr Jon McNerney, Chief Operations Officer confirmed that the workshop gives ISOC “an excellent opportunity to collaboratively consider and identify legal and regulatory frameworks for ICTs in Africa which would create that enabling environment. The development of legal and regulatory frameworks that promote an open and trusted Internet are essential not only to promote access but also to ensure that this access effectively contributes to economic and social development in Africa”.

Session II: Workshop objective and expected outcomes, Eskedar Nega- Programme Officer, ICT Science and Technology Division-ECA

The workshop’s main objective is to assess the development of cyber laws, which is one essential element towards the creation of an enabling environment for the knowledge economy and will look in particular at five components:

1. current status of cyber laws in Africa,

2. legal issue to be covered by such laws:

- **E-jurisdiction, liability and dispute settlement**
- **Electronic signatures,**
- **E-payment & E-Banking**
- **E-commerce and e-taxation**
- **Cybersecurity**
- **IPRs and digital technology**
- **Data protection and privacy**

3. existing templates to be used,

4. highlights of best practices and

5. recommendations on where ECA and partners could assist in the creation of an enabling environment for the knowledge economy, particularly in three focus areas:

- **Awareness raising**
- **Human and Institutional Capacity building**
- **Networking and partnership**

Session III: Presentations

A. Setting the Scene- Legal and regulatory frameworks for the knowledge economy- Overview of current status of cyber legislation in Africa, Ms Angeline Vere-Consultant

Cyber law has been defined as “the law which describes the legal issues related to use of inter-networked information technology (the intersection of technology and law). It is less a distinct field

of law in the way that property or contract law is, as it is a domain covering many areas of law and regulation. Cyber law is the law governing computers and the Internet¹.

Trading electronically differs from the traditional commerce in that tradition trading was developed in a paper based society, e-commerce takes place in an anonymous borderless internet world, so all the rules that were developed for trading in a real environment is inappropriate for this virtual environment. Cyber law encompasses issues such use of electronic and digital signatures, computer crime, intellectual property, data protection and privacy, electronic authentication, liability and dispute resolution.

A general overview of the current status of cyber legislation in Africa was presented. The status shows that although an increasing number of African countries have embarked on designing and formulating ICT policies, the majority of them are still in the early stage of cyber legislation development and enactment. Of the over fifty countries in Africa less than ten countries have moved ahead of other African countries and have enacted some cyber legislation to guide the area of electronic activities.

- **Tunisia** was ranked top of African countries on deployment of ICT in its economy and in development of enabling environment and infrastructure. It enacted the Electronic Commerce law (2000). It covers the areas of application of e-commerce, tax filing, e-banking etc. Tunisia has made remarkable progress in e-payment. It developed an e-payment system called e-EDinar which allows internet sales and purchases and internet banking called CCPNet which allows e-banking activations.
- **Egypt** passed Law No. 15/2004 on E-Signature and established of the Information Technology Industry Development Authority (ITIDA). The law permits electronic signatures and facilitates Government and business use of electronic documents. In 2006, consultations began for the development of the cyber crime law.
- **Morocco** promulgated Comite Interministeriel pour le Developement et la Promotion du Commerce Electronique.
- In **South Africa** the discussion paper on Electronic Commerce of July 1999 served as a starting point for the eventual promulgation of the Electronic Communication and Transactions Act No. 25/2002. The overall objective of the Act is to enable and facilitate electronic transactions by providing for its enforceability and thus creating public confidence in electronic transacting. The Act also provides for the appointment of cyber inspectors whose duties include investigation of activities of cryptography and authentication service providers and also inspection of websites.
- **Mauritius** has enacted the Electronic Transaction Act 2000 and Regulations – The Information Technology (Miscellaneous Provisions) Act 1998. It provides the legal framework for the validation of electronic transactions, appointment of the Controller of Certification Authorities, facilitates the use of digital signatures and gives legal recognition and regulation of electronic records.
- **Ghana** in December of 2008 passed the Electronic Transactions Act and the National Information Technology Agency Act.

¹ en.wikipedia.org/wiki/Cyber_law
28/04/09

- **Cape Verde** has the E Commerce Decree law no; 49/2003. The Decree-Law 49/2003 adopts provisions concerning electronic commerce (through Internet and authority; supervision; final and transitory provisions.)
- **Senegal** in July 2008, passed legislation to govern the development of ICT. The legislation includes law on cyber law, law on protection of private data and the law dealing with electronic transactions.

Although only a few countries have cyber specific laws, most African countries have in their NICI e-strategy plans outlined as one of their objectives, the need to develop the cyber legislation. Included in this category are countries such as **Cameroon, Chad, DRC, Liberia, Malawi, Niger, Nigeria, Burundi, Gambia, Mozambique and Swaziland**. Other African countries have made significant progress in the preparation and drafting of legislation on e-commerce though most of the draft bills have yet to be passed into law. These include and are not limited to:

- **Kenya**, for instance, has already initiated the process of enacting cyber legislation. The Kenya Communications (Amendment) Bill which provides for regulation of telecoms, posts, broadcasting, electronic transactions and domain names, was published in August of 2008. In the same month, the bill went through the first reading in parliament.
- In **Tanzania** the process commenced in 2006 with the submission of a proposal for the enactment of Cyber laws by the Tanzania Law Reform Commission to the Ministry of Justice and constitutional affairs. It proposed separate bills on Cyber crimes, regulation of electronic transactions and e-communications, privacy and data protection and the amendment of the Evidence Act (1967). The second development was the creation of a merged Tanzania Regulatory Authority (TCRA) to oversee postal and electronic communication industries on the mainland. The Commission for human rights and good governance Act (16/2007) provides for the admissibility of electronic evidence, however this is not adequate and there is still need for the Bills proposed by Tanzania law reform Commission to be enacted.
- **Uganda's** draft electronic laws the E-transaction bill, the Computer misuse Bill and The Electronic Signature Bill were approved by the cabinet on 16 January 2008 and after which they had to go to Parliament for debate. The bills are in conformity with the proposed EAC draft framework on cyber laws.

Status of Regional Economic Communities were presented as follows:

1. The Southern African Development Community (SADC)

In 2001 the SADC committee of ministers established the e readiness task force to prepare a comprehensive study of e-readiness status in SADC countries and come up with a plan of action. The results of the study indicated that only South Africa and Mauritius in Southern Africa had established legislation covering the broad range of issues associated with electronic commerce. As a result SADC and the USAID-funded dot-GOV Southern African ICT and Policy Reform Support ("SIPRS") Project collaborated to develop the SADC Model E-Commerce law to harmonize the legal framework for Electronic Commerce. The draft version was tabled at the SADC workshop on

harmonization of e-commerce laws in Johannesburg SA on 24 November 2003. The model addresses core e-commerce issues, such as cyber crime, intellectual property rights, and privacy concerns. The model builds from existing legislation in the region, and from the "Model Law on e-commerce" formulated by the United Nations Commission for International Trade Law (UNCITRAL).

