KICTAnet

Online Discussions

Internet Governance

eDiscussion Report

April 27th – 9th May 2009

Acknowledgments

It is yet another successful deliberation from the KICTANet community. As this was the second discussion on Internet Governance issues, it was more detailed, passionate and engaging. We therefore wish to thank the all participants for the time and effort they put to contributing openly as well as attentively to the concerns that affect our ICT industry. Your thoughts and insights have made all of us more informed and better equipped for the unfolding Information Society. God Bless you.

J. Walubengo and M. Njiraini, Moderator,
KICTANet, Online Collaboration Programme.
jwalubengo@mmu.ac.ke, mwende.njiraini@gmail.com
10 August 2009

Table of Contents

Executive Summary

KICTANet commissioned the 2nd online discussion on Internet Governance, aiming to continue raising awareness of the global Internet Governance issues while reviewing corresponding country positions based on new developments. Specifically, discussions were centered around Infrastructure & Content Issues (Undersea Cable, ccTLDs, IXPs, IPv6), Cyber-Security (Consumer and Data Privacy, National Security Strategies) and Socio-economic issues (ePayment Platforms).

The anticipated landing of several undersea cables on the East African Coast raised discussions on the impact (or lack of) these would have on Access, Affordability, Content and Quality of the Internet Service. It was felt that reliable and affordable last-mile (Local-Loop) solutions would need to be provisioned in order to realise affordable Internet Services. The current mobile (3G) service was welcome but not sufficient to drive down the costs as much as Fiber-To-The Homes (FTTH) and Fixed Wireless technologies would. In other words, International Bandwidth prices may drop but expensive last mile solutions would continue to justify high costs of Internet services – even with competition at both the local and international market layers.

With regard to the Quality (Broadband) Issues, participants felt that Quality of the Services was subjective and an aspect of User expectations and Usage patterns. However, members agreed that Broadband Service was a factor of BOTH Reliability and Affordability. Providing reliable but expensive (exclusive) services would therefore fail the test of Broadband services. Furthermore, it was noted that most Service Providers gave poor contention-ratios on their uplinks to the Internet leading to highly degraded Internet services.

The discussion on the management of the Country Code Top-Level Domain (ccTLD) was one-sided with most participants registering their reservation about the new law that required all second-level domain registrars to be licensed. This issue continues to remain cloudy particularly because the Regulator is yet to publish the regulatory details of how a

split dot.KE registry would be managed as well as the criterion for applying, approving and revoking licenses.

With respect to IPv6 some participants felt that it was not important while others warned that it was a threat in terms of missing opportunities that the next generation internet presents. The role of the Internet eXchange Point (IXP) was widely acknowledged and the Government departments challenged to move content online in order to enhance and optimise the use of the Kenyan IXP.

With regard to Security, it was noted that the provisions of KCA (amendment) Act, 2009 represented the primary threats, an indication that the government recognized cyber security related issues. However, a culture of cybersecurity could be established through management tools such as data classification, security awareness training, risk assessment and risk analysis. These tools would facilitate the identification of threats, classification of assets and rating of assets vulnerabilities in order to implement effective security controls. In addition Users should be encouraged to develop a culture of reading terms and conditions websites – particularly eCommerce based sites.

Participants indicated that privacy and security on the internet was usually not a concern until a user encountered an infringement. Resolution to violation to right of privacy and security was limited by the fact that most citizens do not have the time or money to start legal proceedings. 'Social re-engineering' was proposed as the best method to overcome these challenges.

The determination of the level of cybersecurity preparedness was emphasized given that the availability of high capacity and quality international bandwidth delivered by submarine cable would increase the vulnerability of services and networks in the country. It was proposed that the level of cybersecurity preparedness could be determined with use of the ITU National Cybersecurity/critical information infrastructure protection (CIIP) Self-Assessment Tool. Additionally, participants supported the establishment of the national CERT using the public private partnership (PPP) model.

Participants noted that the national and regional Internet Governance Forums were an indication of the success of the IGF in providing an inclusive governance process. Participants supported the continuation of the IGF as it was based on a multi-stakeholder processes and provided a globally unique environment for a constructive and open exchange of ideas.

Introduction

Background

Several of the East African Countries held their 1st National Internet Governance Forums in 2008. The main objective was to raise awareness and update most of the stakeholders on the issues as debated at the International stage. This year, the focus should be to consolidate the understanding of the issues and boldly stating positions that may have been previously ambiguously defined.

Program Setting and Description:

The online deliberation on the IG issues was run for two weeks on the KICTAnet and other regional lists. The lists have ICT stakeholders from various backgrounds including Academia, Government, Civil Society, Media, and Telecommunication Operators among others. The discussion was preceded by face-to-face meetings.

Program Design (Data Collection, Data Processing)

Data Collection:

The online discussion will be structured along the following themes that will be discussed electronically over a period of 2 weeks

- General Background (1day- Moderator: John Walubengo)
    - IG Definition and Rational
    - National IG Forum :- 2008 Status Report
- Infrastructure Issues (4Days- Moderator: John Walubengo)
    - Undersea Fiber Cable and its impact on: (2d)
        - Access, Affordability, Content and Quality
    - Management of Critical Internet Resources (2d)
        - IPv6 and Country code Top Level Domain (ccTLD) Management
        - National IXPs/NFOB
- Cyber-Security and Trust (4Days- Moderator: Mwende Njiraini)
    - e-Crimes against (2d)
        - Consumers/Users (Privacy Issues)

        - Data and Infrastructure (Data Security)
    - Developing a national cyber-security strategies (2d)
        - What are the Legal Provisions (KCA Act 2008?)
        - Developing National Cyber-Security Strategies(CSIRT)/(CERT)
- Socio-economic Issues (2Days - Moderator: John Walubengo)
    - ePayments (MPESA, ZAP, Digital Certificates)-(1d)
    - Regulating a Converged Environment-(1d)
- Closure and Way Forward (1Day- Moderator: Mwende Njiraini)
    - Examine the desirability and continuation of the IG Forums.

Data Processing:

The various contributions from the Participants were analysed and collated into a Final report.

Aim

To continue raising awareness of the global Internet Governance issues while reviewing corresponding country positions based on new developments.

Objectives

The Objectives of the exercise included:

- To raise awareness of global Internet Governances (IG) issues
- To review previous year country positions in light of new Policy, legal, Technical and other developments.
- To build consensus and new positions regarding IG issues

Main Outcomes/Deliverables

The key outcomes of the exercise included:

1. Summarised eParticipants contributions
2. Final Report for subsequent dissemination to members and other stakeholders

Tools

Online Tools (email, listserver, Internet)

Face2Face Workshop

Resources.

1. Moderators (Online)
2. Participants (Online)

3. Web Resources:
    - Listserver (KICTANet) archives
    - Referenced websites

eDiscussion Proceedings (2 week Discussions)

Theme 1: General Background and 2008 Report (1Day)

Day 1: Internet Governance-Rationale and 2008 Report

Introduction

John Walubengo, the **Moderator**, welcomed members and kicked-off the Internet Governance discussions by saying that the Internet was no longer restricted to being a technical issue but had grown into a global, socio-economic resource affecting all types of stakeholders. The rules, procedures and practices governing the use and evolution of this (internet) resource should therefore be the concern of everyone. At the moment, the governance of the internet was heavily skewed in favor of developed countries in the north and the World Summit on Information Society 2000 (WSIS 2000) attempted to discuss how this could be rectified. Through the UN, WSIS suggested the formation of the Internet Governance Forum (IGF, www.intgovforum.org) to continue the deliberations on how governments, civil society, media, academia, telcos and other stakeholders could have a say and influence the evolution of the internet.

He added that IGF has since held 3 global summits to deliberate on the management and governance of Internet Security, Internet Critical Infrastructure, Internet Access, Internet Crime among other issues. Last year in Kenya, Internet Governance issues were discussed at a national level followed by the hosting of the regional E.A. Internet Governance Forum in November 2008. He said that the Key Achievement realised included:

- Raising Awareness of Internet Governance (IG) Issues
- Exploring Alternate views and solutions on contentious issues
- Hosting the EA IGF meeting

- Establishing locally relevant IG issues

While notable challenges included:

- Failure to launch the IG Course which was to be offered jointly by Strathmore and Multimedia University College(formerly KCCT)
- Failure to have a "Government" position on contentious issues at the IGF, Hyderabad 2008 Meeting

He then invited members to share their comments.

Solomon Mburu said that moderator's comments had set the pace for the discussion and he believed that with the summary offered, there was a better chance of understanding and practically demystifying the challenges regarding Internet Governance (IG), which were not clearly defined in legal documents, such as the Kenya Communications (Amendment) Act, 2009.

He predicted that Kenyans would pressurize Members of Parliament (MPs) to either develop a Data Protection Act or still amend the KCA in favour of local ideas and protecting these ideas from infringement.

Theme 2: The Infrastructure issues of IG (4Days)

Day 2 and 3: Undersea Cable and its Impact

Introduction

The **Moderator** stated that the days' theme was to interrogate several assumptions about the long awaited submarine cable(s) that are poised to hit our coastal city of Mombasa. SEACOM, TEAMs, EASsy are all expected to be operational starting July 09 (SEACOM), TEAMS (Sep 2009) and EASSy (2010?)

