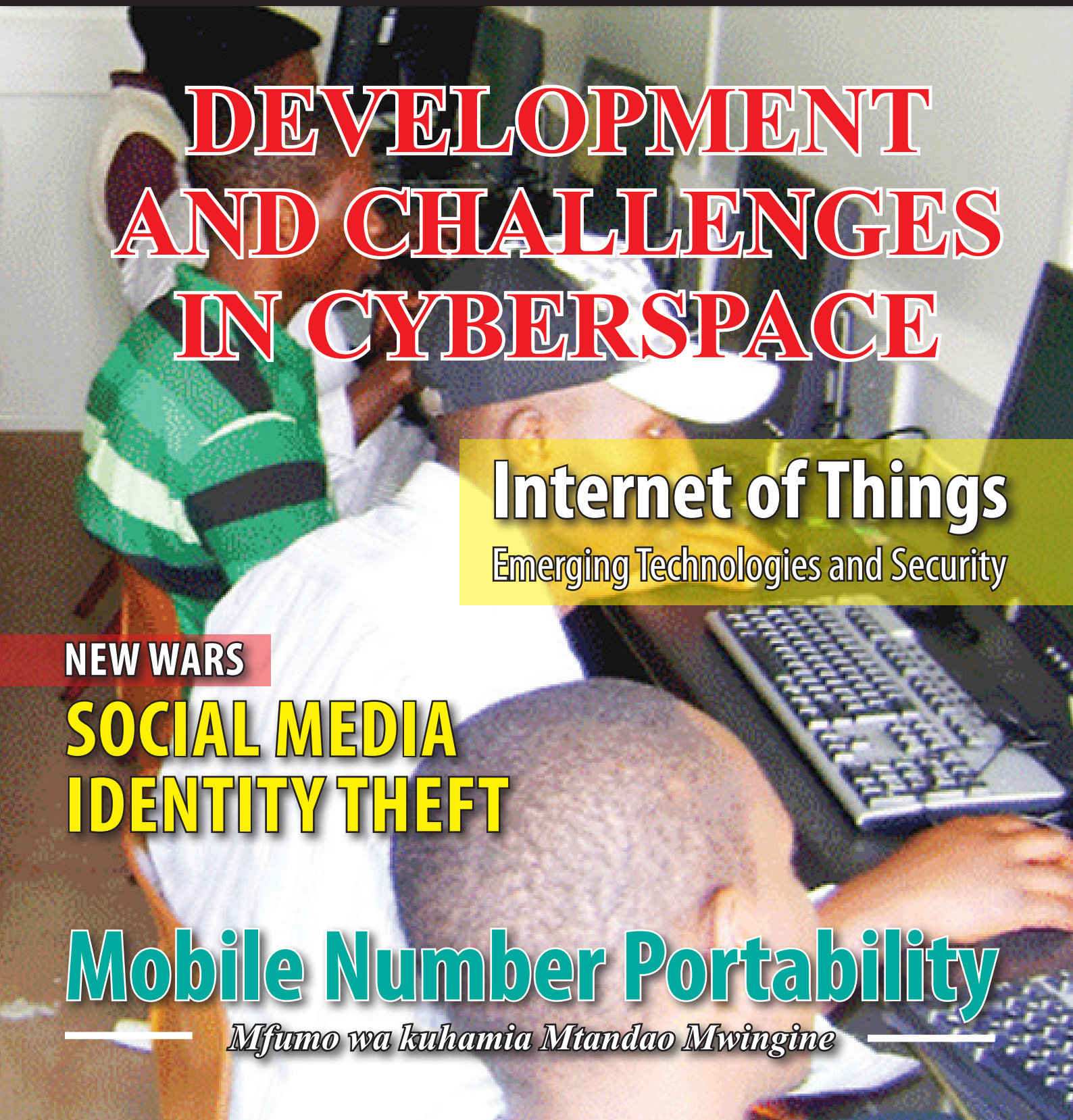
THE
Regulator
FREE COPY
CRA CREATING A LEVEL PLAYING FIELD
Quarterly Magazine of the Tanzania Communications Regulatory Authority
ISSN: 0856 - 8030 | ISO 9001: 2008 CERTIFIED | APRIL - JUNE, 2017



DEVELOPMENT AND CHALLENGES IN CYBERSPACE

Internet of Things
Emerging Technologies and Security

NEW WARS
SOCIAL MEDIA IDENTITY THEFT

Mobile Number Portability
Mfumo wa kuhamia Mtandao Mwingine

TCRA VISION, MISSION, STRATEGIC GOAL AND CORE VALUES

OUR VISION
"To be a World class Regulator of Electronic and Postal Communications".

OUR MISSION
"To effectively regulate electronic and postal communications services, promote efficiency among service providers and protect consumer interests with an objective of contributing to development in the United Republic of Tanzania".

OUR QUALITY POLICY
Tanzania Communications Regulatory Authority (TCRA) is committed to enhancing the welfare of Tanzanians through provision of effective and efficient regulatory services that ensure Universal Access to Communication Services, through Quality Management System in all processes needed in our areas of jurisdiction. TCRA continuously improves and reviews her Quality objectives regularly and communicates the policy within the organization.

STRATEGIC GOAL
This Strategic Plan builds on what the Authority has done in the past and encompasses the above five-year strategic direction (Vision) for the future, which is based on the following Strategic Goal:

"To enhance the welfare of Tanzanians through effective regulation that promotes innovation and ensures universal access to secure, quality and affordable communication services".

MOTTO
"Creating a level playing field".

STRATEGIC OBJECTIVES
The extensive review of sector and evolving technological development resulted in formulating six (6) Strategic Objectives to achieve the Strategic Goal. The Strategic Objectives are described herein below as follows:

- To modernize TCRA operations by utilizing state of the art technologies, enhancing high quality research on regulated services and staff competences.
- To promote efficient, reliable and secure communications infrastructure and applications.
- To promote efficient and affordable communications services and increase access to Postal and ICTs in under-served and un-served areas.
- To protect interests of stakeholders and enhance awareness of their Rights and Obligations.
- To monitor performance of regulated services and enforce compliance to legislation, regulations and standards.
- To coordinate implementation of National, Regional and International Sector Commitments.

The Regulator is published quarterly by the Tanzania Communications Regulatory Authority (TCRA), an independent Government agency established under the Tanzania Communications Regulatory Authority Act No. 12 of 2003 to regulate the electronic and postal sectors in Tanzania.

CONTENTS

Editors Note 2

From the Director General's Desk 3

Towards a Cashless Society 4

Enhancing Postal Home Delivery Services 7

Mobile Number Portability 10

- Kiswahili Supplement 13

Huduma ya Kuhama Mtandao bila Kubadili Namba

Internet of Things 17

Emerging Technologies, Trust and Security 20

Cyberspace War 24

Avoiding Social Media ID Theft 26

ICT Potential for Youth Employment 28

Letter from the Editor

Dear authors, reviewers and readers of the "Regulator",

I AM delighted to cordially invite our dear readers, authors and reviewers of the April – June 2017 edition of the Regulator, the quarterly newsletter of the Tanzania Communications Regulatory Authority. It publishes articles in the field of information and communications technologies (ICT).

The prime purpose of the Regulator is to provide our readers with updates on the developments in the field of ICT. The newsletter also explores the current status and addresses future possibilities. It covers all aspects of ICT; an open-minded stance has enabled us to engage a broader pool of stakeholders; from academia, industry and other regulatory agencies.

Contributions from academia and industry are particularly important for the health and longevity of our Newsletter. Industry and academia are the savvy to the emerging technology and uniquely spearhead innovation. In fact, academia plays a key role in attracting innovative minds to ICT development.

With such a broader inclusion, it is important to put a disclaimer that the information and views set out in these articles are those of the author(s) and do not necessarily reflect the views of the Authority.

ICT impacts all facets of life, and it is uniquely positioned to solve a wide array of 'social challenges' by enabling transformation and interpretation of information in a broad variety of disciplines. In fact, ICT is core for addressing critical societal challenges in various areas, including transportation, entertainment, education, healthcare, energy systems, sustainability, defense and security. To this end we are promoting ICT to address society's critical problems, and your input is critical and most welcome.

The success and reputation of the Regulator is a reflection of the outstanding work by our reviewers and authors who are dedicated to share best quality articles. Special thanks are due to the editorial team; they have done a fantastic job, shaping the Newsletter to ensure it has maintained its place as the country's communication newsletter, addressing issues in the communication sector. The team has worked incredibly hard, particularly in the assessment and processing of the submitted articles.

Lastly I should thank all our submitting authors, who have chosen the Regulator as the publication in which they would like to share their ideas.

As a final remark, I would like to invite readers to send us their comments to enable us to improve the publication.

Dr. Emmanuel C. Manasseh
Editor

Eng. JAMES M. KILABA
Director General TCRA

Security, Privacy and Trust: Major Challenges in ICTs

DESPITE fast advancement and multiple benefits of Information and Communication Technologies (ICTs), issues of security, privacy and trust remain major concerns both at National and Global levels.

When I addressed the World Telecommunication Standardization Assembly (WTSA-16) at the Global Standardization Symposium in Jasmine Hammamet, Tunisia, recently I told participants that emerging technologies in ICTs impose more challenges on **security** (*Networks, systems, devices, data and Users*), **privacy** (*data and Users*) and **trust** (*Networks, systems, devices, data and Users*).

In any ICTs discussion forum, we normally don't miss talking about ICTs related Services, Devices, Growth, subscriptions or Users, Network and Signal coverage and even revenues. Today, we are discussing the impact of emerging technologies on security, privacy and trust in ICTs.

There has been a shift from an internet dominated by Personal Computers (PCs) with wired connections, to the current mobile devices connected by wireless signals. This has facilitated more access to communications and by extension, through Internet, to the cyber world. The main course of discussions at the Assembly was on ICTs related **Services**, **Devices**, **Growth**, subscriptions or **Users**, Network and Signal **coverage**.

Regulators around the world are being challenged by the role/demands of Users (**people**) and evolutions of **Devices** irrespective of where they are mounted, fitted, connected or used as far as Security, Privacy or Trust are concerned. So, it is basically the People who also have cultural diversity complemented by time-zone differences.

From the perspective of developing countries, Tanzanians have done a lot in cyber security. From the perspective of developing countries, Tanzania has a National Cyber Security System in place and stakeholders are involved.

Tanzania has a National Computer Emergency Response Team (TZ-CERT) that is used for dissemination of cyber security knowledge, information and skills to various stakeholders and Users, to enable them to acquire necessary levels of expertise needed to actively tackle serious cybercrime incidents. We have implemented DNSSEC at our Domain Name Registry System. We have a newly established National Data Centre. We have also started to deploy mechanisms to prevent the misuse of data or information from a stolen mobile device in the country.

In the East African Region, Computer Emergency Response Teams (CERTs) have been implemented in four countries and to a large extent, the countries share and exchange information on cyber security incidents and threats. Through the regional Communications Organization (EACO), member countries also meet and discuss issues on the cyber-security.

The particular challenges faced in the context of security, privacy and trust in ICTs could be categorized in five basic factors like Inadequate Standards, Policies, Laws and Strategies.

Standards, Laws and Strategies are required to improve a nation's cyber defense posture. As the matter does not end within one country's borders, the established Standards, Laws and Regulations need to be harmonized within regions and globally. It is believed that there are a few world-class cyber experts to adequately handle cyberspace offenses and defense.

There is a need for the establishment of National Cyber-security Strategies that would promote dissemination of cyber security knowledge, information and skills to various stakeholders and Users, to be able to acquire necessary levels of expertizes needed to actively tackle serious cybercrime incidents, including proper Management of Cyber-Security – beyond national borders.

Some of the developing countries do not have well-established and adequately equipped National Computer Incident Response Teams (CIRTs) or Computer Emergency Response Teams (CERTs). These kinds of facilities when well established provide national approach for coordination, analysis, responses and secure information sharing in regard to cyber security incidents and threats.

There is a need therefore, for developing countries to have hand-shaking national-CERTs that would assist on early detection, monitoring and countering attacks, intrusions, new forms of malicious code distribution or any other type of malicious behavior.

Effective and collaborative management of cyber security is a critical capability for the defense and preservation of civil society. Cybercrime is one of the world's largest and fastest-growing categories of crime in cyberspace.

It is important that all critical infrastructure like Domain Names Registry Systems in countries are properly secured and monitored to prevent attacks which could lead to negative economic impacts in our countries.

Numbering Resources Management for IoTs and M2M are very key as the area is also emerging as new and therefore requires special attention in developing countries.

There is a need to educate users on issues related to security, privacy and trust in ICT. This education will enable users to make informed decisions on the trustworthiness of ICT applications and services including social contacts and selective information sharing.

Proximity Money Payment (P2B): Unexplored Opportunity towards a Cashless Society?

Christopher John Assenga,Tanzania Communications Regulatory Authority
cjohn@tcra.go.tz

1. Payment System

PAYMENT can be defined as the transfer of one form of good, service or financial asset in exchange for another form of good, service or financial asset in proportions that have been previously agreed upon by all parties involved (Investopedia, 2015). According to Bloxham (2010), money and payment systems have developed from cowry shells to contactless payment. Today, money can be in the form of coins, notes, paper or electronic (e-money). Regardless of the form it takes, money is the heart of many business transactions.

Over the past several decades, the payments industry has undergone significant changes. Payment can be executed either in hard cash (money) or electronic money (e-money). New electronic payment instruments have been introduced and the means for making electronic payments have become increasingly available for use in everyday commerce (Gerdes & Walton II, 2002).