2. The Common Market for Eastern and Southern Africa (COMESA) in the East and Southern Africa (COMESA)

The European Union funded the RICTSP to support COMESA in developing policy frameworks and strategies that are geared towards ICT utilization. The formulation of the COMESA ICT strategy emerged at the experts' group meeting of February 2006 and was adopted by the Council of Ministers meeting in 2007. It was also presented to the 6th meeting of the Association of Regulators of Information and Communication of East and Southern Africa (ARICEA) / COMESA in Cairo Egypt in February 2008. This ICT strategy has four main components:

- Institutional framework – the COMESA secretariat to spear head the initiative.
- Legal and regulatory framework – enactment of e-signature, e-transaction, cyber crime Acts etc
- Common ICT infrastructure e.g. COMTEL and ESSAY cable projects.
- Priority e-government services such as e-parliament, e-customs etc.

3. The Economic Community of the West African States (ECOWAS)

In September 2004, a situational assessment survey was conducted which involved meetings with ICT policy makers within ECOWAS. The findings were that there was no appreciable legislation on e-Commerce in member states. As a result a workshop was organized by ECA in Ouagadougou in December 2006. The workshop proposed that a legal framework for e-Commerce and related activities had to be formulated and draft guidelines were to be drafted and circulated to member states before adoption by ECOWAS. Following a workshop on 11 December 2007 in Lome, Togo the participants from the ECOWAS states adopted new guidelines on combating cyber crime in the sub-region. As a result of this process, Ministers in charge of Information and Communication Technologies adopted a harmonized ICT legal framework, a bill on e-commerce in ECOWAS states and a model ICT framework. The Acts aimed at modernizing the instruments for promoting e-commerce, preserving personal data and curbing cyber crime through the necessary sub-regional and national legislation. The Regional workshop on Legal and political frameworks for Information Society in West Africa took place in Senegal on 11-13 March 2009. The workshop recommended inter alia , the extending of harmonization of text to cover important issues not yet examined such as regulating convergence of telecoms and media, harmonizing models of intellectual property rights , cyber security etc by creating regional norms

4. The East African Community (EAC)

The five member states of the East African Community (EAC) are also coordinating efforts to harmonize and pass cyber crime laws that would be effective throughout Burundi, Kenya, Rwanda, Tanzania and Uganda. A common information security policy on cyber crime formulated by East African countries will serve as a foundation for new laws. In 2006, with the support of UNCTAD several EAC workshops were organised which focused on the area of e-commerce, these include the two workshops held in April in Kampala which were on the Cyber laws and E-justice and

Information security. In the same year another workshop on legal aspects of e-commerce was held in December in Nairobi. The workshops agreed on the need to formulate a Regional task force to spear head and develop model cyber laws covering e-signatures, electronic transactions, authentications, cyber crimes and data and consumer protection. The task force also had to review existing laws and thereafter develop a regional legal framework for harmonisation of cyber laws. In June 2008, a framework for the adoption of laws to deal with electronic transactions, e-signatures and authentication, data protection and privacy, consumer protection and computer crime is being reviewed by EAC member states.

5. The Arab Maghreb Union (UMA)

ECA initiated a study on e-commerce in Egypt, Morocco, Mauritania and Tunisia. The study was initiated after the seminar held in Tangiers on the topic ICT and the development of trade between countries of Arab Maghreb Union. The results of the study and the plan for the development of the platform were discussed during the North Africa Trade Forum on “Trade for Growth and Job Creation” held in Marrakech , Morocco from 19- 21 February 2007. The trade forum came up with a proposal for the setting up of a regional commerce platform.

B. Current and emerging ICT law and policy issues

❖ The UNCITRAL texts on electronic commerce and electronic signatures: an opportunity for the adoption of modern legislation in Africa, *Mr. Luca G. Castellani, UNICTRAL*

Mr Castellani informed participants about the importance of building a solid enabling regulatory framework for electronic transactions. For instance, public procurement conducted with electronic means is seen as an important element in streamlining procurement processes and increasing their transparency and efficiency. Thus, adoption of a general law on electronic transactions becomes a necessary requirement for improving e-governance. In a different field, the absence of an efficient system to manage security interests has often been identified as a major obstacle to the development of African credit markets, which is, in turn, key to economic success.

The United Nations Commission on International Trade Law (UNCITRAL) is the core legal body of the United Nations system in the field of international trade law, with the mandate to further the progressive harmonization and unification of the law of international trade. For the past thirty years, UNCITRAL has prepared texts in the field of electronic commerce, paving the way to its wider use in support of trade worldwide.²

The most recent text prepared by UNCITRAL in the field of electronic commerce, and the most relevant to immediately address needs of developing countries, is the United Nations Convention on the Use of Electronic Communications in International Contracts (the Electronic Communications Convention). Concluded in 2005, the Electronic Communications Convention aims at enhancing legal certainty and commercial predictability where electronic communications are used in relation to international contracts. It addresses the determination of a party’s location in an electronic environment; the time and place of dispatch and receipt of electronic communications; the use of automated message systems for contract formation; and the criteria to be used for establishing

² Information on the UNCITRAL texts on electronic commerce is available on the UNCITRAL website at: http://www.uncitral.org/uncitral/en/uncitral_texts/electronic_commerce.html (for the English language; the same content is available also in Arabic, Chinese, French, Russian and Spanish).

functional equivalence between electronic communications and paper documents – including “original” paper documents – as well as between electronic authentication methods and hand-written signatures. It also contains a provision on input errors made by natural persons in electronic communications.

The Electronic Communications Convention satisfies manifold goals: it removes obstacles to the use of electronic transactions arising from provisions contained in treaties adopted before the rise of electronic commerce; it modernizes certain provisions contained in older UNCITRAL texts and ensures that they are uniformly implemented and interpreted; most importantly in this context, it provides a blueprint for those countries lacking legislation on electronic commerce as it contains the basic rules for the use of electronic transactions both domestically and internationally.

The Electronic Communications Convention has 18 signatories, including, in Africa, the Central African Republic, Madagascar, Senegal and Sierra Leone. The UNCITRAL secretariat is undertaking efforts to assist these countries towards ratification of the Convention.

The Electronic Communications Convention builds on other UNCITRAL texts on electronic commerce, and, in particular, on the UNCITRAL Model Law on Electronic Commerce and on the UNCITRAL Model Law on Electronic Signatures.

