

South Sudan to Embrace African Union Commission's Knowledge Economy Initiative

Friday 6 July 2012

By John A. Akec

July 7, 2012 - I have good reason to be optimistic that Africa is about to bid farewell to its old but well-trumpeted image of underperforming in everything economic, including being counted, until recently, amongst world's least digitally connected continents. That Africa is about to miss all the benefits that digital and ICT-powered economies can offer. It has also been most convenient for many opinion leaders to differentiate between what they call countries of Sub-Sahara Africa (or Africa proper with all the implied laggardness, excepting South Africa from this broad brush); and the countries "north of Sahara" such as Egypt, Libya, Tunisia, Morocco, Algeria, and Mauritania; which they implicitly regard to be on the same pulse and at pace with the rest of the developed and developing world. Knowing what initiatives Africans are currently debating, nothing could be farther from truth.

Africa on March towards Information Society

I was greatly encouraged and privileged to attend a recent consultative workshop jointly organised by African Union Commission and UN Economic Commission for Africa in collaboration with Regional Economic Communities (SADC, COMESA, EAC, and IGAD) on Africa-wide harmonization of cyber security legislation. This workshop took place in Addis-Ababa between 20th and 22nd June 2012. During the workshop, I sensed that the frequent dichotomization of Africa into "worst off Sub-Sahara" and "and not-so worst off North of Sahara" is being frowned upon by a new generation African policy-makers, legal experts, legislators, IT professionals, law-enforcement and security agencies representatives, academia and civil society groups.

The new viewpoint in town, I came to conclude, regards such characterizations of Africa as misleading at best, and at worst as an outmoded divide-and-rule tactic – a hung-over from the colonial past - that is still being deployed by few, albeit increasingly isolated voices, to undermine the continent's new found self-confidence and discourage African nations from exerting a concerted effort in order to fully and fruitfully participate in the global economy that is increasingly knowledge-based and information-driven.

Contrary to the aforementioned skeptical view, African professionals- North and South of Sahara- now realise that they are all together in it. That a coordinated action by AU member states on issues of global concern (be that cyber security, a united action on climate change, or creating environment for information society that increasingly use communication technologies to do business over the internet or via a cell phone) is the best way forward.

In fact, many African watchers, commentators, and well-wishers are in agreement that Africa, as never before, is well positioned to shine in the third millennium. And they are right to think so.

The E-Economy's Unparalleled Opportunities

The advent of information age at the back of computer and communication technologies (facilitated by spread of mobile phone and internet connectivity) has brought along huge benefits for all our economies, especially for the countries that have invested heavily in ICT infrastructure as well as human and institutional capacity to manage it.

Now from the comfort of our homes, many of us can chat with friends on social networks such as Twitter and Facebook, apply for jobs online, check our bank accounts, transfer and receive money, sell and buy goods on the internet, compare prices of merchandise on different markets, book air ticket and a hotel room at destination, send and receive emails to and from business associates while on the move; all of which would have been unthinkable only two decades ago.

With convergence of communications systems with computing, television, radio, and entertainment as demonstrated by I-technologies (that is, I-phone, I-pod, and I-pad) led by Apple, Samsung, Blackberry, Microsoft, Google, Amazon, and others; information is now truly ubiquitous- available for the 'digitally-connected' however they want it, wherever they want it, and whenever they want it.

Challenges and Risks of Knowledge Economy

Information society and its twin companion, knowledge economy, do not come risk-free but pose new challenges. Hackers, or information highway men, are increasingly able to access and steal sensitive information stored on computer systems over

internet. The information often belongs to individuals, organizations, governments, and businesses. Hence, identity theft is now commonplace. Companies' product designs, trade secrets, intellectual property, and contracts information remain vulnerable to espionage activities from within and from without- over computer networks. Expert and often self-taught computer nerds with time in their hands in far-flung corners of the globe frequently develop viruses, worms, and malware which they dispatch with great skill over the worldwide web and electronic mail to affect thousands and even millions of computers around the world, wreak havoc and disrupt the operation of vital utilities on which livelihoods depend. Terrorists can also use the internet to coordinate activities and pose threat to national security for countries of all sizes, varying technological, institutional, and military capacities. Individual human rights often risk compromise when personal data is being gathered, transmitted, processed, stored, and used.

To understand the magnitude and scale of cyber crime, a study by Symantec Corporation (Mountain View, California, USA) in 2011 estimated a global annual financial cost of astounding USD 338 billion in direct monetary terms and lost business opportunities due to cyber crime, which far outstripped the global black market dealings in marijuana, cocaine, and heroine all put together in that year. The same study revealed that in every second, 14 adults fall victims to cyber crime, or 1 million adults every day.

Possible Remedies to Cyber Crime

In order to combat cyber crime (that is, crime that takes place over internet and facilitated by using computer systems and networks), while promoting electronic commerce and protecting intellectual property and personal data, national laws must be enacted to prosecute criminals and define in no ambiguous terms what activities in cyber space constitute a breach of national and international penal laws and codes. There should be means and institutional arrangements in place responsible for detecting, reporting, investigating, and prosecuting perpetrators of the computer-based crime. And since cyber crimes can be committed by offenders living outside the national boundaries of their victims (the crime scene), international cooperation in investigating cyber crime becomes a must in order to successfully bring the perpetrators to books. Whenever possible, harmonization of cyber laws and IT policies between countries must take place without sacrificing national sovereignties of the countries concerned.

