HI-TECH DEVELOPMENTS IN THE WORLD: IMPLICATIONS FOR AFRICA

By

Mwaita Patrick
ACCP

Being an ACCP Paper presented at the South African Cybercrime Conference in Pretoria, 4th -5th April, 2013

Introduction

- Africa delights in the benefits of hi-tech developments for maximum exploitation of resources.
- Technology has replaced manual applications from individual personal details to national strategic interests.
- The technological status of a country reflects its economic status.

Cont'd

- Africa needs technology to access improved services, a consequence of scientific breakthroughs.
- Technological innovations include ICT developments which revitalise information use.
- The Internet is one of the most revolutionary innovations of the 21st century, growing at 4 million users annually in Africa (UNAFRI).

Benefits

- It has enabled instant transactions through e-mail, sms, twittering, telnetting, VoIP, video conferencing etc.
- It has opened up new channels to free information and wide exposure.
- Has offered a cheaper mode of conducting business and led to an increase in business cash flows through increased sales and cheaper operating costs or expenditure.

Developments

- Africa is destined to transform from a Dark Continent to a new world.
- The computer is central to all hi-tech developments.
- Increasing use of the internet manifests the significance of communication across boundaries.

ICT Updates

- The United Nations African Institute for the Prevention of Crime and the Treatment of Offenders (UNAFRI) estimates that 1.8 billion internet users with 98 million users in Africa (2011).
- Internet use is revolutionarising the dynamics of international relations, public and private enterprise, movement of goods and services, opening opportunities for global cooperation in governance, commerce, agriculture, industry, environment and security of nations.

Consequences of ICT Development

- 'Cyberisation' of hinterland estimated at 6.8% penetration of devices such as mobile phones ATM, Video, Radio (Morel).
- the dynamics of community and family relations is manifesting new trends of interpersonal contacts.
- ICT progress is double-edged
  - technical challenges; breakdown/failure
  - crime perpetrated on line makes cyberspace dangerous causing economic difficulties and global security concerns.

Cont'd

- Rampant reports of hacking into highly strategic installations and sensitive institutions pose imminent dangers facing the continent in e-security.
- According to Maicibi (2011) more than 60% of internet users in Africa have fallen victim to internet fraud, affecting individuals as well as corporate bodies.

Cont'd

- Tushabe and Baryamureeba (2010) explain that companies hit by cybercrime attacks lose revenue through a decline in stock prices between 1-10%.
- Anti-virus software costs between US$10 to $300 per person.
- A company of 2,500 staff would incur between $25,000 and $750,000 annually in virus protection.

Nature of Cybercrime

- Cyber threats respect no boundary. Secrecy of states and individuals including facebook computers.
- The commission of crime takes on unprecedented precision.
- BBC (20 March 2013) reported a cyber attack on major broadcasters and banking institutions in South Korea.
- Africa with techno-deficiencies will suffer disproportionately.

Whistle-blowing

- Sustained use of hi- tech presumes a technical competence;
- prompt action/capacity building to safeguard Africa's cybercommunity; government and private sector.
- Forensic interventions could boost cyber security.
- Technical assistance from regions of wide exposure to forestall obvious danger.
- Spanish police recently cracked down cybercriminals whose 'ransomware' a tool in ID Thefts defrauding millions of euros from internet users in 30 countries.

Intervention perspectives

- At the beginning of March 2013, the US President issued an executive order seeking better protection of the country's critical infrastructure from cyber attacks.

- Africa should draw lessons and act accordingly with legislations tailored to realities of national security and interface with service providers.

- Advanced expertise, specialised equipment and software, specialised training and research will facilitate vigilance and cyber patrols to enable Africa develop a Pan African cyber police premised on a harmonised basic regulatory framework.

.

Effects of Identity Theft

- The total loss in value is hard to estimate or calculate for Africa.
- Maicibi affirms that globally, about US$200 billion is lost to ID thieves annually.
- 50% of the ID victims find out that they are victims after 3 months.
- Victims to ID theft prefer to suffer the loss without disclosure, increasing direct financial loss. (UNAFRI, 2006).

Intervention Efforts

- Vulnerable cyber population: the intellectual middle and working class, the youth and children represent the potential work force of the continent.
- African countries have some legislation criminalising computer use, but there are challenges regarding enforcement (Owor 2011).

- Gaps in legislation do not give powers to law enforcers to intercept communication, in others there are procedural weaknesses exposing third party victims of cybercrime to undue risks. (Owor,2011; United Nations Economic and Social Council,2009).

Intervention Efforts (cont'd.)