Despite the development in payment systems as in many of developed countries, the common and dominant payment system used by the majority of people in Tanzania is a cash payment system, whereby cash (notes and/ or coins) is used for purchase of goods in shops and to pay for various services (Bank of Tanzania, 2015).

The reason why most developing countries still trade in cash is because of low level of unbanked community as compared to developed countries. About 2.5 billion people in developing countries are unbanked (GSMA, 2014).

2. Financial Services and Inclusion in Tanzania

Many developed countries are getting away from cash payment due to proliferation of banks; thus many of the citizens are well included in financial services. According to Credit Suisse (2015), Nordics are in the lead and it is predicted that they will get rid of cash by 2030. Most of electronic payments in developed countries are done through credit cards and debit cards. In Tanzania, electronic payment such as credit cards and debit cards have not gained a wide acceptance due to low penetration of formal banking services, thus excluding the majority from financial services (National Council for Financial Inclusion, 2016).

Despite the commitment made by Tanzania through the central Bank under the Alliance for Financial Inclusion (in the Maya Declaration) to increase formal access to financial services to 50% by 2015 (Bank of Tanzania1, 2013), reports shows that the banking sector in Tanzania has grown from four (4) banks in 1991 to just 52 banks in 2016 and an overall 609 branch networks (National Council for Financial Inclusion, 2016).

In Tanzania, the level of penetration and access to formal financial services i.e banks is 8.5% and 40% respectively for rural areas while for urban areas it is 23% and 45% respectively. Only 12% of Tanzania's population had bank accounts in 2012 (Bank of Tanzania2, 2012). BoT's report agrees with Weber and Darbellay (as cited in Etim, 2014) that Sub Saharan Africa (SSA) has one of the largest unbanked populations in the world, with more than 80% of population unbanked.

3. Mobile Financial Services

The International Telecommunication Union (2013) defines mobile financial services (MFS) as financial transactions and services that can be carried out using a mobile device such as a mobile phone or tablet. These financial transactions and services are sometimes referred to as mobile money services (MMS) and may or may not be linked directly to a bank account. When linked to bank accounts are known as mobile banking.

MFS can be categorized into three services; namely, Mobile Money Payment, Mobile Money Transfer and Mobile Banking (International Telecommunication Union, 2013).

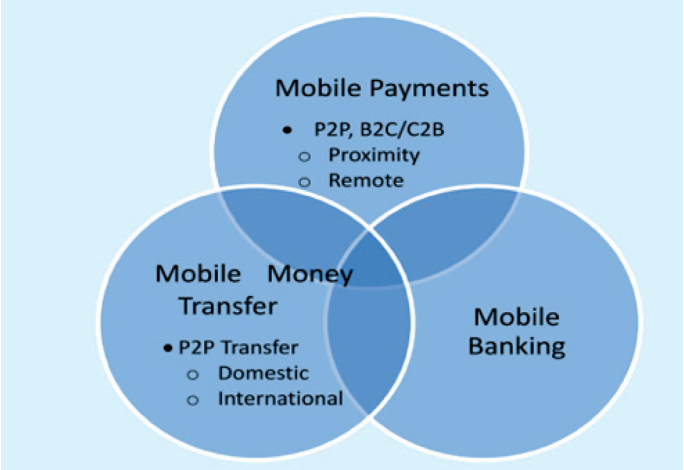


Fig 2: Categories of mobile financial services as per ITU
Source: (International Telecommunication Union, 2013)

4. Mobile Financial Services in Tanzania

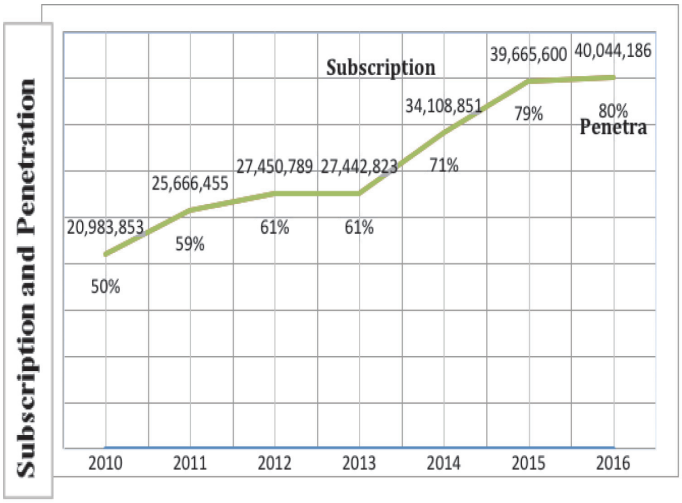
The scope of this article is limited on Mobile Money Payment (P2B Proximity) which involves a customer and physical merchant (such as shop, supermarket e.t.c). The remote P2B which involves a customer with a remote merchant (such as LUKU,

Proximity Money Payment (P2B): Unexplored Opportunity towards a Cashless Society?

DAWASCO, TV Subscription) is not in the scope of this article.

In Tanzania Mobile Financial Services (MFS) were introduced in 2008 and have been widely used for peer to peer (P2P) or personal to personal services such as money transfer, savings and facilitating banking transaction (M-Banking).

While more than 80% of Tanzanians do not have access to a bank, about 80% have access to communication (TCRA, 2016) (see Figure 1.).



Source: (TCRA, 2015)
Fig 1: Mobile subscription and penetration for the period of five years

With an 80% population penetration it means 80% of population virtually has access to financial service through telecommunication.

5. Mobile Money Payment in Tanzania

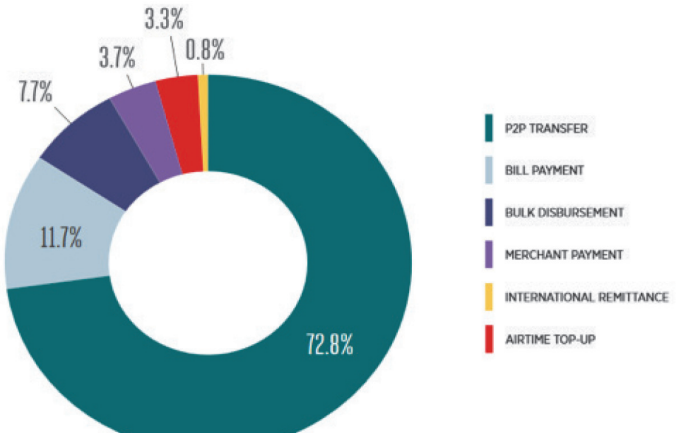
Personal to Business (P2B) or Merchant Payment has been introduced by MNOs in Tanzania to facilitate customers who want to pay for the goods in a same way as those using credit and debit cards. Vodacom launched its Mobile Money Payment services branded "LIPA KWA MPESA" (pay here with M-pesa) in September, 2014. According to Vodacom, "Lipa kwa Mpesa" is an integrated payment system for the business community that allows merchants, retailers and distributors, in a far more secure way, to settle payments by using M-PESA" (Vodacom Tanzania Limited, 2014).

Tigo has 'LIPA HAPA KWA TIGO PESA' (Pay here with Tigo Pesa). Speaking during the GSMA conference, Tigo's Head of Financial Services, Ruan Swanepoel said that "customers from across all networks can now pay for services or products at any of our widest network of merchant shops across the country that have the banner 'LIPA HAPA KWA TIGO PESA' " (Athumani, 2016).

Airtel has "AIRTEL TAP TAP" which uses Near Field Communication (NFC) cards that enable holders of Airtel Money accounts to settle bills using their cards.

Fig 3: Posters of different MNOs indicating availability of P2B services

According to GSMA (2014), out of the three types of MFS, mobile money transfer (P2P transfer) has continue to dominate the global product mix in terms of volume and value, accounting for about 72.8 % of the transactions while mobile money payment (in this case proximity P2B Merchant Payment) contributed only 3.7 % (see Figure 4).



Source (GSMA, 2014)
Fig 4: Global product index mix by volume

5.1. Advantages of Electronic Payment over Cash Payment

High labor costs in managing Cash. Cash management involves counting, reconciliation and transporting to banks. This requires time and labor. If someone receives lots of cash he/she will require a lot of time and labor to handle the same and at the end of the time find it costly to handle cash than electronic money. The Central Bank of Nigeria (CBN) (as cited in Yaqub, et al, 2013) revealed that the direct cost of handling cash was fifty naira in 2008 and was

Unexplored Opportunity towards a Cashless Society?

expecting to reach a staggering sum of one hundred and ninety two billion naira in 2012. In United States of America the cost handling cash is USD 200 billion per year (Benjamin, 2013).

High risk of theft: Cash sales attract thieves who are either employees or non-employees. Many people have been reported injured and some of them killed because of carrying cash.1. On 28th December, 2015 a case was reported of the killing of a person who was carrying a huge amount of cash outside a hardware store north of Dar es Salaam.(ITV, 2015).

Revenue leakage: Cash payment cannot easily be traced and proved. The government loses a lot of revenue when people transact using cash since there is no automatic proof of payment. In a move to fight corruption, the Tanzania Police Force (TPF) in 2014 established a mobile money payment system for all traffic offences. This was done to remove the possibility of corruption. Introducing the system, the Traffic Police Commander, Commissioner Mohamed Mpinga said it has been established to curb loopholes observed in cash payments of penalties for traffic offences (Elizabeth Edward, 2014). The Dar Es Salaam Special Regional Police Commander Simon Siro told the press that they collected a total of 1.3 billion shillings between 25th April, 2016 and May, 2016 (Ayo TV, 2016). The use of mobile payment systems may have contributed to this.

5.2. Factors hindering P2B Merchant Payment Adoption

According to (John, 2016) the reasons why most people do not use P2B are awareness of the service i.e P2B, security, transaction cost, non-clarity on the differentiation between P2B and P2P, complexity in use and non-availability of merchants accepting P2B.

5.3. Conclusion

There is a room to increase revenue through P2B and transform our society into a cashless one. However some measures need to be taken by MNOs including replacing the usage of USSD code with a simple way for customers to access the mobile money payment menu. Technologies such as SIM Tool Kit (STK) and Near Field Communication (NFC) would be suitable if MNOs want P2B to pick up. MNOs should also increase the number of MMP merchants to reach more people. As part of motivating people to use the service they should remove the transaction costs and also, in collaboration with the government, educate people on the importance of the service.

References

Athumani, R. (2016). Tigo introduces wider services. Retrieved August 5, 2016 from http://dailynews.co.tz/index.php/home-news/52174-tigo-introduces-wider-services.

Ayo TV. (2016). Traffic Dar wamezikusanya Bilioni kwa faini tu barabarani (Dar traffic police collect billions in road offences penalties). Retrieved August 2, 2016, from https://www.youtube.com/watch?v=3d5Twng1Gps.

Bank of Tanzania1. (2013). Directorate of Banking Supervision Annual Report 2013. Retrieved August 15, 2015 from https://www.bot-tz.org/BankingSupervision/Reports/DBS ANNUAL REPORT 2013.pdf

Bank of Tanzania2. (2012). Financial Innovation and Financial Inclusion in Tanzania. In Proceeding of the sixteenth conference of financial institutions 26th - 27th November, 2012. Arusha.

Bank of Tanzania3. (2015). Payment System - Statistics. Retrieved August 24, 2015 fromhttps://www.bot-tz.org/PaymentSystem/statistics.asp.

Benjamin, C. B. D. (2013). The Cost of Cash in the United States. Retrieved August 2, 2016, from http: // fletcher.tufts.edu/ CostofCash/~/media /Fletcher / Microsites / Cost of Cash/ CostofCashStudyFinal.pdf.

Bloxham, A. (2010). Cashless Britain: a short history of payment methods. Retrieved November 16, 2015 from http://www.telegraph.co.uk/finance/personalfinance/8177684/Cashless-Britain-a-short-history-of-payment-methods.html

Edward, E. (2014, February 2). Trafiki wala rushwa sasa kusota njaa. Retrieved August 2, 2016, from http://www.mwananchi.co.tz/kitaifa/ Trafiki-wala-rushwa-sasa -kusota -njaa / -/1597568/2169900/-/format/sitemap/-/11ugu26z/-/index.html

Etim, A. S. (2014). Mobile banking and mobile money adoption for financial inclusion. Research in Business and Economics Journal, Voulme 9, No 4, 1–13.

Gerdes, G. R., & Walton II, J. K. (2002). The Use of Checks and Other Noncash Payment Instruments in the United States. Federal Reserve Bulletin, Volume 88, No 8, p.p 360-375.

GSMA. (2014). 2014 State of the Industry Mobile Financial Services for the Unbanked. Retrieved May 8, 2016, from http://www.gsma. com/ mobilefordevelopment /wp-content/ uploads/2015/03/SOTIR_2014.pdf

International Telecommunication Union. (2013). The Mobile Money Revolution. Part 1: NFC Mobile Payments. Published August 26, 2015, on https://www.itu.int/dms_pub/itu-t/oth/23/01/T23010000200001PDFE.pdf

Investopedia. (2015). Payment. Published November 5, 2015, from http://www.investopedia .com/terms/p/payment.asp

ITV. (2015). Watu 2 wamepigwa risasi na kuporwa fedha wakiwa katika gari lao eneo la Nabaki Afrika DSM. Retrieved August 2, 2016, from https://www.youtube.com / watch?v=Brg3JjKF_pc&feature=youtu.be

John, C. (2016). Assessing Factors Affecting Adoption of Mobile Payment in Tanzania. University of Dar es Salaam.