He then shared his take/opinion on their impact based on a scale of Low(1), Moderate(2) and High(3) as given below:

I. Access: Score=1, Low Impact on Access

The undersea cable is a top-tier infrastructure that has no impact at the (User) Access level. The user access level is a function of the maturity of the domestic (local) infrastructure. Unless this is developed proportionately, Kenya may have an awkward situation similar to a country with top-notch Universities (Submarine cable) but no Primary and Secondary Schools to provide the continuous supply of students (no Access).

II. Affordability: Score= 2, Moderate Impact on Internet Service Costs.

It is expected that the prices are likely to go down from the current retail levels of about 2500USD per 1MB to between 500-1000USD per 1MB of bandwidth. However the **Moderator** had serious doubts as to whether these prices would be sustained at these low levels given that investors would be seeking a Return on Investment (ROI) targets that anticipate a huge uptake of the bandwidth. In the likely event that the expected uptake fails to happen, he predicted that prices may begin to go up by the end of the 1st year of the cable operation. The investors in the cable may then begin to 'milk' the few subscribers who may have jumped onto the highway in order to cover the cost of the capital sunk into the cables. The Moderator gave the example of the SAT3 where the submarine fibre cable which landed in the West African region had little impact on pricing.

III. Content: Score=1, Low Impact on Content.

The Moderator noted that digital content should be independent of infrastructure. In his opinion the submarine cable was not a prerequisite for the availability of lecture notes in digital form. In addition the submarine cable was not a prerequisite to digitizing government records. Content is intricately related to eventual cost of internet service and ideally should be fully developed before the landing of submarine cable.

IV. Quality: Score=2, Moderate Impact on Internet Quality.

"Broadband Quality of Internet" is what every service provider is advocating for. But Broadband standard in Kenya is way off the mark when compared to India or Europe. Though the **Moderator** remained skeptical he foresaw that the undersea cable having moderate impact on quality because of the poorly managed domestic user and telecommunication networks. Most telecommunication networks may act as gateways to the submarine cable are infected by viruses, spam, proxies, and ill-configured servers, routers and switches that introduce congestion and bottlenecks rather than facilitate broadband access to the submarine cable.

Sam Gatere stated that he agreed with the low assessment on the impact the cable would have on access since the glorified undersea cables are actually top tier and not landing at his house or office! He proposed that the submarine fibre optic capacity needed to be demystified to the end user. In his view possible ways of getting access and broadband access to the end user would possibly be facilitated by triple play providers such as Zuku who were offering Internet as well as other info-tainment products.

On affordability and specifically to the Kenyan scenario **Sam** thought the PPP (Public Private Partnership) model would ensure some form of 'Public Good' service that safeguards the end user and cushions them from possible exploitation by infrastructure investors. He cited the SEACOM venture that has the private sector players such as Safaricom. Safaricom already offers "broadband" Internet services. If they benefit from high speed Internet through this SEACOM partnership the end user in this case may actually enjoy faster, more reliable Internet access.

With regard to the impact of the cable on local content for Sam thought it was a sorry or sad state of affairs. He agreed that content should be independent of infrastructure. Local universities developing digital content would benefit from digitizing knowledge and finding new ways of learning and delivering the same.

Victor Gathara stated that he had been involved in the drafting of a preliminary report on the impact of the sub-marine cable on development in Kenya. He agreed with Moderator's assessment of the impact of the submarine cable but stated that cables presented an opportunity.

In his assessment the access score on a scale of 1 to 5 would be 2 given that the mobile phone companies will be in a position to offer internet access at a fraction of the current cost. He expressed concern with who would take full advantage of this (given that he agreed with the Moderator's score of 1 with regards to content). However, he did not foresee bandwidth prices going up given the number of cables expected to land as well as the players in the market. In his opinion content would be king and therefore dictate pricing.

Victor proposed the inclusion of another category that deserved analysis and that was important for development. He said Kenya seemed to be banking on the Business Processing Outsourcing (BPO) sector. Companies such as Safaricom had launched call centres. However, he proposed that there should be more effort concentrated on 'Back Office' kind of activities such as data entry, digitization, animation, etc and less on customer interaction services like call centres. He felt that in the midst of the current global financial recession, companies will not want to be seen exporting jobs abroad. In addition it was not wise for the country to blindly copying the India model of the BPO sector.

In conclusion, **Victor** stated that the key thing was to have a shared vision of where Kenya wants to achieve with the initiatives in the business sector given the existing disconnect between stakeholders. He proposed that a truly active national association (may be KICTANet) would assist in developing a comprehensive ICT Park strategy and facilitating collaboration between industry and universities. He then promised circulate the preliminary report to Listers for comment

Brian Longwe stated that access was not merely an infrastructure related issue. Though it was true that the submarine cables impact tier 1 it was also true that most of the deployed access infrastructure is currently under-utilized. Brian noted that there were over 100,000 households with ability to access Asymmetrical Digital Subscriber Line (ADSL). However, due to the cost associated with these services only a fraction of the households, probably 2,000-3,000 actually subscribe to it.

With regard to pricing, **Brian** said that the expected impact on pricing would be between US$200-$400 per MB (wholesale for ISPs), this would further be forced downwards by the high competition that both shareholders as well as bulk customers of the cable systems would bring to the marketplace.

He urged participants not to forget that TEAMs was a 'developmental' cable system that is it's investors were not aiming to making any money from the cable rather their aim was to deliver the commodity (bandwidth) to their marketplace at the lowest possible price, then make their returns from better margins that they achieved in the market. Contrary to many people's expectation, there was a chance that broadband access might be very close to free.

With regard to content, specifically on content vis-à-vis infrastructure, he felt this was a chicken and egg situation. In his opinion with the availability of infrastructure there would be few or no more excuses for the lack of local content. Bottom line is, that Kenya has lots of creative talent that needs to be harnessed as well as numerous business opportunities for content aggregators who would source and sign up various types of content and put it onto the new networks.

With regard to the poor score for broadband Quality of Service (QoS), he argued that the poor rating was off the mark. He stated that the watershed that these submarine cables will bring, plus the almost limitless amounts of bandwidth that will be available would have an incredibly impact on quality. All the 'pent-up-demand' that has been created by the terribly slow satellite systems currently used would be released. Consequently, there

could be an explosive increase in use - with a massive increase in overseas multimedia and web 2.0 services. Hopefully this will gradually become more localized as many of the content delivery networks set up local nodes for mirrored and 'local presence' service equivalents.

Bill Kagai doubted Brian's statement about the TEAMS project being “developmental” rather than “profit” oriented. In his rejoinder **Brain Longwe** said that there were a number of different ways to go about major infrastructure development:

1. For-Profit: Putting together a business case with a clear Return-On-Investment (ROI) benefit; looking out for funding, then building and deploying. Hopefully the market would respond well and the investors get their return (e.g. SEACOM).
2. Means-to-an-end: Determine the total costs for the project, approach the primary stakeholders; Oil companies in the case of oil pipelines, gas companies in the case of gas companies, operators and ISPs in the case of bandwidth; sell them the concept of delivering the commodity to themselves at cost (or as near to cost as possible); set up an "Operations and Maintenance" structure which levies the same parties; build and deploy; once the bandwidth is delivered it's a "free-for-all" in the marketplace - with ‘costs’ at a very low level, prices would eventually follow due to competition (e.g. TEAMs and EASSY)

He said this is was one of the main reasons why projects such as TEAMs and EASSY have faced stiff opposition, criticism and outright attempted sabotage – because they have the potential to cut the feet out from under any similar commercial venture.

In response **Bill Kagai** stated the following

1. For Profit - Seacom -This sounded like a brilliant business and economic model.
2. Means-to-an-end - TEAMS: Referencing his university economics this option appeared as the only economic model they did not teach at the University of Nairobi an institution established by an Act of Parliament.

In summary, he felt that TEAMs had already waged a price war with no products in the market yet and was skeptical that TEAMs would indeed be cheaper than SEACOM in terms of costing internet service.

Faima Basly shared her observations gathered from forums she had attended:
Access: If access was looked at purely from an individual perspective then it would be seen as low (Score 1) and clearly not realize the benefits of having an undersea cable at all. There are already signs of high demand for increased bandwidth if complaints from consumers today are anything to go by. This must then feed the notion that with the undersea cable would find ready users apart from the corporate and SOHO (Small office home office) variety. This then in the appropriately competitively structured market that would trickle down to apartment buildings and soon into the suburbs.

Furthermore, she said, with 'clever' government subsidies targeting structured learning institutions (schools, universities, libraries) habits could be built and carried over by students. However, she hoped that demand would match supply. **Faima** thought that with the proliferation of lower cost high-end mobile phones in Africa and the readily available Chinese 'wannabe' models, access would be readily facilitated. This may not speak much for computer literacy but that may be the price that would have to be paid.

The issue of affordability would be relative in her opinion. It will be two fold; from the perspective of the provider and from that of the user. She was certain the providers would have their numbers worked out and it would now be a matter of waiting for the uptake from the consumers end. Apart from running Business Processing (BPO) or media houses she stated that it would interesting to see how other businesses responded to better priced internet bandwidth when their main concern was emails. **Faima** noted that the internet was being curtailed during working hours even in the developed world as a result of the distraction it caused to staff through applications such as facebook and chats. In some extreme cases because of availability of internet on mobile-phones some employers were restricting the use of phones to tea-breaks and lunch hour, as all

communication could be done via email and landlines. Given this scenario she wondered if majority of the existing business would 'jump on the bandwagon' when the sea cables landed.