This sounds all well and good, but it is a tall order. And sadly, many countries and institutions are not aware, let alone being prepared to deal with risks associated with our increasing dependence on ICT. The good news being that the recent AU Commission and UN Economic Commission for Africa sponsored consultative workshop on cyber legislation is a call to arms for AU member states to address the threat posed by cyber crime.

The AU Commission Response

For three consecutive days, a multidisciplinary team of 80 experts representing IT profession, lawyers, legislators, policy-makers, defence establishments, law enforcement agencies' and private sector, academia, and civil society met at UN Conference Centre in Ethiopian capital of Addis Ababa, to debate a draft AU Convention on Cyber Security Legislation; share experiences of national cyber legislations enactment, international best practices and cooperation in combating cyber crime; discussed the utilization of ICT technologies such as public key infrastructure (PKI) and digital signatures for safe and secure transaction on the internet, and building of human and institutional capacity in areas of cyber security, among others.

The workshop deliberated on the draft AU Convention. The 58-page and 4-part draft convention document covers organisation of electronic commerce, protection of personal data, combating cyber crime, and common provisions dealing with implementation and monitoring mechanisms of the convention once adopted by Member States.

If all works according to plan, the Convention will be adopted by the next round of meeting of AU Ministers of Telecommunications and ICT scheduled to take place in September 2012. In the meantime, Members States are urged to express views, consult with stakeholders, and send comments to drafting committee by mid July, 2012 at the latest.

Workshop Recommendations

The meeting also came out with recommendations that included calling on Member States to enact laws for combating cyber crime; regulate electronic commerce; invest in equipment and communication infrastructure; embark on human capacity building in IT and communication sector, and law enforcement agencies; build institutions responsible for policing cyber space and combating cyber crime; adopt appropriate controls that would reduce risk and permit secure and efficient transaction over computer networks; protect personal data during transmission and processing; protect intellectual property, and create an enabling environment for knowledge economy; provide e-services to their citizens, and realise e-governance; integrate cyber security into national IT strategies, high-level policies, and action plans; and train lawyers and prosecutors on cyber laws and investigation of cyber crimes.

The experts meeting also urged Member States to support dotAFRICA top level domain (TLD) and actively participate in activities organised by international body responsible for internet governance (ICANN – International Corporation for Assigned Names and Numbers, a non-profit body responsible for management of internet domain names, IP addresses, and root name

servers), and embark on mass sensitisation programmes to raise awareness amongst institutions, government decision-makers, businesses, and the general public about opportunities and challenges that are associated with information society.

Operationalisation of South Sudan Top Level Domain Name (.SS)

South Sudan was represented at the consultative workshop by Engineer Stephen Juma Lugga, the Undersecretary of the Ministry of Telecommunications and Postal Services, Mr. Lam Jock from Ministry of Defense and Veteran Affairs, and the author of this article as an academic.

The trio had an opportunity to meet with Ms. Anne-Rachel Inne, ICANN's Africa Regional Relations Manager, discussed with her the steps and procedures needed to be taken by South Sudan to implement the already approved South Sudan top level domain name (.SS). The meeting was fruitful and will speed up South Sudan operationalisation of country's top level domain (.SS TLD).

There was a warm welcoming atmosphere through the workshop for South Sudan's team from the organisers and participants who showed eagerness to assist South Sudan to get on its feet and participate fully in AU Commission professional activities.

What South Sudan needs to do?

South Sudan needs to take immediate steps to build its human and institutional capacity in order to create an enabling environment for knowledge economy, and enact cyber security legislation. The country should urgently set up a national telecom operator, operationalise country's gateway, and set up a national telecommunications regulator. Institutions and organisations within the country need to recognize the importance of IT by creating directorates or IT departments dealing specifically with IT-related concerns, including cyber security. Judges, police, and law enforcement agencies need to be trained on investigation, prosecution, and combating of cyber crime, and protection of personal data and intellectual property. Public-private partnerships must be encouraged to develop IT solutions that the national economy needs to thrive and to provide e-services and e-governance to citizens.

The government of South Sudan will also do well to introduce ICT at all levels of education starting from nursery and primary school and upwards, and support training schemes that will raise the levels of ICT literacy across the population and economic sectors.

Most important of all, the President of the Republic, Lt. Gen. Salva Kiir Mayardit, needs to set the tone for a national ICT vision, strategy, policy, and action plan for the next five to ten years; and commit resources to embracing and operationalising the AU's knowledge economy initiative.

**Dr. John Apuruot Akec is the vice chancellor of University of Northern Bahr El Ghazal and chairperson of Academics and Researcher Forum for Development, a think-tank registered in South Sudan. He edits a blog bearing his name at www.JohnAkecSouthSudan.blogspot.com. He can be reached at www.unbeg.edu.sd*