The UNCITRAL Model Law on Electronic Commerce, adopted in 1996 and complemented with an additional article in 1998, is intended to facilitate the use of modern means of communications and storage of information. It was the first legislative text embodying the fundamental principles of non-discrimination, of functional equivalence and of technological neutrality. Thus, it established the conditions for equivalence between electronic data messages and paper-based concepts such as “writing”, “signature” and “original”. It also established rules for the formation and validity of contracts concluded with electronic means, for the attribution of data messages, for the acknowledgement of receipt and for determining the time and place of dispatch and receipt of data messages.

The UNCITRAL Model Law on Electronic Commerce has been very successful, having already been adopted in more than 30 jurisdictions and having inspired provisions in many more. In Africa, it has been adopted, for instance, by Cape Verde and Mauritius.

Adopted in 2001, the UNCITRAL Model Law on Electronic Signatures aims at giving additional legal certainty to the use of electronic signatures. It establishes criteria of technical reliability for the equivalence between electronic and hand-written signatures by following a technology-neutral approach which avoids favouring the use of any specific technical product. This means in practice that legislation based on this Model Law may recognize both digital signatures based on cryptography (such as public key infrastructure – PKI) and electronic signatures relying on other technologies. The Model Law further establishes basic rules of conduct that may serve as guidelines for assessing responsibilities and liabilities of the signatory, of the relying party and of trusted third parties intervening in the signature process such as certification service providers. Finally, the Model Law contains provisions favouring the recognition of foreign certificates and electronic signatures.

The Model Law on Electronic Signatures has been adopted in Africa by Cape Verde, among others; it has also been enacted by a number of commercial partners important for African trade such as China, the United Arab Emirates and Viet Nam.

The adoption of these three UNCITRAL texts would provide a country with a comprehensive general framework for the use of electronic transactions in commercial operations; moreover, many

provisions, such as, for instance, those on electronic signatures, may also find application outside the trade field.

Other texts prepared by UNCITRAL and by other organizations may address more specific needs. Thus, for instance, Chapter 3 of the United Nations Convention on Contracts for the International Carriage of Goods Wholly or Partly by Sea, adopted in 2008 (the “Rotterdam Rules”) deals with electronic transport records, which may be negotiable or non-negotiable, thus representing the electronic equivalent of bills of lading. An example outside the field of work of UNCITRAL is offered by the Guidelines on the Protection of Privacy and Transborder Flows of Personal Data prepared by the Organization for Economic Co-operation and Development (OECD) and regarded as standards in their field.³ These texts may complement the fundamental UNCITRAL instruments discussed above.

The mandate of UNCITRAL extends beyond legislative drafting, covering also technical assistance in legislative reform and coordination of the efforts of other intergovernmental organizations active at the global and regional level. Thus, for example, UNCITRAL cooperates closely with UNCTAD in promoting the adoption of electronic commerce texts in developing countries and building the capacity for their correct implementation.

At the regional level, the Southern African Development Community (SADC) has drafted a Model Law on Electronic Transactions inspired by UNCITRAL texts. Many more opportunities lie ahead. For instance, the Organisation pour l’Harmonisation en Afrique du Droit des Affaires (OHADA) and its member States might consider preparing an OHADA Uniform Act on Electronic Commerce based on UNCITRAL texts; the adoption of such Act together with the Electronic Communications Convention would ensure legal uniformity inside and outside the OHADA space.

At the country level, the UNCITRAL secretariat offers assistance in legislative drafting, including reviewing existing drafts and contributing to workshops and seminars in support of legislative work. This task is often carried out with local partners and international donors with a local presence. In case of interest, work on electronic commerce may be included in existing country initiatives.

As part of its recommendations, the UNICTRAL representative made a first suggestion to a developing country wishing to adopt modern legislation on electronic commerce to consider the adoption of UNCITRAL texts, starting with the Electronic Communications Convention. As these texts are considered global standards, any deviation should be carefully weighed against the disadvantages that lack of uniformity may bring. The UNCITRAL secretariat is ready to provide technical assistance as appropriate. In short, the answer to this legislative need may be just a few emails (and attached reports and explanatory notes) away.

The work of UNCITRAL on electronic commerce continues also on the legislative side. In particular, the Secretariat is engaged in the study of the legal aspects involved in implementing cross-border single windows with a view to formulating a comprehensive legal reference document. The single window is defined as “a facility that allows parties involved in trade and transport to lodge standardized information and documents with a single entry point to fulfil all import, export, and transit-related regulatory requirements”. While single window facilities do not necessarily need to be in electronic form, “[i]f information is electronic, then individual data elements should only be submitted once”.

³ Available on the OECD web site at:
http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html
28/04/09

Mr Castellani concluded by emphasizing that paperless trade and single windows are of paramount importance for trade facilitation; indeed, they may have a direct impact both on streamlining logistics and on expediting customs procedures and making them more transparent. These topics are particularly relevant for African countries. It is therefore highly advisable that African States participate in this work closely sharing their experience and signaling needs so as to ensure the preparation of texts fit for adoption worldwide. At the same time, African States should consider further intensifying their efforts to adopt legislative texts on electronic commerce, thus fostering the wider use of electronic means in support of their international commercial operations.

❖ **E-jurisdiction, liability and dispute settlement, Mr. Sam Dawa, Legal Informatics- Faculty of Law, Makerere University, Uganda**

Computer crime was defined as a crime that could be classified into the following categories:

- Content related crime, for example, child pornography and criminal, copyright infringement
- Traditional crimes committed by means of a computer, for example, harassment, hate speech, fraud and theft
- Attacks on computers and computer systems, for example hacking

The presenter also reviewed the various challenges to jurisdiction in its traditional sense, including: world wide access to the Internet, world wide dissemination of content and the existence of different legal regimes.

Providing a status of what African nations were doing, Mr Dawa referred to the setting up of regulatory authorities (Uganda – NITA & UCC, Kenya – CKK, Rwanda – RITA, Nigeria – NITDA & NCC) as well as the enactment of legislations, including substantive and procedural laws that criminalize certain activities online and create procedures for investigation, prosecution, punishment and sentencing of offenders, while enhancing global collaboration in cybercrime and cybersecurity enforcements (Uganda : five bills on electronic transactions, electronic signatures, computer misuse & anti-pornography bills , South Africa -ECTA, 2002, Kenya – Kenya Communications - Amendment- Act, 2008).