National Council for Financial Inclusion. (2016). National Financial Inclusion Framework 2014-2016. Retrieved May 5, 2016, from http://www.afi-global.org/sites/default/ files/publications/tanzania-national-financial-inclusion-framework-2014-2016.pdf

Tanzania Communications Regulatory Authority. (2016). Quarterly Communications Statistics. Retrieved April 11, 2016, from http://www.tcra.go.tz/images/documents/ telecommunication/CommStatMarch16.pdf

Vodacom Tanzania Limited. (2014). Vodacom Tanzania Launches new M-PESA Services. Retrieved November 19, 2015, from https://www.vodacom.co.tz/aboutus/news

Yaqub, J O;Bello, H.T; Adenuga, I.A;& Ogundeji, M. . (2013). The Cashless Policy in Nigeria : Prospects and Challenges. International Journal of Humanities and Social Science, Volume 3, No 3, pp.200-212.

Enhancing Home Delivery

■ **Abel John - Senior Postal Affairs Officer**
Tanzania Communications Regulatory Authority
Email: abel@tcra.go.tz

THE postal sector is explicitly undergoing a profound transformation. The market is moving away from letters towards goods and services driven by e-commerce. This transformation is purely market driven and not a choice of the sector. The postal industry has embraced innovation in order to respond to the rapid evolution of consumer needs and to remain competitive in changing markets. In today's digital society, innovation allows postal services to evolve into an essential element in the digital eco-system. At the same time, posts have been actively pursuing new areas of growth by diversifying their services

Posts have built giant organizations over the years, especially in the emerging markets, to meet universal obligation, which makes this transformation more difficult, as the posts struggling to survive by transforming and restructuring to harness the benefit accrued by e-commerce are in their prime time.

Tanzanians are partially addressed due to the fact that the physical addressing and postcode system exists in a few areas especially urban. It is therefore difficulty for Tanzanians to participate in buying goods through electronic (online) auctions. This is a big disadvantage of the existing postal addressing system to Tanzanians and if not resolved it will have catastrophic consequences to the national economy. Mail is generally addressed to post office boxes since this is the only delivery service for ordinary mail offered by the Tanzania Posts Corporation (TPC).

The physical address is either not known or unavailable to many people. In Tanzania therefore a typical address of ordinary mail would bear the name of the recipient, a numerical serial number of a private letter box and the name of the post town, the district or region as the case may be.

The existing addressing system has several disadvantages, major among which are:-

- The address is not unambiguous due to missing postcodes;
- Majority of Tanzanians have no physical and postcode addresses.
- Delays in deliveries are caused by wrong Post Office Box numbers, similarities in location names, multiple appearances of family names, etc;
- The private boxes in the post offices are few compared to the number of users in major cities and towns;
- The practise of sharing Private Office Boxes between multiple customers increases the possibility of wrong and late deliveries;
- The current system is not easily responsive to high quality service demand for e-commerce;

CHANGING THE PARADIGM OF THE POST

Rethinking the delivery model has seen posts introducing many initiatives which take into consideration not only price but plans and people dimensions.

With social media, mobile devices and the ease of communicating preferences, some people find it is more convenient to have e-commerce purchases delivered to their office or redirected to pick up points or lockers. Other preferences could include groceries, medicine prescriptions for the sick, elderly and some meals delivered at home.

From a route planning perspective, different strategies can be taken when implementing transformation, planning must be measured objectively and scientifically by, for example, correctly evaluating the routes and putting in place sustainable transformation measures that meet expectations.

The posts operators have realised the need for change hence have started reacting by developing new logistics concepts to follow the trends of growing e-commerce and falling mail volume, by placing more focus on delivery of small parcels and priority items.

New delivery models have to be developed which should allow on-time delivery, delivery on demand, short-term delivery or multiple daily deliveries while also being cost and time effective; to avoid empty rides and at the same time offer more services, collecting functions performed, postmen both delivering and taking information through improved logistics.

Most routes are made up of travel to the first delivery point and from the last stop or service time at the address; unproductive travel or deadhead between addresses. Evaluating route duration is done by adding the duration of the indoor and outdoor tasks. These itineraries therefore call for a rethinking of the delivery model through working with these variables.

Historically cities in the developed countries have been accustomed to seeing a model where mailmen deliver mail on foot or using a bicycle, courier and drivers delivering parcels using vehicles and in some cases collecting from street letter boxes and replenishing mailmen routes. Sometimes some even use trucks. With this approach, many routes can serve the same area and these can originate from different depots and mail centres.

The Post industry can be transformed by undertaking initiatives such as mail sorting technology and combining operations to perform regular mail delivery, street letter box collection and small parcels delivery operations in the same route. The objective of this approach is to service the same area and same number of addresses/points but with fewer resources.

Quality selection and products delivered to homes attracts many citizens to pay the subscribed amounts. Currently the awareness is low but with time it will grow just like the way smartphones started out as a tool for stockbrokers and corporate executives before becoming mass-market devices.

Home delivery is changing postal paradigms.

The focus should be on two areas, delivery and customer service, so that resources are concentrated in excelling in delivery modals. As with any delivery service, people need to be willing to pay for what the service is worth. Too many people are looking to get all their groceries or restaurant items for the same price they pay in the store and without having to pay large delivery costs.

Examples are online e-commerce sites like Amazon which have succeeded because they were not in search of profitability in the early stage; rather they positioned themselves for the long haul knowing that as time goes on, internet infrastructure would develop to a stage where consumers would develop trust for the web and high speed internet would eventually come.

The simple reality of Tanzanians and least developing countries sending less mail every year continues to drive the need to transform our national postal services. As the market leader in consumer parcel delivery, the post must also respond to the growing demands of online shopping; the goal being to create a sustainable Post that is able to respond to the changing needs of the citizens. Digitally connected consumers, looking for lower prices, greater convenience and a seamless experience in buying, receiving and returning products, are forcing companies and postal organizations to rethink traditional parcel delivery methods.

Armed with social networks, greater choices and rapid reviews of companies and services, these savvy consumers, already driving e-commerce demand, now are forcing increased competition for the "last mile," the literal home stretch in delivery service – to the door, parcel lockers, access points or crowd storage.

Understanding customer needs and creating solutions aimed at improving their delivery experience is an important aspect of gaining market share. That relationship can also be leveraged to sell new services directly to consumers which presents additional revenue opportunities,

Successful companies and postal organizations harness the power of today's consumer to remain relevant while capturing increased market share. Since consumers wants same day, time definite, alternative collection points and whole range of specialist services.

Consumer convenience and cost reduction have been the primary objectives guiding the change. Traditional postal organizations, already locked in competition with private delivery companies are now facing the possibility of companies like Amazon creating their own delivery supply chains combined with the very real threat of share economy start-up.

Resent Study Highlights

The postal market trends: There is a trend that has determined that business to consumer (B2C) will continue to grow in significance across geographies over the coming years. The trend shows that B2C will surpass business to business (B2B) in terms of parcel volumes. Cyber firms around the world are scaling up to meet future consumer demand, expanding capacity and modernizing networks in the parcel delivery business:

These investments are being made to remain competitive in the face of new entrants in last-mile delivery and with the understanding that delivery experience is a key variable for customer satisfaction.

Enhancing Home Delivery

Consumers now have many more choices and options for delivery services. Successful courier-express-parcel companies will focus on the recipient and deliver on consumers' wish lists:

Communicate proactively: Consumers place high importance on tracking and notification by sending information about delivery through e-mail or mobile devices.

Delivery control: Consumers are demanding a better last mile service that keeps them in control of how, when and where their parcels are delivered. Delivery schedule or secure delivery options are the highest importance in urban consumers.

Delivery locations: As choices broaden, consumers want new delivery options such as lockers or pickup locations that enable a secure, 24x7 and sometimes anonymous delivery option.

Delivery timing: While there is significant investment in speed, companies should focus on giving consumers a range of delivery times that provides flexibility depending with the locality.

Creating new delivery products: Urban customers are particularly focused on speed and service. New products such as same day delivery are increasingly becoming available, may lead to entirely new retail experience and can be monetised ,creating the dual benefits of improving the customer experience while generating new sources of revenue.

Deliver to People not Places: Providing highly valued personalized services such as tracking and delivery scheduling and notification services help to create stronger bond and protect market share and create new revenue streams.

Offer paid and free services: Combining paid and free services will enable postal organisations to significantly reduce embrace the large market share as well as reaching a broader base of customers, impacting market share protection and growth.

Tanzania Posts Corporation has taken the initiative of introducing new products such as pCUM, EMS, EMS Cargo and the new service of Posta Mlangoni (the post at the doorstep) as a new service offered by the Corporation for the purpose answering the call for the need of home delivery through the use of the infrastructure of New Addressing and Postcode System. Under this system, the address indicates clearly a house number and street name and the respective postcode.

Articles intended for office/home delivery must be conspicuously marked "Posta Mlangoni" either in writting affixing a special label, or rubber stamping at the head of the address side and be presented at a post office counter or delivery offices.

The mode of addressing any "Posta Mlangoni" item with Postcode shall bear a detailed address as below:-

i. Full names/ Title of the addressee (MUST)
ii. Name of company/Building/Floor number/Apartment (Option)
iii. House number and Name of Street/Shehia (local government administrator)/Kitongoji (locality) (MUST)
iv. Name of Kijiji (village)/ Serikali za Mtaa (Local Government) (For Rural or Semi Urban)
v. Post office private box/bag (where necessary)
vi. Postcode number and Ward/Area (MUST)
vii. Name of Town/DISTRICT/ REGION (MUST)
viii. Country (For International Item)

For example:

Amani Shangwe,
45 Jamhuri Street,
P.O.Box 148,
11104 KISUTU,
DAR ES SALAAM,

The delivery of items (ordinary letters, packets) should be done on the door at 45 Jamhuri Street at Kisutu Area in Dar es Salaam.

DELIVERY OF "POSTA MLANGONI" ITEMS

- The delivery should take place according to road maps supplied;
- No delivery note (call note) will be issued for delivery of "Posta Mlangoni" post code items;
- No signature for delivery of the "Posta Mlangoni" items is required;
- Delivery at the owners premises shall be done according to their wish.

Conclusion

In the near future with proper planning and leadership, a clear implementation framework and technology, rethinking the delivery model with sustainability in mind not only falls under a corporate responsibility obligation but becomes a viable and profitable opportunity for posts. The expectation will be met by Posts delivering and providing convenient options and increased control to consumers, developing a direct digital connection with customers and generating sustainable revenue streams. All this involves a shift in organizations culture, vision, values, norms, systems, language, beliefs and habits hence the need to look to new streams of business alongside with customer first mentalities, through innovation in the areas of products and services, technology, process and business models.

"Let's step out of our comfort zone and test new ideas upon which we can build the future of the post" Bishar Hussein Direct General UPU (2015)

References:

Derek Osbon; Reinventing the Post, Building a sustainable future (2015)
MER-Mail & Express review spring 2016
MER-Mail &Express review spring 2015
http://www.upu.int/en/activities/e-commerce/about-e-commerce.html

Mobile Number Portability In Tanzania

Introduction

MOBILE Number Portability (MNP) is the ability to change a mobile service provider without changing one's telephone number. It allows subscribers to keep their telephone numbers when they move from one mobile service provider to another.

There are different forms of Portability in communications, namely: Service Portability where the customer keeps their number while changing services e.g. pre-paid to post-paid; Location Portability which applies only to geographically based services, i.e. fixed line portability, and Mobile Operator Portability where the customer changes from one operator to another. TCRA has implemented this last type of portability, which was put in service on 1st March 2017.

MNP brings increased freedom of choice to customers whereby they are capable of assessing the quality of services offered by different mobile operators and move with their numbers. It should be noted that without MNP customers could actually switch anyway and give up their number, thus incurring a utility loss, which is why some customers stick to a service provider that is not their preferred choice. With MNP, the number becomes the identity of the subscriber.

MNP brings several advantages to consumers, service providers and the ICT industry in general. Generally, MNP encourages competition because no operator would like to lose an existing customer, thus leading to improved Quality of Services (QoS), Quality of Experience (QoE), network coverage, customer care services and services innovations with affordable prices. New entrants in the market need better opportunities to win existing customers and MNP creates this favourable market condition. From a mobile operator point of view, MNP increases the number of happy and satisfied users of the services, which again leads to increased revenue growth and reduced number of customer complaints.

The absence of an MNP service in a competitive environment makes personal and business communications costlier. It when involves a change of SIM-cards, manual notification of number change and change of stationery such as letterheads, envelopes, business cards, signage or billboards; which can potentially lead to loss of business.

Mobile Number Portability Implementation In Tanzania

Mobile number portability has been implemented based on the Electronic and Postal Communication (Mobile Number Portability) Regulations, 2011. Several stakeholders have been involved, including Mobile Networks Operators, Value Added Services Aggregators, Banks and the MNP Clearing House Administrator (an independent trusted and licensed third party) with the aim of making sure the services do not affect other services such as mobile banking and mobile payments.

The MNP Clearing house administrator manages port-orders and updates the stakeholders where a particular number has been ported to using a central reference database that updates the local databases of the stakeholders.

In terms of call routing, MNP in Tanzania has been implemented using the All Call Query method, where the Mobile operator, before routing the call, check the local database which is updated by the centralized database operated by the MNP clearing house (MNPCH) administrator as illustrated in Figure 1 below.