With regard to content **Faima** disagreed with the score given (1). In her opinion the minute connectivity becomes available and affordable then a lot of sharing would begin and would be pleasantly surprised as to the gems that may be unlocked. Content would in itself need to be shepherded and managed. She would therefore be looking forward to contributing to the upcoming online discussion on content.

In her opinion content development would take on 'a monkey see monkey do' approach as has been the case in the developed countries where once people understood the essence and the scope of content the country may well take the lead in Africa. After all Kenya was a reference point for many in East, Central and parts of Southern Africa and with the entrepreneurial spirit this would be a matter of time. On this basis on a scale of 1 to 5, content would have score of 2.

Mwende Njiraini shared her views as follows:
With regard to content: She disagreed with the statement that "digital content should be independent of infrastructure". Without the availability of reliable connectivity it would be impossible to deliver the content to the intended recipients. If for example the health fraternity would wish to implement tele-medicine, digitizing the content is the first stage while delivering the content over a reliable broadband network is the second stage. She was sure none of us would want to be misdiagnosed on the basis of an image for delivery that has acquired errors in transmission.

In her view broadband quality was highly subjective and dependent one's internet usage patterns, for example those interested in audio or video streaming would demand higher quality. Network operators may employ bandwidth/traffic management techniques to meet user demand. This has resulted in the debate of network neutrality[1]; in the United

[1] http://www.circleid.com/posts/print/network_neutrality

States for example, the network neutrality is one of the most contentious debates on the telecommunications policy. This debate has ensued as Internet firms such as Google, Yahoo and eBay on one hand seek to have non-discriminatory access to network infrastructure written in to law and regulation. On the other hand telecommunication and cable network operators such as AT&T, Verzion and Bell South perceiving Internet firms as 'freeloaders', accruing profits at their expense, are seeking to have legislation established that would let them charge additional fees for use of their networks[2]. Network neutrality may not be of concern to us at the moment as we focus on facilitating universal broadband on an open access basis. However this may change as network operators see their 'hard earned' broadband connectivity 'chewed' up by applications that they themselves do not offer[3].

Michuki Mwangi had the following comments to make:
With regard to access**:** He believed that there was a need to move beyond the marketing hype into the realities. In his opinion, there was no broadband in Kenya. In his understanding broadband means affordable and fast connectivity. What available was Average-to-Unreliable connectivity that cost more than it was worth.

He felt that the despite the ongoing investments in wireless solutions, the country could be held in the pre-broadband phase for a long time. He added that mobile broadband seems to be a working solution but its ability to scale-up would continue to pose challenges on quality. Therefore investment in fixed infrastructure solutions like fibre to homes and corporate organizations would be important considerations to be made if the country was to leap into broadband phase.

With this in mind, it would be ideal if regulators would open up the last-mile (within residential areas) to anyone interested to investing in that space with fixed infrastructure. The de facto point here was that for a long time residential access has been neglected for

[2] http://www.washingtonpost.com/wp-dyn/content/article/2006/02/06/AR2006020601624_pf.html
[3] http://www.washingtonpost.com/wp-dyn/content/article/2006/01/21/AR2006012100094.html

a long time as the focus had been mainly at corporate level within the central business districts (CBDs) until the mobile 2G and 3G solutions were introduced. He said that policy had a role to play in providing incentives for players who make efforts in providing fixed infrastructure in residential locations.

With regard to affordability **Michuki** felt that the pricing would remain high until an inexpensive local loop solution was found. As far as the cables goes it would be good to know more details before users could make any conclusions. For instance is the $500-100 per month for Bits or Bytes? It would be good to know what pricing model the cable operators wanted to have in place for instance would one buy a data circuit from point A to B and does it come with or without internet?

He said that selling circuits was the ideal way to go since it allowed operators and others players to buy large pipes STM1 (144 Mbps) for example from Nairobi to London. It was cheaper to buy transit capacity from London at a price of about $10 per megabyte (MB) per month the other costs will be for the circuit back to Nairobi and that can be low if talking of big pipes. But then the models are not clear it becomes difficult to make conclusions.

With regard to content Michuki said that the only way we could drive up content availability is by placing the requisite infrastructure. As it stands, very few stakeholders host content locally since the pricing is high and facilities are few. He estimated that the total collocation/hosting capacity available in Kenya as being well under 2,000m^2. In comparison to Europe one company Telehouse had 30,000m^2 of data-center space, with 20,000m^2 being in the United Kingdom.

Kenya had some advantages in this area - for instance cheap land and professional labor that was not comparable to European Union rates. The only expense was power however Kenya has abundant supply of solar energy that could serve the demand for green data-centers that could be built. Michuki brought to the attention of participants to the fact the Europe had ran out of hosting space since 2006. This situation had led to the emergence

of Asia as the next collocation destination. He argued that region should realize that it could be the home to the world's future data centers with low cost energy, land and labor in our favor. With the hosting of local and international content locally costs would be driven down to levels previously not imagined.

With regard to quality**: Michuki** said the quality of service would improve subject to the following;

1. Better and affordable local loop infrastructure (rather than oversubscribed wireless/mobile base stations): He understood that the regulatory licensing structure had a negative impact on this as operators had to pay an annual fee per installed site. He suggested fixed wired solutions that had no recurrent costs as the way to go.

2. Increased percentage of locally hosted/accessed content (peering traffic) which was subject to less contention and better access speeds.

3. Better pricing models on transit capacity which will reduce the contention ratios given by service providers.

4. More training of engineers in building scalable services and routing infrastructure.

Mwende Njiraini reacting to **Michuki's** statement that "there was no broadband in Kenya and making reference to a case in the UK where Wanadoo accused by the rival service providers (BT Group and Telewest) of "...confusing consumers by promoting services with speeds of 150kbps or 256kbps as Broadband"[4], said that there was a need to define the term "Broadband".

[4] http://news.bbc.co.uk/1/hi/technology/3563320.stm.

Secondly, she shared an article that provided a good reason why there was need to seriously consider local content development. The article stated that companies such as Youtube, Facebook, Myspace which had large audiences in developing countries, Kenya being no exception. These countries however had limited and expensive broadband thus generating little advertising revenue and requiring more resources (servers, bandwidth). To reduce costs associated with providing services some internet companies have taken "the drastic step of cutting off developing countries" from accessing their services![5]

Harry Delano reinforced **Michuki's** earlier assessment of the state of affairs with regard to the country's current "Broadband connectivity" by exploring the two key factors of affordability and quality.

With regard to affordability the landing of the Submarine cable, there was need for a cost benefit analysis. The analysis would be broken down and synthesized to enable the addressing of the present challenges that curtail broadband connectivity in this country, notably: international bandwidth pricing models and local loop costing. He said that the internet service vendors basically passed on the high recurrent costs in addition to markup on these two fronts to the end users. This was the main reason that internet connectivity had for a long time been a privilege of the few who could afford it therefore eluding the majority.

While the first cost element might be mitigated by the advent of several international fibre circuits, users expected some transparency on the pricing models of international bandwidth to determine the specific cost passed on to end users per MB/MBPS. He said that as things stand now, this was a grey area and in as much as international bandwidth costs remained high for service providers, consequently the end user bill may be inflated.

Secondly, **Harry** stated that while different players worked to build up capacity on the last mile, tangible benefits on the local loop costing were yet to be passed on to end users.

---

[5] http://www.nytimes.com/2009/04/27/technology/start-ups/27global.html?_r=3&partner=rss&emc=rss

He felt that it made no sense to talk of expanding capacity on broadband, when a 64kbps local loop on fibre (from one local Public Data Network Operator (PDNO)) would for instance cost only 5 - 8 % less than what Ken-stream (Telkom Kenya) had been charging before the advent of fibre. He added that PDNO's needed to wake up now, and realize that they had to reach the largely untapped market rather than concentrating on the already over saturated corporate sector.

With regard to quality, he said that the current contention ratios in this market were too high, and had a negative impact on quality of the connectivity. He expected that this would be mitigated by the availability of increased international bandwidth and supported **Michuki** on the need to building our technical/engineering capacity to take advantage of most of the emerging technologies.

Mwende Njiraini, in her contribution to the discussion on residential broadband access, she stated that installing fibre for last mile access involved a substantial commitment of fixed costs, mainly associated with civil works. To reduce this capital cost, some municipalities were installing multiple 'dark' fibre as it was economical to install substantial excess capacity, relative to initial demand. One such initiative was by the city of Stockholm, in Sweden, which owns and operates an Open and Operator-Neutral infrastructure for telephone and data communications, under a city chartered company, Stokab.

She stated that Stokab was founded in 1994 when the telecommunications sector was fully liberalized due to the reluctance of the incumbent operator to meet the demand for high capacity networks. Since then, the company has provided fibre optic infrastructure on an open access basis to service providers and large businesses including telecommunication operators, ISPs, cable television networks, mobile telephone operators, municipalities, county councils, major banks, insurance companies, multi-sited organizations and media companies based in the commercial districts and industrial areas of Stockholm.