In terms of dispute settlement, the following main challenges were presented to participants:

- Change in the nature and complexity of disputes that arise in the telecommunication sector due to ICT trends and globalization;
- Recognition of expeditious and effective dispute resolution as an important objective of telecommunication policy and regulation by policy-makers and regulators;
- Separation of policy-making, regulatory and service provision functions
- Consideration of negotiation, mediation and arbitration as alternative dispute settlement mechanisms;
- The presenter concluded by referring to lessons and opportunities for Africa, as follows:
- Developing countries looking for a model to adopt;
- The need for current laws to be updated;
- The need for support from (inter)national bodies and institutions;
- Launching alternative legal instruments considered as counterproductive and may cause confusion and delay in process

- Although a common legal framework would eliminate jurisdictional hurdles to facilitate the law enforcement of borderless cyber crimes, a complete realization of a common legal framework may not be possible. Transposing Convention provisions into domestic law is difficult especially if it requires the incorporation of substantive expansions that run counter to constitutional principles.

❖ **E-commerce and taxation, Mr. Adam Mambi, Tanzania Communications Regulatory Authority**

The presenter introduced the legal implications of e-commerce by reminding the legal requirements of paper based transactions, such as: writing, manuscript signatures, original documents & seal, fall of hammer under physical auctions, digital infringement of IPRs, evidential requirement of originality, lack of legal framework on cyber payments, evolution of cyber crimes.

Addressing legal issues on e-commerce requires the following questions to be addressed: where things really happen? How should the transaction be authenticated? How to determine the minors when making e-transactions? who are behind the screen (identification)? How can we solve the jurisdiction problem in dispute settlement? Which Legal System will apply? Do we have Cyber laws that protect on-line consumer?

Challenges on e-commerce: include issues related to cyber security (e-crimes, privacy & data protection), evidential obstacles arising from the existing requirement of original and written documents, lack of legal framework on e-signatures, e-Jurisdictional problem, lack of regional legal framework, misuse of e-commerce (child pornography, cyber-squatting etc).

In terms of suggested solutions, the presenter referred to the use of the UNCITRAL Model Law on e-commerce & e-signatures (he functional equivalent approach), the UN Convention on the Use of Electronic Communications in International Contracts, 2005 , Regional Laws (EU Electronic Commerce Directive, EU Directive on Unfair Terms Directives Council & Distance Selling Directive for online consumers and national Laws (e.g South Africa, India, Malta etc) .

Regarding e-taxation, it was noted that the impact of digital technology on e-commerce has posed a great challenge on taxation system at global level given that the technology facilitates the transactions of digitized goods and services on-line, that people can order and make payments online as well as the fact that most laws applies principles on source, residence, permanent establishment and jurisdiction for the purpose of taxation.

Challenges on Cyber taxation include issues such as problems in collecting sales and taxes on remote transactions, remote firms do not have nexus and therefore do not have sales tax collection responsibility, Existing tax systems tend to determine tax consequences based on where the taxpayer is physically located, E-commerce creates some challenges to tax systems that were designed with a different model in mind, lack of harmonized Laws and international Legal Instruments, legal requirements of traditional principles based on source, residence, permanent establishment, likelihood of double taxation & tax evasion

Suggested solutions include the Use of OECD Model Tax convention (the raft of bilateral tax conventions negotiated at global level, OECD Model Tax convention deals with Income and Capital tax, Downloaded goods/service or data such as software, audio or visual works the taxation mechanism can be based on Article 5 OECD, Article 7 of the OECD Model Tax Convention

provides that the profit of an enterprise of a Contracting State shall be taxable only in that state enterprise...

❖ **Electronic signatures, E-payment, Judge Dr. Ehab Elsonbatyon, Egypt**

During this presentation, the Egyptian e-law was presented as a case study and as follows:

- New digital signature law 15/2004 and the regulator (Information Technology Development Authority)
- Draft of e – commerce legislation as an enabling law
- Draft Law on “Regulating the protection of Electronic Data and Information and Combating Crimes of Information“
- Data Protection Law.
- Consumer Protection Law passed in 2006.
- Revision of international and regional commitment.

Recommendations of Dr. Ehab Elsonbatyon on Electronic signatures, E-payment include:

- The electronic marketplace will have to be governed by a clear set of rules, so that corporations, institutions and individuals can have confidence in doing business electronically
- Ensuring the safety and reliability of the system will be crucial.
- A country’s success in the e- era will depend on its ability to participate in the global knowledge-based economy
- There is a need for a comprehensive legal framework that covers: Cyber crime, E-commerce, E- transactions and Electronic signature.
- Existing laws should be reviewed and modified according to the new technologies and applications, including but not limited to: security – public order- penal codes - consumer rights – liability – data protection – money laundering – secrecy laws.
- Public and private sectors entities should take their responsibilities, in terms of
- Compliance, Investments in security, Exchanging information, Peering experiences and alerts, Spread the awareness between networks, Consulting with law enforcements.

❖ **Cybersecurity – Mr. Basil Udotai, Technology Advisers - ICT Lawyers, Nigeria**

Main Cybersecurity related issues:

- Intelligent systems and networks are being deployed across Africa for a wide range of services;
- Increasing Reliance on ICT by individuals, businesses and governments run personal, business and official government processes;
- On the whole sensitive and critical operations are being migrated online;
- As traditional law enforcement and security are impossible within these networks;
- And as ICT pose grave challenges to law and the legal process;
- Threats to individuals, businesses and governments are enormous – directly impact on the ability of ICT to deliver on the potential of economic growth and development

Given the particular nature of ICTs (Global; Knowledge based; Digital and electronic; Fast Paced and Real Time; Inherently Insecure; Interoperability as Standard; Mired by Legal Externalities - 3rd Party Devices; Anonymous; Unlimited Scalability; Fiercely Competitive; Cheaper Communication; Ever changing and continually evolving; Virtual but operates in the physical environment), the presenter recommended that Cybersecurity strategy should include:

- **Policy:** Must set out what to promote; prohibit and protect
- **Law:** substantive and procedural law criminalizing all undesirable activities, creating legal procedures for investigation, prosecution necessary for conviction;
- **Capacity Building:** both institutional and human capacity building geared at establishing technology, facilities and skills;
- **Public Private Partnership:** most critical networks are now privately owned and managed around the world, fast becoming the case in Africa. Thus, the need to build consensus, agree on standards, rules and best practices for cybersecurity;
- **Industry Cooperation and Alliance:** Industry must work together to build synergies around standard practices that promote a culture of cybersecurity in the private sector;
- **Public Enlightenment:** Must center around the nature and impact of cybercrime;
- **International Cooperation:** necessitated by the global nature of the network environment and the ability of criminals to operate across jurisdictions – good global framework – Cybercrime Convention

Main challenges presented were as follows:

- Reliance on existing criminal law and enforcement procedures;
- Who takes responsibility and leadership for cybersecurity at the national level?
- Which agency to entrust responsibility - the Single or multiple Agencies argument?
- Government lack expertise and skills at critical levels;
- Government ICT Agencies more interested in penetration and market based growth than security;
- Industry lacks interest and sees no state in pushing reform – business model based on a cost/benefit analysis;
- Global framework often perceived as neocolonialist;
- Need to put food on the table, build infrastructure, and cater to basic needs of the people – in Zambia cybercrime law was criticized as dealing with an elitist issue – Computers!