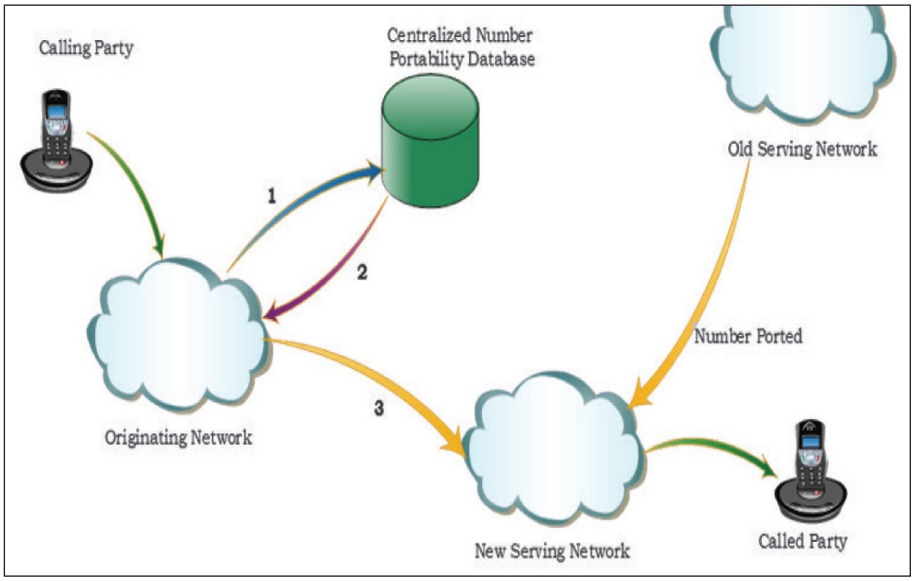


Figure 1: Call Handling in MNP

In Figure 1, if customer B (called Party) has ported from the Old Serving Network (Donor Operator) to a New Serving Network (Recipient Operator) and is being called by Customer A (calling Party) in the Originating Network (ON), the ON checks in its local database, which is regularly being updated by the Centralized Number Portability Database, to know which network is currently serving customer B and then route the call accordingly.

The Mobile Operators are connected to the MNP Clearing House through a physical connection to the primary site and via Virtual Private Network (VPN) over the Internet to the secondary site for disaster recovery reasons. The MNPCH handles and manages the port requests from recipient operator to the donor operator and notifies the porting customer on the progress of the

Mobile Number Portability In Tanzania

request till the order is completed. The MNPCH then notifies all mobile operators by broadcasting the successfully ported number, so that they update their local database as illustrated in Figure 2 below.

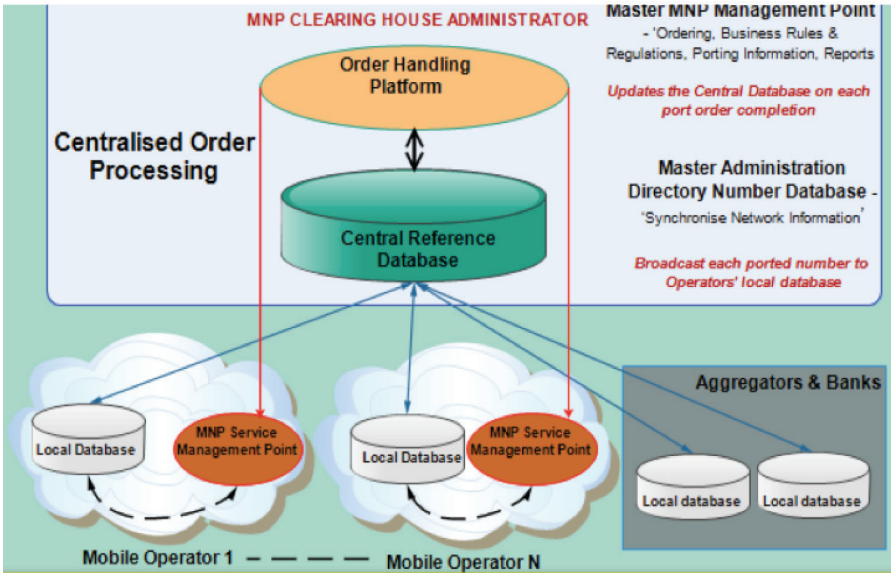


Figure 2: Port Order Handling in MNP

Porting Process

Porting processes describe the procedures to be taken by individual customer (pre-paid and postpaid) who wants to port from one network to another. This is summarized below:-

1. The Customer goes to the retail shop or authorized dealer of his/her chosen new mobile service provider and informs the staff dealing with MNP that he/she would like to move to this network and keep his/her mobile number.

2. The staff will ask the customer to complete an application form; the Porting approval Request Form, whereby part of this form is an explicit statement that the customer agrees that he/she is liable for outstanding loans (airtime and/or mobile money) to his/her existing operator if any.

3. The customer will be required to provide proof of identity, either a National ID, Voting ID, Driving License, Passport or other officially validated photographic identity document. The customer needs to have the working phone with the number he/she wishes to keep.

4. If the customer has mobile money in his/her mobile wallet, he/she will be advised to cash this out prior to porting to avoid the wallet becoming orphaned, which will take complex process to be recovered.

5. The customer will be asked to text the word "PORT" to a special porting number '15080'. Assistance will be made available if required. This is done to provide more security and authentication.

6. After the customer has sent the confirmation message, the customer will receive a text (SMS) confirming that his/her request has been received and will be informed of the porting request progress by text.

7. Provided that the customer number is not barred or suspended due to previous non-payment, his/her port order will be processed in a very short time, usually less than 10 minutes. However the maximum possible time for processing the request is two working days. All this time the customer will continue to have basic communication services, but mobile financial services will be barred to avoid receiving money while porting is in progress.

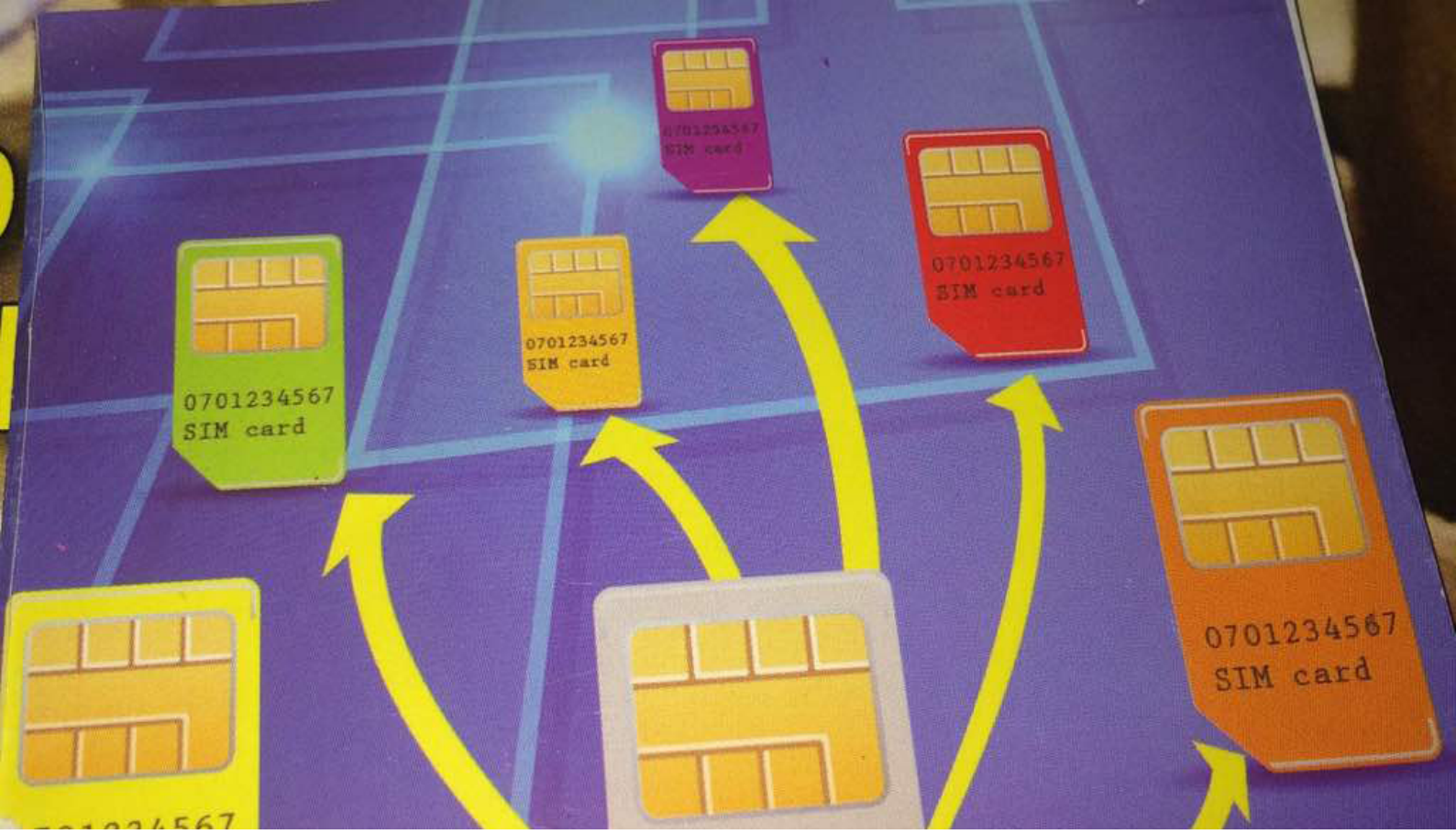
8. The new mobile service provider will provide the customer with a new SIM-card. The new SIM-card may be issued at a cost or free of charge by the new service provider. When the porting process is completed, the customer will receive an SMS asking them to remove old SIM-card and put a new SIM-card to continue with communication as customer of new service provider with his/her number unchanged.

Key Important Issues in MNP

1. **During Porting:** During porting, the new service provider will provide a new SIM-card to the customer at a cost or free of charge. The porting request shall be processed at a maximum of two working days, though in practice this process may take less than 10 minutes even before the customer leaves the recipient operators' point of MNP service provision, e.g. shop.

   Mobile financial services and other value added services will be put on freeze when donor the service provider accepts the port request in order to prevent instances where people might be sending money during the porting process.

2. **Frequency of Porting:** The customer who has ported to a network may decide to port to another network or return to his/her previous service provider, provided that he/she has



Mobile Number Portability In Tanzania

stayed in the current ported-in network for not less than 30 days.

It should be noted that if the customer is new or is a recently registered customer, he/she would not be allowed to port out until 60 days have passed since the date of registration/activation of that number.

3. **Notification of Ported Numbers:** When calling a customer who one may think is in the same network by looking at the corresponding mobile network destination code, but that customer has already ported out of this network; the caller will hear two beep tones as an alert that the called customer has ported out of the network and thus off-net charges may apply. Also when sending money in a similar situation, the customer will be notified accordingly.

4. **Mobile Banking Services:** All Banks providing mobile banking services have implemented systems to support MNP; therefore all transactions made will be routed correctly. However, since the customer will be given a new SIM-card, he/she will be required to visit his/her respective bank branch to activate the new line, should the current service provider support mobile banking services of that bank.

5. **Airtime and Mobile Money:** All pre-paid customers will be required to utilize their airtime before porting to avoid the risk of losing it, as airtime cannot be transferred to the new service provider. In addition, mobile money in the mobile wallet need to be cashed out before porting, otherwise the customer will have to follow a complex procedure to reclaim it after porting to another network.

6. **Retention by Donor Service Provider:** MNP has been designed to be recipient-led and the donor network service provider is not allowed in any way to convince the customer who has decided to port out to stay on. If this happens, the customer should contact the recipient operator or TCRA. However, the customer can decide on his/her own to cancel the porting request before sending confirmation SMS to 15080.

7. **Consumer Complaints:** If the customer has any complaints regarding porting he/she should contact the recipient operator. If the issue is not solved or the customer is not satisfied, then the same can be communicated to TCRA.

Conclusion

TCRA has introduced MNP to foster competition with the aim of improving quality of service, stimulate innovations and thus enhance consumers' convenience and flexibility as they opt to change from one service provider to another that offers better value for money or quality. It should be noted that the days of retaining customers based on network coverage alone is soon becoming a thing of the past. Going forward, the mobile communications service providers will attract new and retain existing customers based on not only network coverage, but also on quality of service, innovative packages, customer relations and tariffs; among other things. Mobile subscribers are encouraged to use this opportunity, which is freely available.

Msimamizi
Jarida la Mamlaka ya Mawasiliano Tanzania
HALIUZWI

MNP Huduma ya Kuhamia Mtandao Mwingine wa Simu Bila Kubadili Namba ya Simu ya Kiganjani

UFAFANUZI

1. Huduma ya MNP maana gani kwa mteja?

Huduma ya kuhamia mtandao mwingine bila kubadili namba ya simu ya kiganjani (MNP), ina maana kuwa mtumiaji anabaki na namba yake ya awali iwapo ataamua kuhamia mtandao mwingine wa simu za kiganjani nchini Tanzania. Kimsingi, ni huduma ambayo inakuwezesha kubakia na namba yako bila kujali unatumia mtandao gani. Hivyo, iwapo utabadilisha mtoa huduma wa simu za kiganjani hutakuwa na haja ya kusumbuka kuwataarifu watu wako wa karibu – marafiki, familia na wafanyakazi wenzako au washirika katika shughuli zako kwamba umebadilisha namba kwani inabakia ileile.

2. Huduma ya MNP ina faida zipi?

- Utaendelea kutumia namba yako ya awali unapohama kutoka mtoa huduma mmoja kwenda mwingine na hivyo kufurahia uhuru na huduma za mtoa huduma mpya.
- Utapokea simu na meseji bila kujali ni mtandao upi umehamia na bila kuwa na haja ya kuwataarifu marafiki, familia na wafanyakazi wenzako au washirika katika shughuli zako kwamba umebadilisha mtoa huduma wako.
- Utaokoa fedha kwa kuwa hutakuwa na haja ya kununua laini mpya kwa kila mtoa huduma au kuwa na simu ya kiganjani zaidi ya moja.
- Utaweza kuchagua mtoa huduma ambaye unaona anatoa huduma bora zaidi, anakidhi matarajio yako na ana ubunifu katika kutoa huduma.