She added that the aim of the company was to contribute to making Stockholm an ICT capital by lowering the barriers to market entry for service providers, and therefore increasing competition. The guiding philosophy for the establishment of the city network was that telecommunications infrastructure should be provided as a 'public good' facilitating access to advanced communications services to all citizens. Stokab's open access network (OAN), hoped to contribute to improved welfare and greater efficiency of municipality services, reduce the need to travel and thus ease traffic congestion ultimately contributing to a better environment. She concluded by stating that this was an initiative that municipalities in Kenya may wish to emulate.

Barrack Otieno agreed with **Mwende** saying her idea was great and timely. He added that local councils could generate revenues in terms of rates which were unfortunately being squandered through fictitious procurements. He argued that it was important to involve the local councils as key stakeholders in the infrastructure business since they had a say with regard to jurisdiction issues in the municipalities.

Day 4: Management of Critical Internet Resources

The **Moderator, John Walubengo** introduced IPv6 and Country code Top Level Domain (ccTLD) Management the subject of discussion on the 4th day by giving a brief background as follows:

1. IPv6: is the new protocol (procedure, standard) for any device (PC, phone, server, camera, etc) communicating over the internet. The old protocol IPv4 is set to reach its limit in the next 2 to 3 years time. The prominent item with these protocols is a unique number allocated to each device that wishes to communicate over the internet. These numbers for IPv4 are getting depleted and will be exhausted by 2011/12/13 depending on which scientists you subscribe to.

   Issue: Put in bread and butter terms, if organizations wanted to extend internet communication to new branches in 2011/12/13, would only be successful if the Kenyan social and techno-structure was ready for the IPv6 transition. The

moderator sought to establish the country's readiness in terms of technical know-how to transition devices, networks, applications, users, etc onto the new IPv6 platform. The country's status and whose responsibility was it to ensure readiness for the transition to IPv6 or if was ok to wait until 2011.

2. Top Level Domain: There is a reserved internet name of each country for example KE for Kenya, .UG for Uganda, and so on, which by extension cover corresponding sub-domains such as xyz.co.ke, xyz.ac.ke, xyz.or.ke, etc. The moderator invited views to establish the management of domain names in other countries. For example the Ugandan, the .UG namespace was created and managed by a private individual while in Kenya, the top level domain name, .KE is managed by Kenya Network Information Centre (KENIC), www.kenic.or.ke, under a Public-Private Partnership.

   Issue: The management of the Kenyan .KE namespace was set to change or has changed in accordance with the recently enacted Kenya Communication Amendment Act (KCA Act 2009). Under the provisions of the Act the .KE namespace would be exclusively managed by the Regulator, CCK. The Moderator invited views to establish if this arrangement was good or bad for the internet community and the participants' opinion on the ability of the regulator to disable websites.

In his contribution **Solomon Mburu** stated that KENIC is charged with .KE domain names registration. This is indeed an important step in promoting local content which is faced with a lot of challenges, due to the preference of western ideas. If the regulator, CCK in this case, decides to shut down a domain, then that means the regulator's needs will only put up what they think is better according to their estimation. Solomon argued that while it was fine for the content to be controlled, it would be against the freedoms enshrined in the constitution.

He stated that CCK had no business disabling any .KE domain in the absence of legal

parameters put in place to sufficiently control such media. In his opinion, the local content is under threat as more and more (especially the upcoming domains) would rather be .COM instead of .KE. This in his view was not the best way to promote local content development.

In her contribution, **Mwende Njiraini** encouraged participants to review an IPv6 Presentation[6] titled: "IPv6 research highlights" done by participants of the Diplo Foundation Internet Governance Capacity Building Programme at the IGF in Hyderabad. The presentation provided a good introduction to the issues that needed to be considered in the adaptation of IPv6 namely

- Introduction: What is IPv6, and do we really need it?
- IPv6 Transition: What are the technical, economic and developmental aspects of the transition?
- IPv6 Main Players: Who are the main players in this field, globally, regionally and nationally?
- National Case Studies: What is happening in different countries? (Kenya included – may be not as detailed!)

She invited participants to acquit themselves with the AfriNIC IPv6 Policies for allocations and assignments[7].

With regards to the .KE ccTLD, the Kenya Communications (Amendment) Act, 2009[8] section 83D states that: No person all update a repository or administer a sub-domain (presumably .co.ke, .ne.ke, .or.ke, etc) except in accordance with a license granted under this act. Currently, the ccTLD domain is managed in the interest of the local internet community. The objective of KENIC is to "promote, manage and operate the delegated .KE ccTLD in the interest of the Kenyan Internet community, being mindful of the global Internet community interest in consistent with Internet Corporation for Assigned Numbers and Names (ICANN) policies." **Mwende** sought to contributions to the following questions:

6 http://diploedu.diplomacy.edu/poolbin.asp?IDPool=798
7 http://www.afrinic.net/docs/policies/afpol-v6200407-000.htm#5

- What in your view would be the criteria that organizations/institutions will need to satisfy in order to be licensed to act as repositories or administrators of .KE sub domains?

  In her opinion the organizations/institutions should first and foremost act in the interest of the 'local internet community'.
- What do you think would be the effect of separately managing sub domain on the existing public private partnership model that has been used as international best practice [9].

Finally, she drew the attention of participants to presentation titled "*Evolution of KENIC and Overview of the Kenya Communications (Amendment) Act of 2008*"[10] proposed for presentation at the KENIC AGM scheduled for 8th May 2009.

The **Moderator** thanked participants for useful links shared with regard to ccTLD management especially in light of the move to an exclusive regulatory regime.

In his contribution on IPV6, **Michuki Mwangi** stated that the word ADOPTION rather than transition should be used because IPv4-based networks will still be existence for at least another two decades if not longer.

He reiterated that end-users were ignorant of the IP version they were using and that a majority of them had no clue what an IP address was. Only operator support staff was conscious of its role. It was likely therefore that this status quo would remain as is for a long time.

There was however a need for a mechanism to ensure that consumers bought "IPv6-compliant" devices and software upgrades. To illustrate this Michuki gave the example of old/legacy equipment found its way into some developing countries and granted a second-life through deployment in networks.

---

8 http://www.communication.go.ke/media.asp?id=775

9 http://www.itu.int/itudoc/itu-t/workshop/cctld/035r1.pdf

Taking into consideration these factors he sought participants' views on whether this should be left to the ignorant consumer or should someone up the chain be in a position to regulate what comes into and does not come into the market.

With regard to ccTLD management, **Michuki** stated that each country was entitled to develop its own operational, management and governance models as long as it was consistent and acceptable to the Local Internet community. The definition and constitution of the Local Internet Community (LIC) was left to the country to determine. However in most cases the stakeholders carry the day as the Local Internet community. He gave examples of countries within the African region, Tanzania, South Africa and Mauritius which have reviewed their models to those they deem consistent to the interests of their Local Internet communities. For such changes to be implemented clear engagement of the community must be demonstrated to ICANN and the IANA.

He noted that the KENIC experience was no different and that it was interesting to note that KENIC was listed under IANA as the management of .KE ccTLD[11]. This means that any changes in the management of the .KE domain must arrived at through consensus in the LIC and a formal application made to effect this change.

Michuki understood that the Kenya Communications (Amendment) Act 2009 intends to license management of sub-domain registries, in his view this was confusing. There was no clear objective in the proposed split of the registry and the impact that this would have on operators who manage .co.ke, .ac.ke and go.ke independently. He invited participants to review the South African experience to establish why that country was moving away from a split registry to a single registry and learn from their experience.

He stated that if the intention of the law as to license the registrar (ISP or other organizations engaged in domain registration on behalf of others), his opinion was that

---

10 http://www.kenic.or.ke/2009_KENIC_AGM_Programme.pdf

11 http://www.iana.org/domains/root/db/ke.html

licensing has its pros and cons and this may not have a positive impact on the growth of the namespace. If on the hand the intention was to license every domain registrar (every domain owner) then in his opinion that would be absurd!

In conclusion, he stated that the management of the ccTLD determines its success. For example .EG and .ZA were both entered in the Root-Zone in 1990 have today recorded tremendous success. The .ZA has over 500,000 domains while the .EG though small had 6,000 domains in 2006. The KENIC model has managed to grow from 1,200 to 10,000 domains in a span of 6 years (from Feb 2003 to Feb 2009). While this growth remains disproportionate to the population its relatively comparable to Internet penetration. Consequently, changing the model may have its pros and cons.

Michuki raised concern on the need for research/study to assess the impact of the proposed changes. He stated that essentially all changes to the ccTLD operations/management should aim to make the name space efficiently available (ease of registration), interesting (new second levels, auctions for hot names – creates attention around the namespace) and certainly affordable. He warned that anything else would break the growth momentum the ccTLD has worked hard to build and taking into consideration that many other factors come into play for there to be an interest in registrations at the ccTLD level.

Victor Gathara in contributing to the IPv6 stated that he was fearful that the adoption of IPv6 would be similar to the 'y2k' bug scenario. In his opinion there was seemed to be much ado about nothing and sought to be corrected on his opinion that the adoption problem was for the boys (and girls:) who sell devices, operating systems and applications? He wandered why should he should be worried if he regularly 'upgraded' or 'patched' his system or if he was still running Win 3.1 (or the Linux equivalent) and had no need for the internet?