❖ **Data protection and privacy, Ms Alimata Dah OUATTARA, Commission Informatique et Liberté – Burkina Faso**

The main issue raised during this presentation focused on the fact that cyber laws should protect the fundamental rights of privacy of an individual. Through everyday transactions the Government and other entities end up collecting immense amounts of data from individuals and businesses. The law should provide a clear distinction on what constitutes personal data and what is termed public data. Personal data be treated with the appropriate level of protection and should not find its way to the public domain without express consent by the citizen. A case study of the Burkina Faso's special authority which main objective is to address issues of data protection and privacy in the digital environment was also presented.

❖ **IPRs and digital technology - Maitre Nafaa Laribi - Cabinet Faleh et Laribi – Tunisie**

Cyber law should cover the intellectual property laws that relate to cyber space and its constituents. This includes copyright law (in relation to computer software, computer source code), trademark law (in relation to domain names), Patent law in relation to computer hardware and software. The law should offer copyright protection of information duplication and distribution on the internet. The consequences and liability for copyright and trademark infringement should be clearly spelt out.

C. Subregional/ Regional Harmonization of legal and regulatory frameworks for the knowledge economy highlights on e-commerce, cyber crime, personal data protection), the case of ECOWAS- *Professor Abdoullah CISSE- Université de Bambey- Sénégal*

Prof A Cisse made a presentation on the work ECA has undertake with ECOWAS and UEMOA in formulating and harmonizing ICT legal framework for the ECOWAS region. The framework comprises a set of guidelines for e-commerce, cyber criminality and Personal data protection.

Prof Cisse presented the challenges faced, the process for the formulation and adoption, and results and perspectives, taking into consideration existing global frameworks and the need to adapt them to the African context. He also examined the responsibilities of various actors for the implementation at the regional and national levels. Considering the existing initiatives on the cyber laws at global, regional sub regional and national levels, the mechanisms for cooperation and sharing experiences were also discussed.

The following recommendations were made:

- Sensitization of different targeted categories of professionals/users thru elaboration of appropriate guides and organization of specific workshops.
- Advocacy for the decisions makers on the establishment of national committees for transpositions of the adopted frameworks at national level
- Organize capacity building programs on the formulation of cyber laws, e-commerce and protection in the cyber space (cyber criminality and persona data protection).

V/ Discussion on the adoption of a road map to facilitate implementation and improvement of Legal and Regulatory Frameworks at national & regional levels, moderated by Ms. Eskedar Nega, ISTD/UNECA

Participants recommended that in the area of e-legislations, ECA and its partners could support countries in the following areas:

- Awareness raising
- Human and Institutional Capacity building
- Networking and partnership

Facilitating the holding of sustained cyber legislation public enlightenment /awareness campaigns.

Besides the enlightenment of the public awareness campaigns could also target the private sector. The awareness programmes may also be extended to institutions within the business community focusing more on the advantages of using cost efficient communication technologies such as broad band, voice over internet protocol and satellite communication and the implications of online transactions. Once the public is aware of benefits of e-commerce then they can lobby the government to create the appropriate legal and regulatory framework. As alluded to before Africa is lagging behind in this area due to lack of financial resources. There are huge costs involved to set up and operate technology and ICT systems. Once there is public heightened awareness among captains of industry, then it will be much easier to encourage the private sector to play a leading funding role in ensuring that solid e-commerce legal and regulatory frameworks are in place.

Capacity building of e- commerce institutions and human capital.

In general only a small percentage of lawyers in Africa are familiar with cyber legislation. This is also true of the judiciary, staff in ministries and civil servants in relevant departments. It is important to introduce a sustained training programme suited to the needs of this category of professionals. This calls for a radical transformation in the education and training systems, science and technology policies and development strategies. Extensive technical and managerial capacity-building programs are particularly important in view of the need to formulate and implement policies, standards and develop a proactively supporting legal and regulatory environment. ECA may consider funding, or partnering donor agencies to fund continuing legal education modules on e-commerce in various African universities or other ICT centres of learning. These capacity building initiatives would guarantee the future of e-commerce in Africa.

Encourage co-operation and networking among African countries in the area of developing the cyber laws.

It is better to consider regional strategies rather than piecemeal approaches by individual countries for the transition to knowledge economies by African states. ECA should continue encouraging and working with the RECs, to coordinate efforts to harmonize and pass cyber crime laws within their regions. ECA could support the member states to translate international templates and regional draft cyber laws into national cyber legislation.

Recommendations also included the setting up of an electronic platform for training on cyber laws as well as the creation of a chair on African cyber laws, as a mechanism for sharing experience on sensitization, capacity building and research.



Annex 1 : Agenda

Workshop on Legal and Regulatory Framework for the Knowledge Economy

Agenda

Tuesday, April 28	
8:30	
9:00	Registration
10:00	<p>Session 1: Opening</p> <p><i>Chair: Sizo Mhlanga, Chief ICT Section, ISTD/ECA</i></p> <p style="padding-left: 40px;">Welcoming remarks, <i>Ms. Aida Opoku- Mensah- Director, ISTD/ECA</i></p> <p>Opening Remarks: <i>Mr Pierre Ouedraogo, Organisation Internationale de la Francophonie (OIF), Jon McNerney, Internet Society (ISOC)</i></p> <p style="padding-left: 40px;">Objectives, Themes and Expected Outcomes- <i>Ms. Eskedar Nega, ISTD/ECA</i></p> <p>Session 2 : Overview of Legal and Regulatory frameworks for the knowledge economy</p> <p><i>Chair: Mr Pierre Ouedraogo, Organisation Internationale de la Francophonie (OIF)</i></p> <p style="padding-left: 40px;">Setting the Scene- Legal and regulatory frameworks for the knowledge economy, <i>Ms Angeline Vere- Association of African Communications Lawyers</i></p> <p><i>Round Table I: Discussion on Current and emerging ICT law and policy issues</i></p> <p style="padding-left: 40px;">The UNCITRAL texts on electronic commerce and electronic signatures: an opportunity for the adoption of modern legislation in Africa, <i>Mr. Luca G. Castellani, UNICTRAL</i></p> <p style="padding-left: 40px;">E-jurisdiction, liability and dispute settlement, <i>Mr. Sam Dawa, Legal Informatics-Faculty of Law, Makerere University, Uganda</i></p> <p style="padding-left: 40px;">E-commerce and taxation, <i>Mr. Adam Mambi, Tanzania Communications Regulatory Authority</i></p>
10:30	Coffee Break