3. Ni wakati gani naweza kuhama na namba yangu?

Utaweza kutumia huduma hii ya kuhamia mtandao mwingine bila kubadili namba ya simu ya kiganjani kuanzia Machi 2017.

- Mwezi Machi 2017, huduma ya kuhamia mtandao mwingine bila kubadili namba ya simu ya kiganjani itatolewa na makampuni yote ya simu za kiganjani.

4. Nani anaweza kutumia huduma hii?

Huduma ya MNP itatumiwa na wateja wote nchini wanaolipia huduma kwanza na wanaolipia huduma baada ya matumizi. Ili kutumia huduma hii, simu ya mtumiaji lazima iwe inatumika, yaani haijafungiwa au kusimamishwa kwa muda.

a) Iwapo unatumia huduma kwa utaratibu wa malipo baada ya huduma, yaani Post-Paid, utaweza kubadili mtoa huduma isipokuwa tu kama umefungiwa au kusimamishiwa huduma kutokana na kutokulipia ankara za matumizi;

b) Iwapo unatumia huduma kwa utaratibu wa malipo baada ya huduma na hujakamilisha masharti ya msingi ya mkataba na mtoa huduma wako wa sasa, utatakiwa kulipa malimbikizo ya madeni kama yalivyoainishwa kwenye mkataba;

c) Iwapo unatumia huduma kwa utaratibu wa malipo baada ya huduma utapokea ankara ya matumizi yako hadi namba yako itakapohamishiwa kwa mtoa huduma mpya. Utatakiwa kulipa Ankara hizi kabla ya kuhamia kwa mtoa huduma mpya;

d) Utaendelea kupokea ankara za matumizi hadi namba itakapohamishiwa kwa mtoa huduma mpya. Utapokea Ankara ya mwisho hadi siku 60 baada ya kuhamisha namba yako; kisha utapewa siku 30 za kulipa Ankara hizo, vinginevyo utakuwa katika hatari ya uhamaji wako kusitishwa au namba yako kufungiwa;

e) Iwapo unalipia huduma kabla ya matumizi, yaani Pre-Paid, hutaweza kuhama na salio lililopo na utatakiwa kutumia salio hilo kabla ya kuhama, la sivyo salio lako litapotea;

f) Iwapo una salio katika akaunti ya pesa mtandao ni lazima ulitoe salio hilo kabla ya kuhama vinginevyo salio litabaki bila mwenyewe na itabidi ufuate mchakato mrefu ili kuweza kupata pesa zako ambazo wakati wote zitakuwa salama hadi utakapokamilisha mchakato huo.

5. Itanigharimu kiasi gani kuhama na namna yangu?

- Hakuna gharama za kuhama na namba yako. Hata hivyo, kabla ya kuhama itabidi ununue laini mpya ya simu ya kiganjani, yaani “SIM card” kutoka kwa mtoa huduma mpya.

6. Ni nini ninatakiwa kufanya ili kupata huduma hii?

1. Nenda vituo vya mauzo au kwa wakala anayetambuliwa wa mtoa huduma unakotaka kuhamia na umueleze mhudumu kwamba ungependa kuhama na namba yako.
2. Mhudumu atakutaka ujaze fomu maalum ya maombi (fomu moja).
3. Sehemu ya Fomu ya maombi ya kuhama ni tamko rasmi kwamba unakubali kuwa utawajibika kwa madeni yoyote ambayo yanatokana na huduma ulizokuwa unapata kutoka kwa mtoa huduma wako wa awali kama yapo.
4. Utatakiwa kutoa vitu vifuatavyo: -
   a) Kitambulisho chenye picha yako – kinaweza kuwa Kitambulisho cha Taifa, Kadi ya Mpiga Kura, Leseni ya Udereva au pasipoti au kitambulisho chochote rasmi kinachotambulika.
   b) Simu ya kiganjani inayofanya kazi yenye namba unayotaka kubaki nayo.
5. Iwapo una salio katika akaunti ya pesa mtandao utashauriwa kutoa pesa kabla ya kuhama ili kuepuka usumbufu kama ilivy-

Huduma ya Kuhamia Mtandao Mwingine wa Simu Bila Kubadili Namba ya Simu ya Kiganjani

oelezwa kwenye masharti ya kuhama.

6. Utatakiwa kutuma meseji yenye neno "HAMA" kwenda namba '15080' ambayo ni namba maalum ya kuhama. Msaada utatolewa iwapo utahitajika ili kufanikisha hili.
7. Utapokea meseji kukujulisha kwamba maombi yako yamepokelewa.
8. Iwapo namba yako haikuzuiliwa au kusimamishwa kwa muda kutokana na kutokukamilisha malipo ya madeni ya mtoa huduma wako wa awali, maombi yako yatashughulikiwa na utajulishwa kwa meseji kuhusu maendeleo ya mchakato huu.
9. Mtoa huduma wako mpya wa huduma za simu za kiganjaji atakupatia laini mpya.
10. Ili kuzuia kupokea mihamala ya fedha mtandao wakati wa kuhama, huduma za kifedha zitasitishwa kwa muda mpaka namba ikapohamishwa kwa mtoa huduma mpya, ambapo utatumia huduma zake za fedha mtandao kama utajiunga na huduma zipo.
11. Katika kipindi cha kuhama huduma za kupiga na kupokea simu na ujumbe mfupi zitaendelea kama kawaida.
12. Katika hali ya kawaida uhamaji utakamilika haraka, mara nyingi siku hiyo hiyo au, iwapo utachelewa sana, ndani ya siku mbili za kazi baada ya kukamilisha utaratibu wa maombi. Wakati huo namba yako itakuwa imeshahamishwa kwa mtoa huduma wako mpya na laini yako ya awali haitatumika tena. Utatumiwa ujumbe mfupi kuwa uhamaji umekamika na ubadilishe laini.
13. Ikifikia hapo, weka laini mpya uliyopewa na mtoa huduma wako mpya kwenye simu yako. Iwapo huna uhakika wa nini cha kufanya, unaweza kwenda kwa mtoa huduma wako mpya au wakala wake au kuwapigia simu na wataweza kukusaidia.
14. Mchakato umekamilika.

7. Kuna mengineyo kuhusiana na huduma hii?

- Meseji ambazo zimetumwa kwako, lakini hazijaingia kwenye simu yako zinaweza kupotea wakati wa kuhamishwa kwenda mtandao mwingine ambacho ni kipindi kisichozidi dakika kumi na tano (15).
- Meseji za sauti yaani "voicemails" za zamani ulizokuwa umepata na kuzihifadhi kwenye laini ya simu zitapotea. Namba za simu za watu ambazo umezihifadhi kwenye laini ya simu itabidi uzihamishie kwenye "memory" ya simu au "memory card" ili zisipotea utakapoweka laini mpya ya mtandao unaohamia. Aidha, itabidi ufanye utaratibu na mtoa huduma wako kuhusu huduma nyingine ulizokuwa unazipata moja kwa moja kutoka kwa mtoa huduma wako wa awali kama huduma za kibenki (mobile banking).
- Hutaruhusiwa kuhamia kwa mtoa huduma wa tatu au kurejea kwa mtoa huduma wako wa awali ndani ya siku 30 baada ya uhamaji wa kwanza.
- Ingawaje watoa huduma wote watatumia ujuzi na watakuwa waangalifu katika kutekeleza majukumu yao, katika kutoa huduma hii, hakuna fidia ambayo itatolewa kwa kuchelewa, kuvurugika au kukosekana kwa huduma kutokana na mchakato wa kuhama.

8. Wakati ninapopiga simu au kutuma fedha, nitajuaje kama iwapo namba hiyo imehama au la?

- Iwapo unapiga namba ambayo unadhania iko kwenye mtandao mmoja na wako lakini namba hiyo imehamia mtandao mwingine, utasikia mlio unapoanza tu kupiga simu hiyo kukutahadharisha kwamba gharama za simu unayopiga zinaweza kuwa juu zaidi ya unavyotazamia. Kwa mfano, iwapo uko kwenye mtandao wa Vodacom na unapiga namba ya Vodacom ambayo imehamia Tigo au Airtel au mtandao mwingine wowote, utasikia mlio unapoanza kupiga simu hiyo.
- Unapotuma fedha, utajulishwa kuwa namba ya mtumiaji wa simu unayemtumia fedha imehamia mtandao mwingine na hivyo kukupa uhuru wa kuamua kuendelea kutuma fedha au la.

9. Je, nitapokea simu nyingi za maafisa mauzo wa watoa huduma kunizuia nisihame?

- Hapana. Mtoa huduma wako wa sasa hatakiwi kukupigia simu wakati wa mchakato wa kuhama kujaribu kukushawishi kuwa ubakie naye. Hata hivyo, mtoa huduma wa sasa anaweza kukupigia simu kuhusiana na malimbikizo ya malipo ya huduma alizotoa kwako kama yapo.

10. Je mtoa huduma wangu wa sasa anaweza kujaribu kunishawishi nibakie naye wakati nikitaka kuhama?

- Hapana. Mtoa huduma wako wa sasa hatakiwi kuwasiliana nawe wakati wa mchakato wa kuhama ili kujaribu kukushawishi kubakia kwako. Iwapo atajaribu kukushawishi unatakiwa kutoa taarifa kwa mtoa huduma wako mpya unapohamia.

11. Iwapo mtoa huduma wangu wa awali atanipigia simu au atanisumbua kama njia ya kunitaka nirejee kwenye mtandao wake ndani ya siku 30 baada ya kuhama, nitoe taarifa kwa nani?
    - Toa taarifa kwa mtoa huduma wako mpya.

12. Nifanye nini iwapo nitakuwa na tatizo au malalamiko?

Kwanza wasiliana na mtoa huduma wako mpya ili kupata ufumbuzi. Isipowezekana, au usiporidhika, lalamika kwa Mamlaka ya Mawasiliano Tanzania (TCRA).

13. Ni namba zipi zinazoweza kuhamishwa?

- Namba yoyote ya simu za kiganjani inaweza kuhamishwa bila kujali inatumiwa kwa aina gani ya huduma – mfano maongezi, meseji, data, kujua maeneo kijiografia kwa mfumo wa GPS na kadhalika

14. Huduma za kuhama zinapatikana muda gani kila siku?

- Huduma za kuhama zitapatikana wakati maduka, ofisi na maeneo ya mauzo ya mtoa huduma wako mpya vitakapokuwa

Huduma ya Kuhamia Mtandao Mwingine wa Simu

vimefunguliwa kwa wateja.

15. Ninaweza kubadili mawazo wakati wa mchakato wa kuhama?

- Unaweza kubadili mawazo wakati wowote kabla ya kutuma ujumbe mfupi wa maneno wa kuthibitisha kuhama kwenda namba 15080. Mara tu ujumbe huu utakapotumwa, hutaweza tena kusimamisha maombi yako ya kuhama na mchakato wa kuhama utaendelea hadi utakapokamilika.

16. Nitafuatiliaje mwenendo wa maombi yangu ya kuhama?

- Utajulishwa kwa njia ya meseji kuhusu mwenendo wa mchakato wa maombi yako ya kuhama mpaka utakapokamilika pia utajulishwa kwa ujumbe mfupi wa maneno.

17. Nini kitatokea iwapo maombi yangu ya kuhama yatakataliwa au hayatakamilika?

- Utatakiwa kuwasiliana na mtoa huduma wako mpya kupata ufumbuzi wa tatizo.

18. Kama niko kwenye mfumo wa kulipia huduma kabla, yaani pre-paid, na nina salio la muda wa maongezi na huduma nyingine, ninaweza kuhama navyo?

- Wateja walio kwenye mfumo wa kulipia huduma kabla ya matumizi hawataweza kuhama na salio na watatakiwa kutumia salio hili kabla ya kuhamia kwa mtoa huduma mwingine la sivyo salio lako litapotea.

19. Iwapo ni mteja wa kulipia baada ya huduma, yaani post-paid, ninaweza kuhama iwapo mkataba wangu wa awali haujaisha au iwapo sijalipia huduma nilizopata?

- Ndiyo. Wateja wanaolipia baada ya huduma wanaweza kuhama na namba zao. Hata hivyo, mwanzoni mwa mchakato wa kuhama, wateja hawa wanatakiwa kukamilisha malipo ya malimbikizo ya ankara zao ikiwa ni pamoja na gharama zozote zilizokubaliwa kuhusiana na kukatisha mkataba kabla ya muda.

20. Itakuwaje kwa meseji ninazotuma au kutumiwa wakati ninapohama?

- Meseji ambazo zimetumwa kwa mteja kabla ya kuhama, lakini zikawa hazijafikishwa kwa mteja huyo zinaweza kupotea.

21. Je, naweza kuhamisha namba moja mara ngapi kwa mwaka?

- Unaweza kuhamisha namba yako mara nyingi kadri unavyotaka. Hata hivyo,huwezi kuhamisha namba moja kwa mtoa huduma mwingine ndani ya siku 30.

22. Iwapo nitahama na kupewa laini mpya na zikapita siku 30, je itabidi nifuate utaratibu uleule kurudi kwa mtoa huduma wangu wa awali?

- Ndiyo. Kila mara unapotaka kuhama na namba yako, utatakiwa kwenda kwenye ofisi za huduma kwa wateja, kwa wakala wa mtoa huduma au kwa mtoa huduma wa mtandao unaotaka kuhamia kuomba kuhamia mtandao huo. Utapewa laini mpya ya simu yenye namba ileile.