With regards to .KE namespace, **Victor** stated the concern with the regard to implementation of the provisions of the Kenya Communications (Amendment) act was

the competence of regulator, CCK in the management of the namespace. In his view the custodian of what is for our collective good (read government) is the reasonable choice. Legislation should be clear on under what circumstances CCK can act and cannot act on .KE.

In response **Evans Kahuthu** to **Victor's** contribution on IPv6, he stated that there was no need to worry over another 'y2k'-like scenario resulting from the switch to IPv6 because in his understanding the technology behind IPv6 has been tested under what was IPv5. In addition, some of the vendors have their software supporting both IPv4 and IPv6 simultaneously to ensure seamless transition.

Regarding, who should be worried about the adoption of IPv6, **Evans** agreed with **Victor** that the end user should not be worried about implementation rather it is the vendors that needed to ensure that their products support IPv6. However, it was his opinion that some end users might experience problems adopting IPv6 due to problems including but not limited to: absence or lack of manufacturer support or impossible software update.

Day 5: Critical Internet Resources, IXPs and NOFB

The **Moderator** started the day's discussion by 'breaking down' the jargon

IXP: stands for Internet eXchange Point, similar to a telephone exchange point, where calls within a particular town, district, province or country are aggregated and routed. An IXP is similar to a telephone exchange as it aggregates internet traffic within a town, district, province or country. Typically, if a country lacks an IXP, then calls/internet traffic destined for a neighbor across the street would end up being routed across expensive international links and then back into the country for delivery.

Issues with regard to IXP: Kenya is fortunate to have a national IXP; however the issue is whether it is being used optimally. How many service providers exchange local traffic at

the IXP? Secondly, of what use is the national IXP if most users are interested in and target foreign content such as yahoo.com, gmail.com, facebook.com, etc rather use similar services available in the country?

NOFB: Stands for National Optical Fiber Backbone. The Kenyan Government under the implementing arm of Kenya ICT Board has been building the domestic fiber cable connecting all districts in Kenya. The fibre is expected to improve and extend access uniformly across the country. Eventually, e-Government services would be accessed over these networks.

Issues with regard to NOFB: Private telecommunication operators have always felt that the government has no business in deploying infrastructure across the country/cities. They feel it is unfair competition brought in to distort the telecommunication market – the general feeling being that it would be more efficient for government to lease fiber links from existing telecommunication operators?. There is concern with regard to the operation and management of this domestic network. How would this fibre optic network co-exist or is it intended to eventually replace the IXP that is currently run by Private Sector?

In her contribution **Crystal Watley** stated that there is a tug of war over the roll out and provision of service, meanwhile the Wananchi (citizen) continues to suffer for lack of access. She requested both the government and the private sector to begin to consider the pressing needs of the people for information and come to definitive agreements so that implementation can take place.

With regard to the subject of local content and international websites **Crystal** stated that if more Kenyans outside of Nairobi had the ability to access the Internet and the skills to design websites under the National IXP, we would see more traffic within the country. In this case, it seems as though selection of a very small portion of the population was considered as representing the entire country. She argued that success of the IXP would only be established after more Kenyans had access.

With regard to NOFB, **Crystal** noted that though the market is good at producing a number of benefits, the provision of public goods is its downfall. In her view is it critical at this time of developing the ICT industry of Kenya that we are reaching out to the people to build their skills and introduce the Internet as the educational and business tool it has the power to be. At the moment more than 90% of all Internet use is in Nairobi and Mombasa and the reminder of the country remained unconnected.

Contributing to the discussion, **Michuki Mwangi** stated that the KIXP has had a great impact in Internet scene in Kenya. There are currently 27 peering members with aggregate traffic during peak times averaging 45mbps.

In his view this was not optimal utilization in view of the overall total transit (what is not passing at KIXP) capacity in Kenya. Therefore a greater percentage of traffic is international

Given this scenario what then was the role of the exchange. In his view the online submission of tax returns and participation in IPO such as Safaricom would require a stable local internet infrastructure that was independent of both the international cable and satellite connections.

In his view the following were missing dependencies:

1. With increased penetration (number of subscribers) there is bound to be an increase in traffic to 100mbs and higher - hence the availability of affordable access for non-corporate users and more residential users online.
2. Local content hosting would require the building of more collocation facilities. This would attract CDNs who are keen to do edge caching and require reliable hosting services. It also would mean that there will be a market opportunity for collocation hosting services.
3. E-government: Michuki called to the attention of participants that Kenya Revenue Authority (KRA) has more traffic at the KIXP than some well known service

providers. It therefore meant that there was a need for more e-government traffic.

4. Creativity on relevant content including e-government and free SMS website. He said that the collapse of Sasanet was a pity as the service provider had considerable traffic at the KIXP.
5. E-learning and e-commerce would attract home users to get online during off-peak hours. Michuki found it interesting that development of web content had been skipped in favour of mobile content. He proposed engineering mobile content solutions to work for the web.

With regard to NFOB **Michuki** stated that the government approach must be appreciated. He was pleased to hear of the issuance of a license to Kenya Power and Lighting Company (KPLC) that would enable the company to sell the extra capacity on its fibre infrastructure. He argued that other companies such as Kenya pipeline company (KPC) and Kenya Railways should take a similar approach as the availability of fibre optic cable capacity would result in lower access costs.

He therefore encouraged companies such as KPLC, Telkom Kenya Limited (TKL) and city/municipal councils to lease out sections of their poles to fiber/cable infrastructure builders. He stated that the building of the last mile in respect to telecommunications was imperative in achieving complete access. He argued that if there was a lot of fiber in the ground, it would not really matter who runs it. The person who runs it would be the one who can raise the highest revenue for the investor in a highly competitive market space.

Responding to the Moderator claim, **Michuki** stated that it was not possible for such an infrastructure to replace an IXP. This is because even with very cheap dark fibre, it would be a logistical nightmare and financially unrealistic to maintain close to 30 connections to each provider one wished to exchange (peer) traffic with. It was therefore financially viable to have one connection to a single location where operators would connect to other operators via a layer 2 switch. In this case, operators would only pay for the half circuit to the IXP location and manage one link.

Shem Ochuodho clarified that KPC was actually granted an interim license in 2004.

In his contribution **Thomas Senaji** stated that the optimal utilization of the national IXP and any other exchange would largely depend on national communities of interest that would be driven by initiatives in e-commerce and other e-applications within the country and in the East Africa Community (EAC) region. This brought to mind local content as one of the drivers of a vibrant IXPs. In a nutshell, Senaji stated that promotion and proliferation of e-applications with the underpinning need for content are necessary.

With regard to NOFB, Senaji stated that international benchmarks (read Malaysian multimedia super corridor, MSC and Estonian, IT College for ICT human resource development) indicate that governments take deliberate actions to deploy infrastructure including ICT infrastructure to stimulate growth. In this regard, the focus should be on principles of equal and non-discriminatory access to such infrastructure as is the case in countries that have implemented such projects. With such an approach, entrepreneurs should be able to leverage on the infrastructure for innovation across all sectors of the economy.

Theme 3: Cybersecurity and Trust (4Days)

Day 6: eCrimes, Privacy, Privacy and Data Security

Cybersecurity and trust in the use of the internet were the focus of the second portion of the online discussion. Day 6 addressed issues related to privacy[12] and data security.

As an introduction the **Moderator Mwende Njiraini,** stated that Kenyans frequently register to use various online services provided by the government and businesses. This registration process requires that disclosure of personal information including physical, postal address, telephone numbers, credit card numbers, etc. Additionally, the younger generation and the young-at-heart are readily sharing "personally identifiable information[13]" including photos and events through social networking sites including facebook, youtube, myspace, flickr, twitter, etc.

Personal information collected and made available in the public domain such as the electoral register, telephone directory can be combined with information for example from supermarkets loyalty cards to create valuable market information to track individual preferences and purchase profiles. This information may unfortunately be subject to abuse and theft. Consequently, 'trust' in policies[14] and the security measures that the government and businesses establish to protect user information is therefore an essential element for the success of e-transactions[15] (both e-government and e-commerce)

---

12 Protecting your Privacy on the Internet: http://privacy.gov.au/internet/internet_privacy/index.html#2

13 Office of the Privacy Commissioner of Canada: Protecting Your Privacy on the Internet: http://www.priv.gc.ca/fs-fi/02_05_d_13_e.cfm

14 Privacy Policies: http://www.facebook.com/policy.php?ref=pf, http://twitter.com/privacy

15 http://www.diplomacy.edu/ISL/IG/

The day's discussion sought to address the following questions:

- How can we create a cyber security culture in Kenya? What is the role of the educators, peers and parents[16] in digital literacy with respect to privacy and security?

- Does the current legal environment provide for the protection of privacy on the internet? How can we establish a balance between security and right to privacy[17]?

In his contribution **Evans** stated that the purpose of Information Security/Cybersecurity is to protect an organization's valuable resources, such as information, hardware and software. Through the selection and application of appropriate safeguards, Information Security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. The issue of cybersecurity/Information security simply comes down to three things: 1) Confidentiality, 2) Integrity and Availability.

Information Security management/cybersecurity entails the identification of an organisation's information assets and development, documentation, and implementation of policies, standards, procedures and guidelines, which ensure their Confidentiality, Integrity and Availability.

Unfortunately, cybersecurity is sometimes viewed as hindering the mission of the organization by imposing poorly selected bothersome rules and procedures on users, managers and systems. On the contrary, if well implemented, Cybersecurity rules and procedures can support the overall organizational mission.