11:00 13:00	<p>Roundtable II: Discussion on Current and emerging ICT law and policy issues (Cont'd) – moderated by Mr. Dawit Bekele, ISOC- Africa</p> <p>Electronic signatures, E-payment, Judge Dr. Ehab Elsonbaty, Egypt</p> <p>Cybersecurity – Mr. Basil Udotai, Technology Advisers - ICT Lawyers, Nigeria</p> <p>Data protection and privacy, Ms Alimata Dah OUATTARA, Commission Informatique et Liberté – Burkina Faso</p> <p>IPRs and digital technology - Maitre Nafaa Laribi - Cabinet Faleh et Laribi – Tunisie</p>
13:00	Lunch Break
14:30	Session 3: Subregional/ Regional Harmonization of legal and regulatory frameworks for the knowledge economy
15:00	<i>Chair: Ms Sarah Kagoda-Batuwa, East African Community (EAC) Secretariat</i>
15:30	<p>Harmonization of sub regional legal frameworks (highlights on e-commerce, cyber crime, personal data protection), the case of ECOWAS- Professor Abdoullah CISSE- Université de Bambey- Sénégal</p> <p>Q&A session</p>
16:00	Coffee Break
16:30	<p>Discussion on the adoption of a road map to facilitate implementation and improvement of Legal and Regulatory Frameworks at national & regional levels, <i>moderated by Ms. Eskedar Nega, ISTD/UNECA</i></p> <p>Awareness raising Human and Institutional Capacity building Networking and partnership</p> <p>Closing Remarks by ECA, OIF, and ISOC</p>
17:00	
17:30	
18:00	

Annex 2

Overview of existing cyber law templates used in and outside Africa

International efforts are underway to tackle the most important policy issues regarding ICT development and international organizations such as the United Nations Commission on International Trade Law (UNCITRAL) have developed sample or templates of laws that nations to assist countries in developing legal and regulatory framework for e-commerce. These model laws are designed with particular attention to the need for uniform, balanced, equitable standards. In the field of cyber law the following are some of the existing templates that can be used in and outside Africa:-

UNCITRAL MODEL LAW ON E-COMMERCE (1996)

The purpose of the model law is to offer national legislators a set of internationally accepted rules as to how a secure environment may be created for electronic commerce. The principles expressed in the model law are also intended to be of use to individual users of e-commerce in drafting some of the contractual solutions that might be needed to overcome the legal obstacles presented by use of e-commerce. The law however, does not set forth all rules and regulations that may be necessary to cover every aspect of use of electronic commerce.

It is a draft law which has the essential procedures and rules for validation of contracts and data messages, interpretation of principles of contract such as time and place of contracting and formalities of writing and signature in so far as electronic transactions are concerned. The second part of the model law deals with application of electronic contracts of carriage of goods and transport. It is expressed in a technological neutral manner, so that it can apply not only to existing but future technologies. This model was adopted and used in drafting of cyber legislation in the Singapore Electronic Transactions Act 1998, South Africa Communication Act No. 25/2002 and Tunisia Electronic Commerce law (2000) inter alia.

UNCITRAL MODEL LAW ON E-SIGNATURE (2001)

The Model law was designed to assist states in establishing a modern, harmonized and fair legislative framework to address more effectively the issue of e-signatures. The law offers practical standards against which technical reliability of electronic signatures may be measured. The objectives of the model law include enabling or facilitating the use of e-signature and providing equal treatment to users of paper base documentation and users of computer based information which are essential for fostering the economy and international trade. The model law provides for the legal recognition of e-signatures and in Article 6 it goes even further as to provide for circumstances under which the legal requirements for a signature for commercial agreements could be satisfied by an e-signature. Article 8 provides that where an e-signature is used the signatory shall exercise reasonable care to avoid unauthorized use of signature creation data. The model was the basic reference point in the drafting of Russia's, Egypt and Japan's E-signature Acts and the USA Electronic Signatures in Global and National Commercial Act 2000.

COMMONWEALTH ELECTRONIC TRANSACTION ACT of 1999

This is also a substantive model law whose provisions basically states that under a law of the commonwealth a transaction will not be invalid just because it was conducted by use of electronic communications. The Australian and UK Electronic Transaction Acts are closely modeled along this Act and mirror the substantive provisions of the Act.

UNITED NATIONS CONVENTION ON THE USE OF ELECTRONIC COMMUNICATION IN INTERNATIONAL CONTRACTS (2005)

The purpose of the convention is to offer practical solutions for issues related to use of electronic means of communication in connection with international contracts. This convention applies to the use of electronic communications in connection with formation of contracts between parties in different states. It is however not necessary that both of those states be contracting state of the convention. The Convention applies when the law of a contracting state is the law applicable to the dealings between the parties, which is determined by the rules on private international law of the forum state, if parties have no validly chosen applicable law. It establishes the minimum requirements for electronic communication to achieve the same legal validity as traditional writing. It establishes that electronic communications should not be denied legal effect due to the way the information is presented or retained. It also provides that a contract formed by interaction of automated message and a natural person shall not be denied validity on the basis that an automated message was used.

THE COUNCIL OF EUROPE'S CONVENTION ON CYBER CRIMES (2001)

The Convention seeks to harmonise criminal substantive law element of offences and connected provisions in the area of cyber crime and also provide domestic criminal procedures powers necessary for investigation of offences committed by means of computer systems or evidence in relation to which is in electronic form. The convention focuses on the use of ICTs (computers) to commit

1. A range of traditional offences e.g. computer forgery, computer fraud and child pornography.
2. Engage in undesirable acts against ICT e.g. hindering the functionality of a computer system by deleting, deteriorating, transmitting or altering data.
3. and the data the process e.g. accessing of a computer without a right by infringing security measures to obtain data and interception of computer data.

Besides these international model laws at regional level a country can also adopt the

SADC MODEL LAW ON E- COMMERCE

The model law establishes the basic principle of non-discrimination between media or media neutrality. Key provisions of the model are drafted to establish equivalence between paper documents and electronic messages. It also includes consideration of electronic transactions, electronic signatures, and data protection and privacy.