23. Iwapo ninarejea kwa mtoa huduma wangu wa awali, nitahitajika kupata laini mpya kutoka kwa mtoa huduma wa awali na hivyo kufanya laini yangu ya zamani kutokufanya kazi?

- Ndiyo. Utahitajika kupewa laini mpya ya simu kila mara unapohama kwenda kwa mtoa huduma mpya kwani laini yako ya zamani haitaweza kutumika tena.

24. Nitahitajika kulipia laini mpya ya simu?

- Utapewa laini mpya ya simu na mtoa huduma wako mpya ama bila malipo au kwa malipo kutegemea na utaratibu wake.

HAKI NA WAJIBU WA WATUMIAJI WA HUDUMA ZA MAWASILIANO

HAKI ZA WATUMIAJI

MOJAWAPO ya majukumu ya TCRA ni kulinda watumiaji wa huduma za mawasiliano. TCRA inafanya kazi hii kwa kupokea malalamiko ya watumiaji, kusimamia kanuni zinazotokana na Sheria, kufuatilia na kuchunguza malalamiko,kutatua malalamiko, kutoa elimu kwa watumiaji na wananchi na kukutana na watoa huduma kujadili masuala yanayohusiana na watumiaji.

Baadhi ya haki za mteja au mtumiaji wa huduma za Mawasiliano ni:

Upatikanaji wa huduma: Mtumiaji ana haki ya kupata huduma za msingi za mawasiliano kwa bei nafuu.

Kupata huduma bora: Mtumiaji ana haki ya kupata huduma zenye ubora ambazo zinaendana na gharama za huduma. Anapaswa kupata huduma ambazo zinaendana na dhana ya thamani ya fedha inayolingana na huduma:

Kupewa taarifa kuhusu huduma na bidhaa: Mtumiaji ana haki ya taarifa kamili kuhusu huduma zinazotolewa na mtoa/ mwendesha huduma kabla ya kuijunga na huduma husika. Mtumiaji ana haki ya kudai maelezo ya kuridhisha pale ambapo kuna kipengele cha "*vigezo na masharti kuzingatiwa*".

Kutokubaguliwa: Mtumiaji ana haki ya kutendewa kwa usawa bila ya ubaguzi. Ubaguzi huo unaweza ukawa katika mfumo wa kunyimwa kupata huduma au utoaji wa ubora wa huduma mbalimbali kwa wateja tofauti wanaolipa kiasi cha fedha kinacholingana.

Malalamiko: Mtumiaji ana haki ya kulalamika kuhusu ubora, ucheleweshaji, kiasi na viwango vya huduma na masuala mengineyo kuhusiana na mwenendo wa huduma zinazotolewa.

Kutatuliwa matatizo yake: Kila mtoa/mwendesha huduma anatakiwa na TCRA kuweka utaratibu wa kutatua malalamiko ya wateja kuhusiana na huduma anazozitoa au matatizo yanayotokana na huduma hizo. Endapo malalamiko hayakutatuliwa kiasi cha kuridhisha na mtoa/ mwendesha huduma, mteja anaweza kuwasilisha malalamiko yake TCRA.

Usalama na Ulinzi: Mtumiaji ana haki ya kupewa huduma ambazo matumizi yake ni salama na imara. Mtoa/ mwendesha huduma anapaswa kuhakikisha kwamba vifaa vyake vyote vinakidhi mahitaji ya usalama wa afya kabla ya kutumiwa na wateja.

Kuwa na usiri au faragha katika matumizi: Mtumiaji ana haki ya usiri au faragha katika matumizi ya huduma. Sheria na kanuni vinakataza kutolewa kwa taarifa za mteja kwa mtu yeyote bila ya ridhaa ya maandishi ya mteja mwenyewe. Taarifa zitatolewa tu pale ambapo zinahitajika katika uchunguzi wa matukio ya kijinai na kwa utaratibu uliowekwa kisheria na kikanuni.

Elimu kwa Watumiaji: Watumiaji wana haki ya kuelimishwa kuhusu huduma zinazotolewa kwao na masuala yanayohusiana na matumizi ya huduma za mawasiliano.

Kupewa taarifa kabla ya kusimamisha au kukatisha huduma: Wateja wana haki ya taarifa ya kusimamisha huduma hususan zile huduma muhimu. TCRA inawataka watoa/ waendesha huduma wote kuwataarifu wateja wao mapema kuhusu nia ya kusimamisha utoaji huduma wakieleza wazi sababu za kufanya hivyo.

Uwakilishi: Wateja wana haki ya kuwakilishwa katika kufuatilia masuala ya huduma wanazopata.

Kupata taarifa kamili za malipo na ankara: Wateja wana haki ya kupata taarifa kuhusu malipo wanayotakiwa kufanya. Endapo mteja hakufurahishwa na bili yake, anaweza kufuatilia kwa mtoa/ mwendesha huduma ili kupata maelezo ya kina kuhusu anachotakiwa kulipia.

WAJIBU NA MAJUKUMU YA MTUMIAJI

Pamoja na haki, watumiaji wa huduma za mawasiliano wana wajibu kama ifuatavyo:

Kutii sheria za nchi Matumizi halali ya huduma: Watumiaji wanatakiwa kutumia huduma za mawasiliano kwa kufuata sheria za nchi; bila kuvunja sheria. Huduma za mawasiliano zisitumike kama nyenzo ya kufanya uhalifu wa aina yoyote. Sheria mojawapo ni Sheria ya Mawasiliano ya Elektroniki na Posta (EPOCA) ya 2010,Sheria ya Makosa ya Mtandao ya 2015 na Sheria nyingine.

Kulipia huduma wanazotumia: Watumiaji wana wajibu wa kulipia huduma ambazo wamejiunga nazo.

Kuhifadhi Mazingira na Utunzaji wa nyenzo za mawasiliano: Kila mtumiaji ana jukumu la kuhakikisha kuwa matumizi yake ya huduma za mawasiliano hayaathiri mazingira. Aidha mtumiaji ana jukumu la kutunza vifaa na nyenzo zote za mawasiliano karibu yake.

Kuwa makini: Ni jukumu la mtumiaji kuwa makini na kuhoji masuala kama vile kanuni na masharti ya huduma. Watumiaji wanapaswa kujua haki na wajibu wao pamoja na kutafiti taarifa nyingine wanazoweza kupata.

Kuunga Mkono Udhibiti: Mteja anatakiwa kutoa taarifa TCRA pale ambapo anaona kasoro katika utoaji wa huduma yeyote ya mawasiliano.

Kulalamika: Ni wajibu wa mteja kulalamika kwa vyombo husika pale wanapoona kasoro kwenye utoaji wa huduma:

Kutambua kasoro katika matumizi na kutoa taarifa: Watumiaji wanatakiwa kufuatilia utoaji huduma na kutoa taarifa pale wanapoona kasoro.

Internet of Things and TCRA's Areas of Focus – Emerging Issues in Communications

■ **Dr. Emmanuel C. Manasseh**
Tanzania Communications Regulatory Authority
P.O. BOX 474, Dar es Salaam, Tanzania
E-mail: emmanuel.manasseh@tcra.go.tz

ABSTRACT —The Internet of Things (IoT) will bring benefits to a range of sectors and could change the way we live However, realising the potential benefits from IoT innovations, depends on many factors such as network designs, appropriate allocation of resources and regulatory settings. This article identifies areas that are likely to be important in facilitating IoT developments and outlines aspects that have direct implications to the Tanzania Communications Regulatory Authority. The proposed priority areas include resource allocation such as spectrum, numbering and addressing system; networks security and privacy; as well as standards-setting. The study also assesses how existing regulatory framework can be used to further facilitate and enable consumers to benefit from IoT innovations.

I. Introduction

Internet of Things (IoT) refers to network of things that can exchange data through embedded electronics, software, sensors and connectivity. It is the inter- connection of many devices and objects using internet protocols [1], [2]. IoT is regarded as the next stage in digital communications convergence within the wider economy driven by increasingly connected devices accelerated by cloud and big data analytics [3], [4].

The IoT's services will notably impact the entire marketplace ranging from manufacturing and transportation to agriculture, utilities, healthcare and much more [5]. Indeed, IoT technology is generating unprecedented opportunities for developing new services, enhancing productivity and efficiency, improving real-time decision making, solving critical societal problems, and developing new and innovative user experiences [5].

With IoT, there will be more connected objects than people on the planet. The networks and data that flow from them will support an extraordinary range of applications and economic opportunities. However, as with any new technology, there is the potential for significant challenges too. In the case of the IoT, breaches of security and privacy have the greatest potential for causing harm [1], [6].

In addition, many IoT devices will communicate wirelessly, making the availability of spectrum, which is the raw material that underpins wireless services, an important factor. Thus, there is a need to clearly identify the IoT's spectrum needs for various applications and services in order to set strategies for meeting such demands.

Likewise, as for traditional telecommunication voice and data devices, IoT requires identifiers such as unique ID and the number or address to be identified in the network. The type and number of identifiers required depends on their connectivity model. In a vast network of interconnected IoT devices, numbering and addressing policies may need to be monitored and updated. Several countries have already reported scarcity of E.164 numbers due to machine to machine (M2M) communications and have updated their numbering policies by introducing separate dedicated M2M number ranges. Such decision largely depends on the country situation regarding number exhaustion.

Standards play a central role in enabling the creation of markets for new technologies. For the IoT to flourish, interoperability must apply across all parts of the system, including the transmission networks and the data being transmitted. Data and devices must have proportionate "security by default". Standards must protect against cybercrime and security threats and help to ensure that the system is trustworthy and trusted. They should also support energy efficiency as this will help increase the range of potential applications and manage the burden on energy supply.

Since it is widely known that the IoT will create enormous opportunities for the private sector and the government, TCRA is taking steps to ensure that Tanzania does not lag behind in utilizing these IoT services and applications. The main focus of the Authority is on promoting and creating a regulatory environment that fosters investment and innovation in the emerging IoT. Thus, TCRA's commitment is to develop a regulatory framework for the IoT to evolve in a way that will ultimately benefit citizens and consumers.

In this regard, TCRA is fostering and promoting a clear aspiration and vision for the IoTs. The aspiration is that our country will not lag behind in the development and implementation of the IoTs. The vision is that the IoT will enable goods to be produced with more creativity, services to be provided more effectively and scarce resources to be used more sparingly. Achieving this vision will deliver significant economic and societal benefits.

II. Key Areas of Focus

A. Spectrum and networks

It is expected that globally up to 50 billion 'smart' devices, ranging from cars and parking smart meters to coffee machines and retail stores would be connected to the internet by 2020, each using a tiny spectrum band to get online. Some IoT devices could make use of the existing mobile networks, while some could make use of spectrum at 2.4 and 5 GHz band, which is

Internet of Things and TCRA's Areas of Focus – Emerging Issues in Communications

used by a range of services including Wi-Fi. However, as the IoT sector develops, existing mobile or Wi-Fi networks may not always be suitable for millions of IoT devices to communicate data. Consequently, there may be a need for additional spectrum in the long term. Given this, TCRA will continue to monitor IoT spectrum utilisation, particularly in licence exempt bands, to identify when additional spectrum may be needed.

In the UK, te communications regulator - OFCOM has allocated 10MHz of very high frequency (VHF) spectrum in the 55 - 68MHz, 70.5 - 71.5MHz and 80.5 - 81.5 MHz bands, which is suitable for delivering IoT services in remote and rural areas. The main concern is that antenna size may prove to be a barrier to some IoT applications.

B. Standards

Standards play a central role in enabling the creation of markets for new technologies. As is typical for emerging technologies, commercial partnerships are driving competing standards for the IoT. Left unchecked, this carries a risk of restrictive standards being set and enforced by monopolistic providers and of fragmentation inhibiting the interoperability of devices, slowing growth and reducing the opportunities for entrepreneurs.

For the IoT to flourish, interoperability must apply across all parts of the system, including the transmission networks and the data being transmitted. Data and devices must have proportionate "security by default". Standards must protect against cybercrime and security threats and help to ensure that the system is trustworthy and trusted. They should also support energy efficiency, as this will help increase the range of potential applications and manage the burden on energy supply.

C. Skills and Research

There are important opportunities for developing skilled people. A broad range of skills will be key to the design, development, installation and maintenance of the IoT. There is a need for highly educated and qualified researchers and developers across multiple disciplines to create the applications that will deliver the greatest benefit to users.

Computational thinking and interpreting evidence is crucial in making informed decisions about every-day use of the IoT. Computer programming, including rigorous study of algorithms and representations of data, underpins the specialist skills needed.

D. Legal and Regulatory Framework

IoT technologies are likely to create new regulatory challenges. For example, the introduction of autonomous vehicles may significantly reduce road traffic incidents, but is unlikely to eliminate them completely. New questions of liability and protections for citizens and businesses will inevitably arise. Resolving these questions will be a critical factor to enable the introduction of more radical opportunities and poses novel regulatory and governance challenges.

Moreover, the IoT already poses challenges in the sensitive area of personal identity and privacy. The scale of personal information, particularly locational and financial information, which is collected by existing technology, is huge. This data collected will only increase as we use more and more IoT technologies. The regulatory agencies will need to maintain the necessary capacity to handle the challenges of balancing benefits and harms in the area of personal data.

Good regulatory framework is expected to anticipate and respond to new challenges posed by the emerging technologies quickly and effectively while balancing the consideration of potential benefits and harms. TCRA carefully and systematically considers the impact of emerging technologies in strategic and operational planning in order to develop a flexible and proportionate model for regulation in domains affected by these emerging technologies such as the IoT.