In the case of Kenya, the way to create a culture of cybersecurity is through management tools such as data classification, security awareness training, risk assessment and risk analysis in order to identify threats, classify assets, and rate their vulnerabilities so that

16 Privacy illustrations: http://www.priv.gc.ca/information/illustrations/index_e.cfm

17 Article 12 of the Universal Declaration of Human Rights :http://www.un.org/en/documents/udhr/index.shtml#a12

effective security controls can be implemented.

In response **Judy Okite** stated that there was a need to create a culture of reading of the terms and conditions on the websites. This she emphasized would form the first line of defense. However, availability of personal information on the internet without a person's is a separate issue. Another means of creating a cyber security culture in Kenya was capacity building (for lack of a better word) with regard to online sharing of personal information. This should be addressed when introducing users to the internet to ensure that they were comfortable with the information that they shared. In Judy's words "whatever kind of information, that is online, just make sure you will still be proud of it 10 years to come, this will define you...whether it's true or false....your have just created your online profile!"

In response to Evans and Judy contributions the Moderator stated that privacy on the internet is usually not a concern until one encounters an infringement. For example theft and misuse of personal information held by the government, bank, school, employer, local supermarket, etc, may result in irritating phone calls/emails from a telemarketing agents who have gained access to your shopping patterns through loyalty cards or a surprise phone call from a long lost friend who has just seen your photo in an online version of 'fashion police'!

Unfortunately, most citizens do not have the time or money to start legal proceedings in this regard. Consequently, 'social re-engineering'[18] has been proposed as the best method to overcome the challenges associated with infringement of privacy. This involves exercising your right to opt-in or out, carefully reading privacy policies and end user agreements.

---

[18] Social engineering is "a term that describes a non-technical kind of intrusion that relies heavily on human interaction and often involves tricking other people to break normal security procedures" or "the act of manipulating people or exploiting people's weaknesses to gain unauthorized access to secure information, assets, or facilities".

Social re-engineering is "the act of ensuring that the people-aspect of the information security spectrum is well taken-cared of".

In his contribution, Henry Delano stated that the country had in the last 10 years experienced exponential growth in the ICT sector with the advent of internet and later the mobile technology. It is expected that the landing of undersea optic fibre cables was an important milestone in this sector that promises to significantly open up the local 'cyber space' and revolutionize virtually all sectors of the economy. Henry reiterated that despite the fact that the country was set to accrue benefits arising from the undersea optic fibre cable there was need to prepare and put into place properly co-ordinated measures to mitigate the challenges that will arise with this connectivity specifically cyber security.

The undersea cable provides an opportunity for high speed cyber based crimes including network security breaches (hacking), identity thefts, data thefts, Denial of service (DOS) attacks, cyber espionage activities and others. Simply put with the availability of international fibre a typical smart hacker sitting across the room will have the capability of accessing your personal computer and data in less than 50 milliseconds. Slow and congested international internet connectivity via satellite frustrates many would be hackers and other cyber crime activities. Consequently, the country's cybersecurity capacities have not been challenged and tested to the limit, to assess their capabilities. He stated that the country 'cyber-peace' currently enjoyed might be short-lived.

In his observation the local cyber space is witness locally generated cyber crime activity. Thus it is expected with certainty that 90% - 95 % of this cyber crime traffic emanates from beyond its borders. With End user systems that are poorly secured, or not secured at all this exposure is likely to spell a disaster-in-waiting, especially for sensitive institutions and organizations.

A number of key national infrastructure and installations have embraced embrace technology and are getting online becoming potential targets for a cyber attack that seek to sabotage provision of essential services. It is therefore imperative that security be an inbuilt feature in these infrastructures and installations. The ministry under whose portfolio ICT lies, is key in formulating policy and security standards for all arms of

government. The policy and standards should be regularly reviewed to keep pace with the ever mutating challenges in this arena.

Efforts geared towards establishing a national cyberspace security strategy would be needed. The wide array of expertise and talent in the private sector could assist in the drafting of this strategy and in the establishment, enforcement and monitoring of compliance to the various cybersecurity standards and benchmarks.

The **Moderator** drew the participants' attention to the Information Security Management System (ISMS) ISO/IEC 27001[19] certification which organizations may wish to consider seeking. The certification includes the following elements:

- Security Objectives
- Information Security Policy
- Security Organization
- Asset Classification and Control
- Personnel Security
- Physical and Environmental Security
- Computer, S/W, Data, Operation, and Network Security
- System Access Control
- Systems Development and Maintenance
- Business Continuity Planning
- Compliance

Solomon Mburu in his contribution sought to know if subscription to mobile and online payment platforms such as ZAP, m-Pesa or Magic pay, meant that one was selling one's

[19] http://www.iso.org/iso/catalogue_detail?csnumber=42103

privacy to the firms offering these services and if these firms were making subscribers' privacy their 'property'. In his users ranging from 'mama mboga' and to CEOs did not bother to acquaint themselves with the terms and conditions usually made available in 'small print' when subscribing to any cyber-related content or service. He noted that cyber products must be clearly explained especially with regard to the privacy.
He reiterated that the passing of the Freedom of Information Act should be supported by the enactment of a Data Security Act. The posting of the draft Freedom of Information Act and the draft Data Security Act by Permanent Secretary, Ministry of Information and Communications would evoke more participation and discussion on the mailing list.

Contributing to the discussion, **Crystal Watley**, stated that it is only when we have something valuable exposed do we move to secure it. In her opinion the move toward securing the Kenyan netspace will only take off once there was important content online such as financial history, credit card information, address information and so on. This would require legislation. The Freedom of Information (FOI) Act should be speeded up to "force" government to avail data online. The recently signed (then unsigned?) law on communications has some enabling legislation for e-commerce. However, **Crystal** was not sure it takes into account security and it was important that the government should determine who had the onus to secure data on one's network. In her opinion, security is a problem for industry players rather than the ordinary citizen ("Wanjiku"). If you create a site where you require my credit card details then by all means you should take the blow if someone steals the information and misuses my card!

Victor Gathara, drew the attention of participants to: http://www.bdafrica.com/index.php?option=com_content&task=view&id=14416&Itemid=5821

Day 7: Data and Infrastructure Security

The 7th day of the online discussion addressed cybersecurity specifically data and

infrastructure security.

By way of introduction, the **Moderator** stated that it in recent times it was not uncommon to hear about cyber terrorism, cyber crime, cyber attacks, Information Warfare, etc. Recent examples of cyber attacks in Estonia and Georgia show that the Internet offers an inexpensive and easy weapon of modern warfare

.

Fortunately, Kenya may not have yet experienced critical security threats possibly because majority of users/organizations have access to 'less than broadband speeds' thus providing no incentive for meaningful exploits. This presents a situation where low usage and poor connectivity has acted as our "security". However, with the growing use of the Internet, encouraged by the availability broadband connections locally, nationally (Fibre optic national project, operator networks) and internationally (TEAMS, SEACOM), the number of incidences of online security breaches are set to increase.

Harry Delano in his contribution sought to know the level of cybersecurity preparedness at government, operator, service providers, private sector organizations and educational institutions level? In addition he sought to establish if an assessment had been made on the level of cybersecurity preparedness to date, particularly with the impending landing of international submarine fibre optic cable and what was needed to protect data and infrastructure from increased threats and the corresponding cost.

Building on the **Moderator's** assertion that Kenya had not experienced a critical security threat, **Evans Kahuthu** stated that was important for end users and information owners to understand that just because they have not been compromised, it did not necessarily mean that they were secure since this in security context is "Security by Obscurity".

Evans stated that it was important to understand that hackers write code with certain parameters of the target and thus when they execute such programs only applications that meet this criterion are compromised. In addition, he recommended that before organizations can go on a spending spree on security programs, applications and human resource it is worthwhile for them to know that "Insiders" pose the greatest security threat

to their information. With this in mind, there is need to implement internal access control mechanisms to help eliminate this threat.

With regard to the country's current level of preparedness, from a random analysis of existing web applications, networks and hosting companies, it is evident that there is a lot of work needs to be done. Cases in point include the following:

1. Recent "war drives" around Nairobi city center reveal that most wireless networks are unsecured which provides a convenient entry point for most black hat hackers into the business networks.
2. Most of the dynamic web applications have severe database security vulnerabilities. Using default security assessment methods, it is very easy to gain access to the underlying database data and structure.
3. Though it is not considered as a "critical" application, the "KICTANet database" stores passwords in clear text which is a violation of the database confidentiality rule.

To help protect our infrastructure and data, given the above scenarios, awareness is paramount as this establishes the basis security implementation. In addition policies, standards procedures are important are to help govern the process.

John Walubengo raised the following questions with regard to randomly selected websites:

- Banking: https://s2b.standardchartered.com/ssoapp/login.jsp

  Question: How sure are you that the site you are browsing is actually what it claims to be and not a hoax operating from someone's internet laptop in Mogadishu or Bungoma?

- Customs Services: https://forodha.kra.go.ke/

  Question: This is the KRA eCustoms site. I still do not know why I cannot access

it using my Firefox browser, though it works with Microsoft Explorer. In Security terms, this is known as discriminatory non-availability of services.

- Utilities: http://www.posta.co.ke/

  Question: I was trying to get their postapay service. Question is what guarantees do we have that as government services get online - they do stay online?