Other jurisdictions that may wish to adopt legislative measures to facilitate e-commerce may base their cyber law on the models from other countries such as:-

TUNISIA ELECTRONIC EXCHANGES AND ELECTRONIC COMMERCE ACT OF 2000

I. electronic documents and	electronic documents and electronic signature considered
-----------------------------	--

electronic signature	as valid as the traditional written documents and signatures
II. National certification authority	Provides for the establishment and duties of National certification Agency
III. electronic certification services	Any person who intends to be registered to provide these services to be licensed by the Agency
IV. Electronic Commerce Transactions	The merchant should provide full information on a transaction before a contract is concluded this a consumer protection clause
V. protection of private information	The certification service provider may not process an individual's personal information without express approval.
VI. Infractions and penalties	Provides for penalties for non compliance with the act's provisions

SOUTH AFRICA ELECTRONIC TRANSACTION ACT 25/2002

i. Legal recognition of data messages	Computer generated documents placed on same footing as traditional legal documents
ii. Automated transactions	Refer to electronic transactions concluded by data messages
iii. Formation and validity of agreements	Agreements by means of data messages is concluded at time and place where acceptance of offer was received by the offeror.
iv. Cryptograph providers	Deals with registration of such services
v. Accreditation authority	The Act provides that the Director General in the dept of communication
vi. Unsolicited goods, service/communications	No agreement considered concluded if a consumer has not responded to unsolicited requests (spam)
vii. protection of personal information	The data controller should have the consumer's express permission to collect, collate process and store personal information.
viii. power to inspect , search and seize	The cyber inspector is granted these powers over any website of activity on any information system
ix. warrant of arrest	A magistrate or judge may issue a warrant of arrest if there is reason to believe that a cyber crime has been committed
x. Jurisdiction	The court has jurisdiction over acts committed in South Africa or whose effects are felt in South Africa

INDIA ELECTRONIC COMMERCE ACT OF 1998

I. Electronic records and signature	Provides that electronic records and signatures can be accorded the same level of legal recognition as paper records and signatures.
II. Integrity and authentication of secure electronic records and signatures	Defines specific categories of records and signatures that are afforded greater evidential presumption due to their reliability and trustworthiness.
III. Electronic contracting	Deals with the form in which an offer and acceptance may be expressed and legal recognition of electronic contracts.

IV. Effect of digital signatures	Addresses the legal issues related to the use of e-signatures.
V. Acceptance of electronic filing and Duties of certification Authorities	This section authorizes any department or ministry to accept electronic filing of documents. Also empowers any government department to specify conditions and procedures for electronic filing.
VI. criminal penalties	Provides penalties for internationally damaging a computer system, tampering with data, trespassing etc

AUSTRALIA ELECTRONIC TRANSACTION ACT OF 1999

i. Validity of electronic transactions	Provides that a transaction is not invalid because it took place wholly or partly by means of one or more electronic communications.
ii. Writing	If a person is required to give information in writing, that requirement is taken to have been met if the person gives the information by means of data message
iii. Signature	If the signature of a person is required, that requirement is taken to have been met in relation to an electronic communication an electronic signature is used
iv. Production of document	If a person is required to produce a document that is in the form of paper, an article or other material, that requirement is taken to have been met if the person produces, an electronic form of the document,
v. Retention	If a person is required to retain, for a particular period, a document that is in the form of paper, an article or other material, that requirement is taken to have been met if the person retains an electronic form of the document
vi. Time and place of dispatch and receipt of electronic communication	if an electronic communication enters a single information system outside the control of the originator, then, unless otherwise agreed between the originator and the addressee of the electronic communication, the dispatch of the electronic communication occurs when it enters that
vii. Attribution of electronic communications	Electronic communication, the purported originator of the electronic communication is bound by that communication only if the communication was sent by the purported originator or with the authority of the purported originator.

LIST OF PARTICIPANTS

Legal and regulatory framework for the knowledge economy workshop
 CODIST-I
 28 April 2009

No.	Name/Title	Organization	Email
1	Abdoullah CISSE	Universite de Banbey, Senegal	acissea@gmail.com
2	Simon Batchelor	Gamos	uneca@gamos.org
3	Eskedar Nega Program Officer	UNECA	enega@uneca.org
4	Roughiatou Thiam	INEADEC, Dakar, Senegal	roughiatou.thiam@ineadec.org
5	Selam Fekade Rodriguez	-	selam001@gmail.com
6	N'Dember Ange Herbain	Ministère des finances (Gabon)	dembert2@yahoo.fr
7	Briegitte Anguile- Diop	Ministère des Affaire Etangers (Gabon)	b.illassa@yahoo.fr
8	KAMDEM Emmanuel	ECCAC-ECCAS	kamdemmanuel@yahoo.fr
9	Dr. Leulseged Alemie	Ethiopian ICT Dept. Agency	leul_alemie@yahoo.co.uk
10	Houssein Ahme Hersi	Ministère des postes & Telecom	h-hersi@yahoo.com
11	Leonard O. Aloo	East African Law Society	l_aloo@yahoo.com
12	Ehab Elsonbaty	Expert-Egypt	eabelsonbaty@hotmail.com
13	Justusole Naituriae	Kenya Embassy	topoika@yahoo.com
14	Mamadou Karambé	ORTM - Mali	karamadou@yahoo.fr
15	MBA Ndong	Ministère des	mba.ndong@finances.gouv.ga

No.	Name/Title	Organization	Email
	Jérôme	Finances (Gabon	
16	Godfred Frempong	Science and Technology Policy Research Institute	goddie58@yahoo.com/gh
17	Basil Udotai	Technology Advisors, ICT Lawyers, Nigeria	basil@ta.com.ng
18	Baligr Belgacem	TTN	baligar.belgacem@tradenet.com.tn
19	Djibril Traore	ONP – Mali	djibriltraore2005@yahoo.fr
20	John Kieti	NACC – Kenya	jkieti@nacc.or.ke/jkieti@gmail.com
21	Dr. Mouhamadou Lô	Adie – Senegal	mouhamadou@adie.sn
22	Abigail Thabete	Dept. of Land affairs	athabethe@dla.gov.za
23	Michael Murungi	ICT Lawyer – Kenya	mmurungi@kenyalaw.org
24	Ben Akoh	OSIWA	bakoh@osiwa.org
25	Zaidi Zied	Tunisian Embassy, Addis Abab	zaidizied@yahoo.fr
26	Judith M. C. Tembo	Communications Authority	jtembo@caz.zm
27	Shirega Minuye	Women’s Information Services and Networks org	contact_wino@yahoo.com
28	Mzwandile R. Mabuza	Swaziland Posts & Telecomms	regulator@sptc.co.sz
29	Ambrose Ruyooka	Ministry of Information & Communications Technology (ICT)	ambrose.ruyooka@icit.go.ug / ambrose.ruyooka@gmail.com