- Lack of harmonised legal systems in Africa undermines apprehension and prosecution of perpetrators (Akuta, Ong'oa and Jones 2011).
- ICT is a new development in Africa for which resources to combat are not readily available. The need to invest in ICT development becomes crucial.
- Unique rehabilitation measures for identified cybercriminals to feed into body of knowledge for local capacity.
- Limited scope of hi-tech operations

Unique African Profile

- Ill trained, ill equipped enforcement officials,brain drain.
- Inadequacy in legislation makes cyber crime difficult to prevent in Africa.
- Abuse and exposure to risk of criminal victimisation propagated through these gadgets.
- Science-illiteracy increases vulnerability to cyber attacks.
- Criminal attacks and technical failure are eventualities Africa needs to prepare to handle.
- Unemployment, greed, illiteracy are risk factors.

Institutional mechanisms

- Collaboration
  - ACCP with relevant agencies in enhancing cyber security preventing, prosecuting and punishing cybercriminals awareness campaigns to sensitise the cyber-community.
  - Building on the available crop of experts in conjunction with partner agencies, Africa can establish a strong coalition.
- Africa needs to domesticate the relevant conventions to secure her cyber space.

Cont'd

- ACCP on possibility of tech-science training as a basis for effective cyber literacy and security.
- ACCP to extend coalition; govt-private sector to include experts who can promote the campaign tailored to the realities in their regions; employment.
- Continued research will provide new insights and assess relevance of existing control measures

International perspectives for Protection

- Resolution 65/230 the 12th UN General Assembly established an open-ended intergovernmental expert group to add weight to the search for an integrated approach to the problem of cyber crime and responses to the challenges by Member States, including best practices, exchange of information on national legislation, technical assistance and international cooperation.

Downloading International perspectives

- ACCP officials among the Intergovernmental Expert Group seen as a useful connection between Africa and the international crime prevention network.

- ACCP to hold several activities to increase understanding and alertness of communities about cyber challenges: action-oriented researches, training on cyber-related issues, workshops/conferences on cyberlaw and security, host experts, publish and provide network of professionals for advisory services.

Conclusion

- The benefits of technological innovations have made life more liveable and enjoyable.
- Transformation in all sectors of life will be based on technology.
- In terms of communication, technology has been manifest with most widespread and direct effect to the growing majority, computers and electronic gadgets for information processing such as personal cell phones are in popular use in Africa.

Conclusion cont'd

- The need for international cooperation using conventions from United Nations General Assembly, African Union, COMESA, Commonwealth, Council of Europe, European Union, East African Cooperation and SADC on Cybersecurity. Africa needs technical support from global intervention to facilitate the insulation of her people and industries from risks.

Conclusion Cont'd

- Technical competences for maintenance of hi-tech applications should be developed through investments in ICT.
- Provide a technical expert group to guide cyber developments.
- Align implementation of technological devts with technical expertise

Conclusion cont'd

- In the recent past, there have been genuine efforts to put regulatory mechanisms based on local legislation, international cooperation, sharing of good practices and information highlighting widespread sensitisation and awareness raising strategies which are tailored and packaged to suit specific audiences.
- Need for Continental network of Computer Emergency Response Initiatives

- The success of these strategies will depend on an interaction of the following factors: the availability of technical support to Africa in sustaining the exchange of knowledge, acquisition of expertise based on available regional and international conventions, international cooperation, tailored legislation and resources as well as scientific breakthroughs to spearhead innovative mechanisms such as relevant software for cybersecurity.

- African institutions such as ACCP, UNAFRI universities and colleges as well as schools together with the available local experts some of whom serve on the United Nations Intergovernmental expert group (IEG) should serve as the core of a continental technical support team to push the African cybersecurity programmes forward to their planned targets.

Conclusion and Recommendations

- African traditional values of community responsibility to promote responses to emerging threats.
- Cybercrime is a new epidemic affecting all our people. Its prevention requires the involvement of all the people regardless of status and physical location.
- Expertise from all conferences be packaged for villages, markets, homes and institutions to the victims; the elderly, the illiterate.

Recommendations Cont'd

- Utilise Drama/songs, the media, traditional leaders with sermons and teachings with comparative influence in areas of technical competence.
- Educational institutions should develop their curriculum to include cyber alerts in their instruction to pupils/students, who should in turn to share this knowledge with their families – parents, guardians, siblings, friends and relatives.

Recommendations Cont'd

- Victims of cybercrime should be encouraged to open up and share their testimonies to enhance awareness.
- Maximum disclosure will substantially lead to effective responses from the more capable and technically suited cyber literate community and appropriate intervention by the experts.

Thank You