- Education: http://www.elearning.strathmore.edu/login/index.php

  Question: Possibly the busiest educational site in sub-Saharan Africa. Question is how sure are you that the assignment posted by the student was not done by the neighbour?

Walubengo requested the network administrator to check out **Evan's** claim that KICTANet passwords were stored in clear text to avoid fraud.

In her contribution, the **Moderator** noted that the UK Data Protection Act[20] provides a good data protection and privacy benchmark. The act requires all organizations which handle personal information to comply with the following eight principles, which make sure that personal information is:

1. Fairly and lawfully processed
2. Processed for limited purposes
3. Adequate, relevant and not excessive
4. Accurate and up to date
5. Not kept for longer than is necessary
6. Processed in line with your rights
7. Secure
8. Not transferred to other countries without adequate protection

[20] Data protection guide UK: http://www.ico.gov.uk/Home/for_organisations/data_protection_guide.aspx

In his opinion **Gichuki John Ndirangu** noted that cybersecurity will either get enforced by the Government (which has no idea what information security consists of), or people who come with an initiative and a research facility which will show Proof of Concept to the government and to any organization what operational and physical security consist of. **Gichuki** noted that cyber terrorism, cyber theft and cyber defense should be the first to be included in policies, in addition to training and awareness. With this in place compliance can be effective and should be followed up with security test and audit. He brought to the attention of the participants the first Kenyan security forum: http://lists.my.co.ke/pipermail/security/

The **Moderator** informed participants that one method that may be used to assess the country's level of preparedness with regards to cybersecurity would be the use of the ITU National Cybersecurity/critical information infrastructure protection (CIIP) Self-Assessment Tool[21]. This tool is intended to assist governments in examining their existing national policies, procedures, norms, institutions, and relationships in light of national needs to enhance cybersecurity and address critical information infrastructure protection.

Day 8: National Cybersecurity Strategy

The day's discussion focused on the development a national cyber-security strategy. By way of introduction the Moderator drew the attention of participants to the provisions of the Kenya Communications (Amendment) Act, 2009[22] with regard to cybersecurity:

- Unauthorized access to computer data,
- Access with intent to commit offences
- Unauthorized access to and interception of computer service,
- Unauthorized modification of computer material,

[21] http://www.itu.int/ITU-D/cyb/cybersecurity/projects/readiness.html
[22] http://www.communication.go.ke/media.asp?id=775

- 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 purpose and
- Unauthorized access to protected systems

The **Moderator** invited comments to Harry Delano question: "Are our cybersecurity regulations (law) up to the task, to protect us...?" Participants were encouraged to consider the issue of jurisdiction, the ability of the judicial system to make a ruling with regards to a crime committed through the internet by extra-territorial elements and secondly the role of arbitration as an Alternative Dispute Resolution (ADR) mechanism[23].

Evans Kahuthu stated that the overall objective of a national cyber security strategy is to protect the confidentiality, integrity and availability of information. The provisions contained in the KCA (amendment) Act, 2009 represent the primary threats that keep an organization from attaining its goals. In his view a cybersecurity strategy should be part of an organization's overall asset protection program. The goals and objectives of the strategy should be understood by all employees.

Further, **Evans** stated that from an information security professional point of view, it is important to understand and provide organizational guidance with respect to the computer crime laws that relate to its operation. These would be the law of the country or laws of other countries in the event that organization operated in a multinational

environment. An important part of information security consists of interpreting the law for top management and instituting policy and procedures designed to keep the organization and its employees from violating the law.

With regard to crimes committed across borders, he noted that some countries were requesting the extradition of computer hackers who have never physically entered the country whose laws they have allegedly broken. Unfortunately, evidence rules generally differ in various legal systems, posing problems in the evidence collection approach adapted.

Solomon Mburu acknowledged that the government recognizes cyber security related issues, however there was a lack of stronger mechanisms to control the abuse of internet Vis-à-vis personal security due to the jurisdictional challenge. He argued that with the passing of the Kenya Communications (Amendment) Act, the development of a data protection unit should be a priority.

In responding to **Solomon's** concern **Akich Kwach** referencing an article in the local newspapers stated that the government had set up a special police unit to deal with cybercrime. The article stated that there were police officers who at that time were undergoing training in the United States until which should have been concluded by end of April 09. The article alleged that some of the officers have been recruited from the private sector.

In response **Solomon** sought to know if mobile operators had homogenous data protection systems to monitor misuse of SIM cards such as spreading of inflammatory messages similar to those that contributed to the post-election violence.

Day 9: National Cybersecurity strategy

The ninth day of the online discussion provided an opportunity for participants to discuss

---

[23] http://www.ciarbkenya.org/

the institution framework specifically Computer Security Incident Response Teams (CSIRTs)/Computer Emergency Response Teams (CERT[24]). CSIRTs/CERTs are responsible for preparing for, detecting, managing and responding to cybersecurity incidents as well as creating consumer awareness.

Global cybersecurity is said to be 'as strong as the weakest link'. The Moderator**,** **Mwende Njiraini**, stated that developing countries particularly in Africa have not sufficiently addressed cybersecurity issues. While some countries have initiated efforts to develop cybersecurity capabilities[25] through the establishment of National CSIRTs/CERTs[26], the CERT-TCC in Tunisia is the only active national CERT in Africa[27].

In establishing a National CERT/CSIRT the moderator invited participants to comment on the following:

- What structure could be adopted?
- What services should be offered?
- What elements could be considered to establish trust in this institution thereby encouraging organizations with critical information infrastructure (CII) such as government agencies, banks, educational institutions, water and power companies, etc, to share of cybersecurity incidents?

In his contribution **John Walubengo** argued that the concept of emergency response teams was difficult to comprehend given that the general Kenyan culture thrives on crisis-management arising from our education system. He therefore recommended that

---

[24] CERT is located at Carnegie Mellon University, involved in Internet security vulnerabilities, long term network changes research: http://www.cert.org/

[25] Team Cymru is a specialized Internet security research firm : http://www.team-cymru.org/

[26] One more CERT in Africa: Mauritius Gets Computer Emergency Response Team - http://www.pcworld.com/businesscenter/article/146123/mauritius_gets_computer_emergency_response_team.html
FIRST is the global Forum for Incident Response and Security Teams: http://www.first.org/

[27] http://www.ansi.tn/en/about_cert-tcc.htm

this culture must be overcome the country was to setup a CERT.

In response **Catherine Adeya** noted that it was important to verify what was hindered the establishment of the CERT by raising the following questions: Can we do it? Do we want to do it? Can we justify the prioritization of establishing a CERT?

John Walubengo confirmed that the country had the capacity to run a national CERT unfortunately nothing was being done towards its establishment. He noted that KENIC had covered some ground in this regard and proposed that their experience could be used to crystalize the CERT idea.

In his response **Gichuki John Ndirangu** argued that Department of Defense should take the lead in cybersecurity rather than the country code Top Level Domain ccTLD manager, KENIC.

Catherine Adeya noted that there were multiple initiatives which had not been recognized. She encouraged researchers and students to share their ideas (local innovation) contained in academic thesis.

In his opinion **Barrack Otieno** noted that there was some ambiguity in the country's institutional structures when dealing with cybersecurity. For example what was the role of critical stakeholders such as the National Security Intelligence Service (NSIS) in cybersecurity? He expressed concern that non-state actors may take up responsibilities that they may not be well equipped to handle and recommended use of the public private partnership (PPP) model in establishment of the national CERT.

In his contribution, **Sammy Gatere** sought to know the kind of investment that the government would need to put down to establish an institution to overcome an intangible risk or threat. He was of the view that the current political establishment may not be too interested in digital matters given that issues such as environmental preservation (read Mau forest complex) have lead to protracted political battle despite the glaring evidence

of poor resource management. He supported **Barrack's** view that the country's intelligence agents (NSIS) should be more tech savvy. To prevent a situation where the country was fighting fire without fire equipment it was important to have a CERT up to pre-empt disaster and avert possible aggression as was the case in the Russian-Georgian conflict[28].

Gichuki John Ndirangu noted that the war in Gaza had the same effects including defacing of Anti-Muslim websites by Palestinians and Israel cyber attacks on Gaza television servers for purposes of broadcasting threats. In his view, none of the government sectors in Kenya cared about cybersecurity or cyber terror, for example the use of Unstructured Supplementary Service Data[29] (USSD) by terrorists (Mungiki, etc) to spread propaganda.

In contributing to the discussion **Michuki Mwangi** shared the following quote referring cybersecurity; "broccoli technology: basically its good (healthy for you) but we do not necessarily like the taste of it. The only time we get to eat broccoli is on doctor orders. " Consequently, until and when data and information forms the lifeline of our businesses shall we look at security more seriously.

In response **Sammy Gatere** thought that the analogy; "broccoli technology" was interesting and a befitting description of cybersecurity. In his view security matters would only take center stage when we start seeing actual threats manifest into real security challenges.

---

[28] http://blogs.zdnet.com/security/?p=1670

[29] USSD is a capability of all GSM phones. It is generally associated with real-time or instant messaging type phone services.
http://en.wikipedia.org/wiki/Unstructured_Supplementary_Service_Data

Theme 4 – The Socio-Economic Issues of IG (1Day)

Day 9: e-Payments

Introduction

The **Moderator, John Walubengo**, welcomed participants to the 10th day of the online discussion which would address "hybrid" electronic payments systems and corresponding legal and regulatory frameworks.