No.	Name/Title	Organization	Email
		– Uganda	
30	Pikeli Essodessewe	Autorite de reglementation du secteur des postes et des Telecommunicatio ns, Togo	artp@artp.tg /pikeli@artp.tg
31	Amoussou Cosme	Avocat (Benin) TIC	amo-cosme@yahoo.fr
32	Adam Mambi	TCRA – Tanzania	adammambi@yahoo.co.uk
33	Sam Dawa	Makerere Univeristy	dawa@law.mak.ac.ug
34	Sarr Abdou Abbas	Cabinet SARR, ALLARD Associès, Côte d’Ivoire	sarr.abdou@sarr-allard.com / sarr.abdou@aviso.ci
35	Lebbaz Larbi Abdelfettah	Embassy of Algeria in Addis Ababa	lebbaz79@yahoo.com
36	Patrick Bahizi Mutimura	Rwanda Development Board Director/Legal Affairs	patrick.mutimura@rita.rw
37	Egué-Kraidy Marie-Laure	Agence Ivoirienne de Coopération Francophone	marla_eg@yahoo.fr
38	Jean-Paul Awuor	Publications and Conference Management Section. UN/ECA	jawuor@uneca.org
39	Nankep Pierre	Agence Nationale	pierre.nankep@antic.cm/lnankep@yahoo.fr

No.	Name/Title	Organization	Email
	Lotis	des technologies de l'information et de la communication (ANTIC), Cameroun	
40	Kofi Benning	Ministry of Communication – Ghana	kofi.benning@moc.gov.gh
41	Violet Nkambule	University of Swaziland	violet@science.org.swa.sz
42	Desmond Koroma	UNFPA-LO, Addis Ababa	koroma@unfpa.org/deskoroma@yahoo.co.uk
43	Aynew Washelegne	JHU – Tsehai	aywashe@yahoo.com
44	Hailu Mideksa	Ethiopian Television	hailu_mideksa@live.com /gelila.hailu@gmail.com
45	Menelik Yabowork	InfoMed Technology	meneliky@infomedtec.com
46	Getachew Jemaneh	Addis Ababa University	getachew-j@yahoo.com
47	Daniel Minillu	Hawassa University	danminillu-2004@yahoo.com
48	Tigist Eneyew	Systems Africa	tigist@esystemsafrika.com
49	Ouattara Alimata	Commission de l'Informatique et des libertés du Burkina Faso	alimatadah@yahoo.fr
50	C. Kwajok	Sudan Embassy – Addis	jada@ties.itu.int
51	Danio Miguel Augusto	Angola – NCIT	danio.augusto@cnti.gov.ao

No.	Name/Title	Organization	Email
52	Folake Olagunju	ECOWAS	folagunju@ecowas.int
53	Carmelo Modu	EQ Guinea – Ministry of Transport, Post and ICT	carmelo.modu@gmail.com
54	Isaac K. Kwarko	NCA, Ghana	isaac.kwarko@nca.org.gh /kobina.kwarko@gmail.com
55	Issa Tangara	SOTELMA	taniss@sotelma.ml
56	Mohamed A. Boncana	AGETIC	mboncana@agetic.go.ml
57	Ahmat Mahamat Gamar	MPTIC/Tchad	ahmatgamar1@yahoo.fr
58	Ngnanone Payanfou	Tchad/MPTIC	payanfou@yahoo.fr
59	Faradj Mahamat Djaddr	Chad	djadduelhadjfaradj@yahoo.fr
60	Abdelkader Taled	Morocco	morocco.emb@ethionet.et
61	Mohamed Timoulali	ECA	mtimoulali@uneca.org
62	LOKO C. Theodore	Benin	cthloko@yahoo.fr
63	Adelmonem Kioua	Tunisie	veille.juridique@planet.tn
64	Nafaa Laribi	FL-Avocats / ISOC Tunisie	mafaa.laribi@flavocats.com
65	Malonga Albert	Ministère de la Recherche scientifique Congo	malonga-malga@yahoo.fr
66	Ngoulou Boniface	Recherche Scientifique Congo – Brazzaville	ngboni@yahoo.fr
67	Sizo Mhlanga	UNECA	smhlanga@uneca.org

No.	Name/Title	Organization	Email
68	Jon McNerney	Internet Society / www.isoc.org	mcnerney@isoc.org
69	Luca Castellani	UNCITRAL	luca.castellani@uncitral.org
70	Sarah Kagoda-Batuwa	East African Community Tanzania	sarah@eachq.org, sarahkago@yahoo.com
71	John Kariuki	National Communications Secretariat, Kenya	kariuki-jn@yahoo.com
72	Sam Dawa	Makerere University	dawal@law.mak.ac.ug
73	Adamu Mombi	TCRA, Tanzania	adammambi@yahoo.co.uk
74	Susan M. M. Mulikita	Communications Authority Zambia	smulikita@caz.zm
75	Jean Marie Noah	Telecommunications Regulatory Board of Cameroon	nojemar@yahoo.fr
76	Abdisemed Mussa	Pathfinder International	amussa@pathfind.org
77	Jea-François Lebihan	ITU	jean-francois.lebihan@itu.int
78	Eshetu Alemu	Eth. Telecom Agency	gm@eta.gov.et
79	Christine Runnegar	Internet Society	runnegar@isoc.org
80	Dawit Bekele	Internet Society	bekele@isoc.org
81	Ibrahim Sangho	Ministère Santé Mali	ibrahima.sangho@yahoo.fr
82	Djibriel WADE	Africable – Mali	djibwade@yahoo.fr
83	Lamine Mahamadou	AGETIC – Mali	lamine@agetic.gov.ml

No.	Name/Title	Organization	Email
	DIALLO		
84	Filifing Diakite	Primature – Mali	filifing@primature.gov.ml / /filifing@gmail.com
85	Deborah-Fay Ndlovu	Research Africa, South Africa	dfn@research-africa.net ; deborahfayn@gmail.com
86	Crystal Orderson	South African Broadcasting Corp. (SABC)	sabcnews90@gmail.com
87	Angeline Vere	Telecel	avere@telecelzim.co.zw
88	Pierre Ouedraogo	OIF	pierre.ouedraogo@francophonie.org
89	Bola Elegbe	African Development Bank	s.elegbe@afdb.org
90	Joseph Mwangi	Ministry of Information and Communication	jmwangi@information.go.ke
91	Sami Faîz	PragmaCom	info@pragma-com.com
92	Afewerk Temtime	ISTD/UNEA	atemtime@uneca.org