E. Network security and resilience

As the IoT plays a larger part in people's daily lives, secure and reliable networks and data storage will become increasingly important. With this in mind, the Authority is investigating how existing activities on security and resilience of the communications networks can include the IoT.

Given the increasing number of objects or "things" that can connect to each other, the complexity of IoT network is presenting a great concern both for the future internet's security and reliable operation [7]. There is a need to put in place a roadmap for security design and internet of things scalability [7].

F. Numbering and Network Addressing

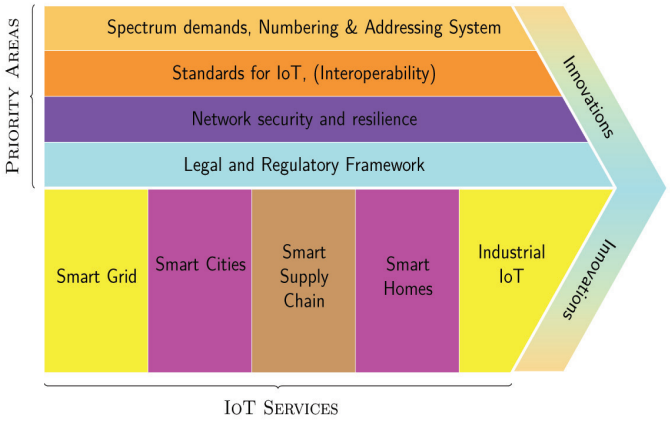
IoT services will likely use addressing systems or addresses based on the Internet standard known as IPv6, the latest version of the Internet Protocol which is able to support connections between a significantly greater number of devices. To support this, Authority monitors the progress already being made by internet service providers in supporting IPv6 connectivity.

III. IoT Enabling Protocols and Application

IoT extends internet connectivity ahead of traditional devices like desktops and laptops, smart-phones and a range of various devices [2]. This calls for development of IoT enabling protocols and applications to ensure IoT devices communicate and

interrelate with the external environment through the internet. It will involve establishment of technical details pertaining to the IoT enabling technologies, protocols and applications; taking into consideration that the objective of the IoT is to support "ubiquity" that enables things to be connected anytime, anywhere, with anything and anyone ideally using any path/network and any service.

In addition, exploring the relation between the IoT and other emerging technologies such as big data analytics and cloud computing is essential as there is a need for better integration among IoT services [3], [8].



Connectivity is the foundation for IoT and the type of access required will depend on the nature of the application. Currently, there are two alternative connectivity tracks for the many IoT applications that depend on wide-area coverage: Cellular technologies: 3GPP technologies like GSM, WCDMA, LTE and future 5G. These wide area networks (WANs) operate on licensed spectrum and historically have primarily targeted high-quality mobile voice and data services. The new radio access technology, narrowband IoT (NB-IoT) has been specifically tailored to form an attractive solution for emerging low power wide area (LPWA) applications.

IV. IoT Connectivity

Unlicensed LPWA: new proprietary radio technologies have been developed and designed solely for machine-type communication (MTC) applications addressing the ultra-low-end sensor segment, with very limited demands on throughput, reliability or QoS. Many IoT devices will be served by radio technologies that operate on unlicensed spectrum and that are designed for short-range connectivity with limited QoS and security requirements typically applicable for a home or indoor environment.

It should be noted that each of the technologies available for IoT connectivity has its own advantages and disadvantages. However, the range of IoT connectivity requirements, both technical and commercial, means cellular technologies can provide clear benefits across a wide variety of applications. In terms of coverage, cellular networks already cover a substantial area of the country.

V. Conclusion

The IoT application domains span almost all major economic sectors: health, education, agriculture, transport and transportation, manufacturing, electric grids, and many more. The IoT has the potential to bring substantial social and economic benefit through the creation of new jobs, an increase in productivity and competitiveness and improvements in service delivery. However, the IoT will place different demands on communication infrastructure and services. Underlying these developments will be policies that promote the availability, quality and use of such infrastructure and services. In this regard, it is required for regulatory agencies to ensure the performance and security of communication networks and services as a contribution towards building trust in the IoT. Likewise, there is a need to put in place good practices to help regulatory agencies move ahead and promote the positive elements of the IoT while minimizing challenges and ensuring broader goals.

References

[1] S. Singh and N. Singh, "Internet of things (iot): Security challenges, business opportunities reference architecture for e-commerce," in Proc. Int Green Computing and Internet of Things (ICGCIoT) Conf, Oct. 2015, pp. 1577–1581.

[2] A. W. Burange and H. D. Misalkar, "Review of internet of things in development of smart cities with data management amp; privacy," in Proc. Int Computer Engineering and Applications (ICACEA) Conf. Advances in, Mar. 2015, pp. 189–195.

[3] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari, and M. Ayyash, "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[4] J. Rui and S. Danpeng, "Architecture design of the internet of things based on cloud computing," in Proc. Seventh Int. Conf. Measuring Technology and Mechatronics Automation, Jun. 2015, pp. 206–209.

[5] M. H. Asghar, A. Negi, and N. Mohammadzadeh, "Principle application and vision in internet of things (iot)," in Proc. Int Computing, Communication Automation (ICCCA) Conf, May 2015, pp. 427–431.

[6] C. Tian, X. Chen, D. Guo, J. Sun, L. Liu, and J. Hong, "Analysis and design of security in internet of things," in Proc. 8th Int. Conf. Biomedical Engineering and Informatics (BMEI), Oct. 2015, pp. 678–684.

[7] A. M. Gamundani, "An impact review on internet of things attacks," in Proc. Int Emerging Trends in Networks and Computer Communications (ETNCC) Conf, May 2015, pp. 114–118.

[8] R. Kirichek, A. Vladyko, M. Zakharov, and A. Koucheryavy, "Model networks for internet of things and sdn," in Proc. 18th Int. Conf. Advanced Communication Technology (ICACT), Jan. 2016, pp. 76–79.

The Impact of Emerging Technologies on Security, Privacy and Trust

Eng. James M. Kilaba, Emmanuel C. Manasseh
Tanzania Communications Regulatory Authority
P.O. BOX 474, Dar es Salaam, Tanzania
E-mail: kilaba@tcra.go.tz, emmanuel.manasseh@tcra.go.tz

ABSTRACT —Emerging technologies have changed the way we live our lives as they shape our homes, businesses, and governments. Applications enabled by emerging technologies range from e-government, e-commerce, environmental monitoring and control, health monitoring, vehicle fleet monitoring, industrial monitoring and control, to home automation. Despite these appealing benefits, there is the potential for significant challenges too. With regards to emerging technologies, breaches of security and privacy have the significant potential for causing harm. Thus, striking the right balance between these technologies and security issues together with the respect for privacy remains an ongoing and pressing challenge.

This article identifies areas for attention that are likely to be important in facilitating emerging technologies. Considered priority areas include regulatory settings, network security and integrity, data privacy and trust.

I. INTRODUCTION

Emerging technologies will improve existing and enable new economic processes such as tracking and managing the inventories of goods, delivering parcels, supporting e-commerce activities (online shopping), optimizing supply chains and manufacturing, creating smart environments for assisted living, personalized healthcare, and so on [1], [2]. Indeed, networks and data that flow from emerging technologies will support an extraordinary range of applications and economic opportunities [3].

The fundamental attribute of emerging technologies is that they benefit from multidisciplinary stances motivated by growing convergence of various fields, which has enabled them to be studied and developed together [4], [5]. However, with the extensive applications of emerging technologies in many fields, they are confronted by various issues related to security and privacy protection [6]. For the envisaged benefits to be yielded from these emerging technologies there are some issues to be addressed.

Emerging technologies are closely connected with people, therefore security and privacy are major issues [7]. In addition, users are more concerned about the trust, especially trust in services dealing with personal sensitive data. Thus, managing these technologies along with establishing effective countermeasures against trust, security and privacy concerns of individual citizens as well as service providers and government agencies is essential for their adoption [3]. This calls for the use of secure and privacy-preserving services in order to ensure the integrity of data without any unwarranted exposure [8]. Likewise, trustworthiness requirements must be assured in order to meet users' trust concerns.

The privacy issues related to emerging technologies include security vulnerabilities, which threaten the privacy of users together with the use of technologies for unlawful surveillance [5]. Security vulnerabilities may include weak authentication, insufficient encryption and insecure firmware. To counter security vulnerabilities, it is advised to think about security from the beginning of the conception at both software and hardware levels [9]. The use of emerging technologies for unlawful surveillance may include using crowdsensing by thieves to find out when a victim is not at home. The term "crowdsensing" refers to sharing data collected by sensing devices with the aim to measure the phenomena of common interest [7].

Notwithstanding the negative impact of these emerging technologies, their diffusion is inevitable in today's interdependent world. This unavoidable diffusion of emerging technologies has added to concerns about the possibility of technologies reaching irresponsible hands.

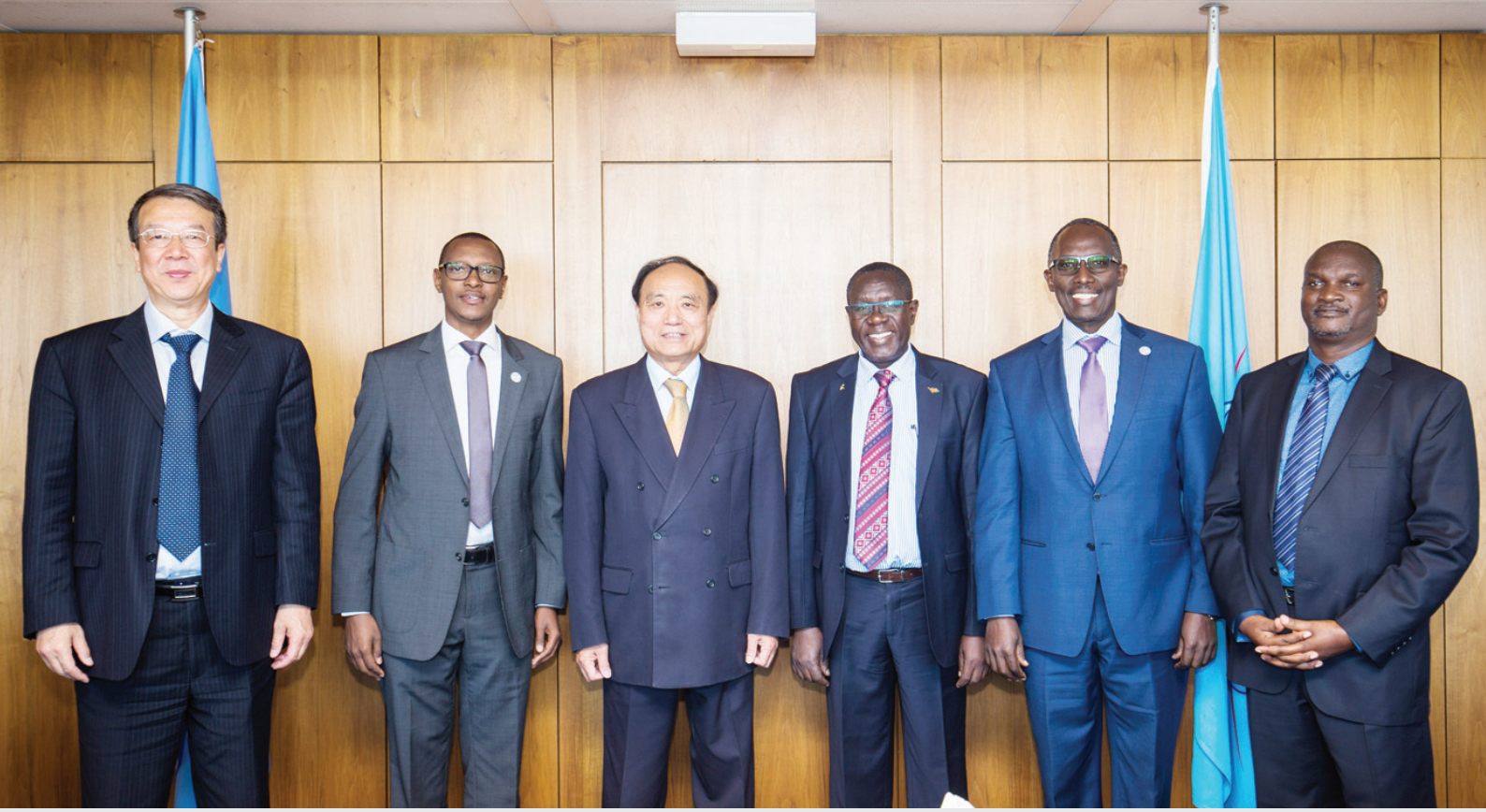
The challenge of securing the entire cyberspace is too large for any organization or country [10], [11]. It is very crucial to ensure that there is a sustained and close collaboration between government and other stakeholders at all levels. National Computer Security Incident Response Team (CSIRT), also known as Computer Emergence Response Team (CERT) plays a crucial role in coordinating, facilitating, encouraging and supporting such participation [10], [11].

In addition, realising the potential benefits from these emerging technologies depend upon appropriate regulatory settings. The focus of this article is on exploring the impact of emerging technologies on security, privacy and trust. Specific threats that emerging technologies and innovations pose for security, privacy and trust together with regulatory issues related to emerging technologies are briefly addressed.

II. CHALLENGES OF SECURITY, PRIVACY AND TRUST

Emerging technologies have raised new opportunities for the implementation of novel applications and the provision of high-quality services over global networks.