Hybrid electronic payment systems exclude the traditional banking systems which do have time-tested and proven legal/ regulatory frameworks. Typically they refer to emerging e-Payment systems that have been best exemplified by the MPESA/Zap phenomena. Such systems cut across multiple industries (Banking, Telecommunication and IT) and present a huge regulation/legislation challenge.

In developed economies, such systems have multiple legislation/regulation that demands that the entities involved in such ePayment services abide by strict Data Protection Acts which protect the customer data/privacy as well as other eLegislation (eCrime, eTransaction) that provides deterrence and assurance mechanism.

In layman terms, consider an MPESA/ZAP User who sends value of 30,000Ksh from their mobile phone account to the parents upcountry when the following happens:

- Disaster strikes (e.g. 9/11, Tsunami, etc) and the electronic records are lost - whose is liable?
- The Parents claim that they did not receive the money or worse still the sender claim they never send the money (non-repudiation issues)
- An eCrime suspect is charged with altering ePayments records at the source (inside job/judicial issues)

The **Moderator** sought contributions on the availability of legal frameworks to protect consumers and businesses against risks such as those mentioned above and the investigative and judicial capacity to administer e-Crime related justice. Additionally participants of the online discussion were encourage to share their opinion of the roles that the Regulator (Communications Commission of Kenya), Banking (Central Bank of Kenya), the Police and Judiciary (NOT) would have within the legal framework.

Solomon Mburu sought to have the discussion on electronic payments systems and corresponding legal and regulatory frameworks extended for two days. In his view the topic of discussion touches the heart of many Kenyans as it involves money. Thus exhaustively discussion this issue was an important step in catering for the concerns of Kenyans living upcountry.

In response the Moderator engaged contributions for an extra two days before the closure of the online discussion.

Barack Otieno stated that he was reliably informed that Mpesa was designed as a microfinance solution. He noted that before Mpesa became popular there was Sokotele service that was a bit cumbersome because it involved queuing in a banking hall (KREP/CELTEL). As these money transfer solutions relied on traditional banking system for trust accounts gave impression that the e-payment solutions were just a means to an end (the money stored in the bank). In this regard, **Barack** proposed that the Kenya Bankers Association, an umbrella for stakeholders in the banking sector and the Communication Commission of Kenya, the regulator for the technology sector should establish frameworks from a banking perspective as well as a technology perspective to manage security concerns. In his view, some of those Mpesa outlets which maintained a significant amount of float were insecure. Another concern was that a good number of users from rural areas are technologically challenged and vulnerable to con men and women.

Victor Gathara proposed that the Ministry of Information and Communications should take the lead in legislation affecting the ICT sector and have an overall management role in it. Additionally he recommended that an Information Technology (IT) security czar was required (or already exists) and may rightly sit in the Communications Commission of Kenya (CCK). **Victor** argued that the ministry should improve its communication strategy to alert all on status of ICT security as he was currently unclear which laws/structures were in place in government to address this issue.

Barack Otieno however disagreed with **Victor's** opinion stating that security was a complicated area and requires a multi-stakeholder approach, i.e. a clearly defined system made up of state and non state actors. In his view the Ministry of Information and Communications had a facilitating role and was responsible for the development of policies. He noted that Kenya had skilled personnel in and out of government unfortunately though there was a failure of tapping into their knowledge through institutions.

In response **Victor** supported the multi-stakeholder approach though in his opinion the buck has to stop with someone in government who would be the custodian of the 'sword'. In this scenario the stakeholders would ensure that whoever wields 'sword', wields it sensibly and for the common good. Consequently, it was the role of stakeholders to engage the government through the various forums including the KICTANet list.

Theme 5 – Closure and Way forward (1Day)

Day 10: Desirability and Continuation of IG Forum

Introduction

The final day of the Kenya Internet governance online discussion addressed the upcoming 4th IGF. The **Moderator, Mwende Njiraini** stated that the IGF is scheduled to be held for first time in Africa at Sharm El Sheikh, Egypt[30]. She noted that the hosting

[30] http://igf09.eg/

of the IGF in Africa presented an excellent opportunity to raise issues that were of importance to the continent, region and country. She noted that the themes proposed to be discussed in the upcoming IGF and contained in IGF-Programme, Format and Schedule[31] for the 2009 meeting include:

- Internationalization of critical Internet resources management/Managing critical Internet resources
- Balancing privacy, openness and security
- Access
- Round table discussions: on the empowerment and protection of children online, the accessibility for people with disabilities, multilingualism and access to local content.
- Workshops[32]: Access, Critical internet resources, Diversity, Openness, Security, Capacity building and Development.

The **Moderator** drew the attention of the participants to the fact that forum will also provide an opportunity to discuss Paragraph 76 of the Tunis Agenda: "examine the desirability of the continuation of the Forum" and therefore invited views and comments to the following questions:

- What method should be used to assess the impact of the internet governance debate through the two phases of World Summit on Information Society in Geneva, 2003 and Tunis 2005 and the 1st to the 3rd IGF?
- What do you think needs to be addressed in the remaining two IGFs?
- How can we as Kenyans, effectively participate at the 4th IGF and translate the lessons learnt?
- Do you think that the IGF should continue after the 5th IGF?

---

31 http://www.intgovforum.org/cms/2009/progpaper/ProgrammePaper.01.05.2009.rtf

32 Workshop proposals: http://www.intgovforum.org/cms/index.php/component/chronocontact/?chronoformname=WSProposals2009ListView

In his contribution **Barack Otieno** stated that despite the not knowing if there were vested interest in facilitating the continuation of the IGF, he would from a knowledge and best practice point of view suggest that the forum proceed to the 5th Session. He was aware that many have termed it as a talk show, however, in his view these talk shows have fostered the spirit of cooperation and diplomacy. In addition **Barack** was of the view that the forum should be given more 'teeth' under an appropriate UN agency and was curious to know the position of 'insiders' such as Dr. Siganga.

In his contribution **Blessings Msowoya** noted that there were actions and remarkable accomplishments arising from IGF despite 'all the talk'. **Blessings** stated that the setting up of the IGF was a follow up of the recommendations made by the WGIG which was set up by the UN Secretary General: The IGF may "identify emerging issues, bring them to the attention of the relevant bodies and the general public, and, where appropriate, make recommendations," but does not have any direct decision-making authority[33]. In his view if people are able to 'spit out' the words, then the IGF is fulfilling its mandate!

Blessings noted that the activities that would take place during the IGF: Workshops, Best Practice Forums, Open Forums and meetings of the Dynamic Coalitions would be based on the following main themes: openness, security, diversity and access. He noted that 'critical Internet resources' a new theme introduced in 2nd IGF in Brazil has become one of the most debatable topics in the IG field.

He encouraged participants to contribute their views on what should be done at and to the IGF as the IGF is 'a discussion forum'. On the basis of what is discussed decisions can then be made. He noted that despite there being some hiccups there has been tremendous progress. He drew the attention of participants to Dr. Jeremy Malcolm paper: "Appraising the Success of the Internet Governance Forum[34]"

In his contribution with regard to the continuation of the IGF **Waudo Siganga** sought to

[33] http://en.wikipedia.org/wiki/Internet_Governance_Forum
[34] http://www.internetgovernance.org/pdf/MalcolmIGFReview.pdf

echo the general consensus with regard to reflecting on the forum's success so far, both internationally and as exemplified by the East Africa Regional and National initiatives. He noted that the IGF has proven to be a unique but successful experiment in multi-stakeholder engagement enabling information sharing and dialogue on topics critical to fostering the sustainability, robustness, security, stability and development of the Internet. The East Africa initiatives demonstrated that the spirit of the IGF as enunciated in the Tunis Agenda can be replicated at the grass-roots, greatly expanding the scope of those whose input will shape the future of the governance of the Internet.

Waudo agreed with the view that multi-stakeholder processes that have underpinned the IGF continue to make it a globally unique environment for a constructive and open exchange of ideas without the limitations imposed by the pressures of negotiation and governmental bureaucracy. He supported the continuation of the IGF internationally and regionally/nationally beyond the 5 year life-span given in Tunis.

Evaluation and Feedback

Technical

The listserver had no technical challenges and was reliable throughout the two week period.

eParticipants

Over three hundred and fifty (350) participants were on the KICTANet list during discussions, however only a few actively contributed to the discussion.

Moderation

The Online discussion was moderated by two e-Moderators. This allowed for expert guidance on various and diverse topics that constitute the Internet Governance domain.

Appendices

Appendix I –Abbreviations

CCK: Communications Commission of Kenya
ccTLD: Country Code Top-Level Domain
CERT: Computer Emergency Response Team
CSIRT: Computer Security Incident Response Team
FTTH: Fiber To The Home
IPv6: Internet Protocol Version 6
IPv4: Internet Protocol Version 6
IG: Internet Governance
IGF: Internet Governance Forum
ITU: International Telecommunications Union
KICTAnet: Kenya ICT Action Network
KIXP: Kenya Internet eXchange Point
MB: megabyte
NFOB: National Fiber Optic Backbone
OAN: open access network
PDNO: Public Data Network Operator
PPP: Public Private Partnership