In fact, the use of technology, in this information society era have improved the quality of life by disseminating knowledge,



CEOs of national regulatory authorities forming the East African Communications Organization (EACO) with the Secretary General of the International Telecommunication Union (ITU), Dr. Houlin Zhao (third left), at the Union's headquarters in Geneva. From right are Eng. James M. Kilaba (Director General TCRA), Dr. Andrew Rugege (ITU Director Africa Region), Mr. Francis Wangusi (Director General Communications Authority of Kenya), Mr. Patrick Nyirishema (Director General RURA – Rwanda) and Mr. Selin Tu (ITU Secretary General's Special Coordinator).

strengthening social cohesion, and generating earnings.

Most of the emerging technologies support "Ubiquity" that enable things to be connected anytime, anywhere, with anything and anyone ideally using any path/network and any service [12]. These services are creating more opportunities but at the same time introducing new challenges in particular security and privacy concerns [13], [14]. With this in mind, it is necessary and essential to consider security and network resilience issues on design and implementation of emerging technologies.

A. Security Issues

Commercialization of emerging technologies has led to public security concerns, including threat of cyber attacks and organized crime [14]. Security threats have been a major concern because security measures that work well on the conventional approaches, do not necessarily adapt well to the emerging technologies [15].

The security vulnerabilities of emerging technologies include security loopholes and security vulnerabilities caused by pre-installed malware. The security loopholes of emerging technologies are programming or other flaws which allow a hacker to reduce information assurance.

For instance, a weak password may allow the hacker to penetrate by using a dictionary attack, i.e., a technique for defeating the authentication system of a computer system by using a large number of passwords [5]. Other security loopholes include software bugs, lack of security awareness, and weak or non-existent antivirus programs [5], [16].

Social networking can be used by criminals to receive unauthorized access to personal information. For instance, a criminal may create a fake profile in Facebook and send a 'friend request' to a victim. By accepting the 'friend request', the victim will allow the criminal to access a tremendous amount of personal information about the victim (e.g., personal data, photos, videos, and location information). In addition, beacons (i.e., tiny wireless transmitters that constantly send radio signals) can be used by criminals to track the location of the users of mobile smart devices. For example, a criminal may install on victims' computers malware which collect location information from beacons and send the collected location information to the criminal [5].

B. Privacy Issues

Human beings value their privacy and the protection of their personal sphere of life. They value some control over who knows what about them. They certainly do not want their personal information to be accessible to just anyone at any time. However, emerging technologies threaten privacy and have reduced the amount of control over personal data and open up the possibility for a range of negative consequences as a result of access to personal data [5].

Emerging technologies pose challenges in the sensitive area of personal identity and privacy. The scale of personal information collected using these technologies is huge, rendering the potential intrusion of privacy a more critical and acute concern.

The Impact of Emerging Technologies on Security, Privacy and Trust

These concerns pertain to the confidentiality of accumulated consumer data and the potential risks that consumers experience over the possible breach of confidentiality [5], [16].

The combination of increasing power of new technology and the declining clarity and agreement on privacy give rise to problems concerning law, policy and ethics.

C. Legal and Regulatory Framework

Emerging technologies are likely to create new regulatory challenges. New questions of liability and protections for citizens and businesses will inevitably arise.

Resolving these questions will be a critical factor to enable the introduction of more radical opportunities and may pose novel regulatory and governance challenges [5], [16].

There is a need for regulatory agencies to develop a flexible and proportionate model for regulation in domains affected by the emerging technologies, to respond quickly and effectively to technological change, and balance the consideration of potential benefits and harms [5].

Most of the emerging technologies are associated with the cyberspace. A key regulatory challenge for dealing with cyberspace stems from the fact that the Internet simultaneously means infrastructure, information technology, services, and media entity – all of which are intertwined in complex and ever-evolving ways [16].

III. COUNTERMEASURES

To address privacy and security threats effective mechanism are required to ensure integrity, privacy, availability, authentication, computability, identification and accuracy [15]. It is a best practice to consider that privacy and security breaches are inevitable and as a result strategies can be planned, prepared and implemented as effectively as possible. It is also necessary to put efforts on the prevention of security threats without limiting the substantial efforts required to detection and response.

A. Security, Privacy and Trust

Assessing and comparing potential services enabled by emerging technologies poses an issue for adopters to choose security and privacy options that are sufficient and robust [16]. This calls for a need to identify a set of attributes that reflect various aspects of security and privacy in an attempt to alleviate security and privacy concerns [16].

Although emerging technologies are typically seen as the cause of security and privacy problems, there are also several ways in which technologies can help to solve these problems. There are rules, guidelines or best practices that can be used for designing privacy-preserving systems. Such possibilities range from ethically-informed design methodologies to using encryption to protect personal information from unauthorized use [5].

In line with privacy-preserving, value sensitive design can be used as a method to design privacy-friendly systems. It provides a set of rules and guidelines for designing a system with a certain value (such as privacy) in mind. Value sensitive design provides a theoretically grounded approach to the design of technology that accounts for human values in a principled and comprehensive manner throughout the design process [5].

Furthermore, industry self-regulation allows businesses to use their expertise in order to solve issues arising out of the use of new technologies. The term "industry self-regulation" can be defined as a process through which an organization monitors its own adherence to standards (including legal standards) and enforce those standards [5].

IV. CYBER SECURITY: REAL-WORLD IMPACT

Cyber security has quickly evolved from a technical discipline to a strategic concept. Strategies are required to improve a nation's cyber defense posture [10]. Since strategic challenges require strategic solutions, and the fact that cyber crime remains a top level threat to many nations, then strategies are needed to tackle it and make the world a secure place in cyberspace [11], [17].

The best strategy is not about protecting everything from every possible attack; rather it is focusing on protecting those important resources which are most likely to be attacked.

Moreover, there is a need to make organizations/governments, more resilient to cyber attack and be able to protect their interests in cyberspace. This requires national strategies that promote dissemination of cyber security knowledge and skills to various groups (government and other stakeholders) to be able to acquire necessary levels of expert needed to actively tackle serious cyber crime issues.

National Computer Security Incident Response Team (CSIRT) or Computer Emergence Response Team (CERT) is responsible for establishing a national approach to incident response and secure information sharing on threats [10], [11], [17]. When computer security incidents occur, it is necessary and essential to handle them in a timely manner [10], [17]. The speed with which governments/organizations can recognize, an-

alyze and respond to an incident will affect the damage and will lower recovery costs. Organized incident management requires defined, repeatable processes and the ability to learn from incidents that threaten the confidentiality, availability, and integrity of critical systems and data [17].

V. CONCLUSION

Emerging technologies are advancing very rapidly, converting yesterday's fiction into today's reality. They have clearly and irreversibly changed and benefited our societies and will continue to break new grounds and change our lives and societies. At this critical juncture, a powerful reminder needs to guide innovation: the concerns for privacy, security and trust. Governments, industries and academia need to work together and articulate guidelines that respect and incorporate these concerns across the wide spectrum of emerging technologies.

Furthermore, a fine balance is required in order to put in place an effective regulatory framework that offer enough protection to manage the risks associated with these technologies without stifling innovation and the potential social and economic benefits.

REFERENCES

[1] M. H. Asghar, A. Negi and N. Mohammadzadeh. "Principle application and vision in internet of things (iot)," in Proc. Int Computing, Communication Automation (ICCCA) Conf, May 2015, pp. 427–431.

[2] A. Al-Fuqaha, M. Guizani, M. Mohammadi, M. Aledhari and M. Ayyash. "Internet of things: A survey on enabling technologies, protocols, and applications," IEEE Communications Surveys Tutorials, vol. 17, no. 4, pp. 2347–2376, 2015.

[3] R. Srinivasan, A. Mohan and P. Srinivasan. "Privacy conscious architecture for improving emergency response in smart cities," in Proc. Smart City Security and Privacy Workshop (SCSP-W), Apr. 2016, pp. 1–5.

[4] S. Singh and N. Singh. "Internet of things (iot): Security challenges, business opportunities reference architecture for ecommerce," in Proc. Int Green Computing and Internet of Things (ICGCIoT) Conf, Oct. 2015, pp. 1577–1581.

[5] J. van den Hoven, M. Blaauw, W. Pieters and M. Warnier. "Privacy and information technology," in The Stanford Encyclopedia of Philosophy, spring 2016 ed., E. N. Zalta, Ed., 2016.

[6] C. Tian, X. Chen, D. Guo, J. Sun, L. Liu and J. Hong. "Analysis and design of security in internet of things," in Proc. 8th Int. Conf. Biomedical Engineering and Informatics (BMEI), Oct. 2015, pp. 678–684.

[7] G. Strazdins and H. Wang. "Open security and privacy challenges for the internet of things," in Proc. Communications and Signal Processing (ICICS) 2015 10th Int. Conf. Information, Dec. 2015, pp. 1–4.

[8] H. Kumarage, I. Khalil, A. Alabdulatif, Z. Tari and X. Yi. "Secure data analytics for cloud-integrated internet of things applications," IEEE Cloud Computing, vol. 3, no. 2, pp. 46–56, Mar. 2016.

[9] F. Bruguier, P. Benoit, L. Torres, and L. Bossuet. "Hardware security: From concept to application," in Proc. 11th European Workshop Microelectronics Education (EWME), May 2016, pp. 1–6.

[10] K. Clark, D. Stikvoort, E. Stofbergen, and E. van den Heuvel. "A dutch approach to cybersecurity through participation," IEEE Security Privacy, vol. 12, no. 5, pp. 27–34, Sep. 2014.

[11] B. Horne. "On computer security incident response teams," IEEE Security Privacy, vol. 12, no. 5, pp. 13–15, Sep. 2014.

[12] A. W. Burange and H. D. Misalkar. "Review of internet of things in development of smart cities with data management and privacy," in Proc. Int Computer Engineering and Applications (ICACEA) Conf. Advances in, Mar. 2015, pp. 189–195.

[13] A. Ouaddah, I. Bouij-Pasquier, A. A. Elkalam, and A. A. Ouahman. "Security analysis and proposal of new access control model in the internet of things," in Proc. Int Electrical and Information Technologies (ICEIT) Conf, Mar. 2015, pp. 30–35.

[14] A. M. Nia and N. K. Jha. "A comprehensive study of security of internet-of-things," IEEE Transactions on Emerging Topics in Computing, vol. PP, no. 99, p. 1, 2016.

[15] S. Mewada, P. Sharma, and S. S. Gautam. "Exploration of efficient symmetric AES algorithm," in Proc. Symp. Colossal Data Analysis and Networking (CDAN), Mar. 2016, pp. 1–5.

[16] A. Abuhussein, F. Alsubaei, S. Shiva, and F. T. Sheldon. "Evaluating security and privacy in cloud services," in Proc. IEEE 40th Annual Computer Software and Applications Conf. (COMPSAC), vol. 1, Jun. 2016, pp. 683–686.

[17] R. Ruefle, A. Dorofee, D. Mundie, A. D. Householder, M. Murray, and S. J. Perl. "Computer security incident response team development and evolution," IEEE Security Privacy, vol. 12, no. 5, pp. 16–26, Sep. 2014.

Hacking: War in the Cyberspace

Dr. Frank P. Seth, (DSc. Technology – Software Engineering - LUT),
Dar es Salaam University College of Education (DUCE),
IT Department,
P. O. Box 2329, Dar es Salaam.
f.p.seth@gmail.com

The Problem

WHILE hacking is considered a criminal activity and hackers as evil, hacking has nowadays evolved yet into a higher order and has become a state-sponsored drudgery. Hacking has evolved from individualized or company based hacking, which aimed at bullying people, disruption of business operations, stealing information, financial gains through theft, into a state-to-state hacking that is motivated by political reasons (RT, 2013a). Some states endeavor to penetrate other state's affairs (RT, 2013a) for whatsoever reasons, and this trend is rapidly increasing.

In the ubiquitous computing and the Internet of Things (IoT) era we live in, hacking is increasingly difficult to mitigate. For example, various app-stores are populated with several millions of apps every year. Most of the apps are free, attractive, useful, easily accessible and directly downloadable to handheld devices and computer systems. Some of the apps are capable to open back-doors for hackers to attack the systems. On the other hand, emails have never been all safe as it used to be in the past. Many attacks have been achieved though mailing systems, extending the threat immeasurably (Aljazeera, 2017).

In practice, we cannot avoid using emails or restrict mobile devices to all citizens. This means, hackers have a wide ground for mobilizing their attacks globally using the legitimate 'can't-do-without' infrastructures such as Internet, mailing systems, mobile devices, computers systems, etc. This is a global threat.

Little by little the war fought between nations has shifted from physical artilleries to technological deadly soft weaponries by the name of software, enhanced by the ever-increasing power of networking. Internet is irrefutably important; without it life is difficult. However, the Internet has become like a sick heart that you can't remove unless you are committing suicide. In this regard, the Internet has been and is the vehicle that facilitates all the evil attempts in the cyber world; yet we cannot afford to shut it down.

The Questions

Having a glance at the problem stated above, what should a country do to cope with the changing cyber milieu? I put forward a few questions for pondering and further investigation:

i. As a country, are we prepared to fight in the cyberspace?
ii. If not fighting, do we have machinery and capability to protect our internal affairs?
iii. The military work has never been a part time job. As a country, do we have a full time cyber brigade?

The Rationale

The article aims at raising awareness on the security issues as far as the cyber environment is concerned. National security has never been exclusively a government or a particular institution's responsibility; it is rather a collective one. The more people are security-minded the safer we are as whole. However, every nation has a key strategic responsibility to protect its people, resources, critical infrastructures and physical borders, to mention a few. In the era of technology, the cyberspace is the new realm that requires strategic attention.

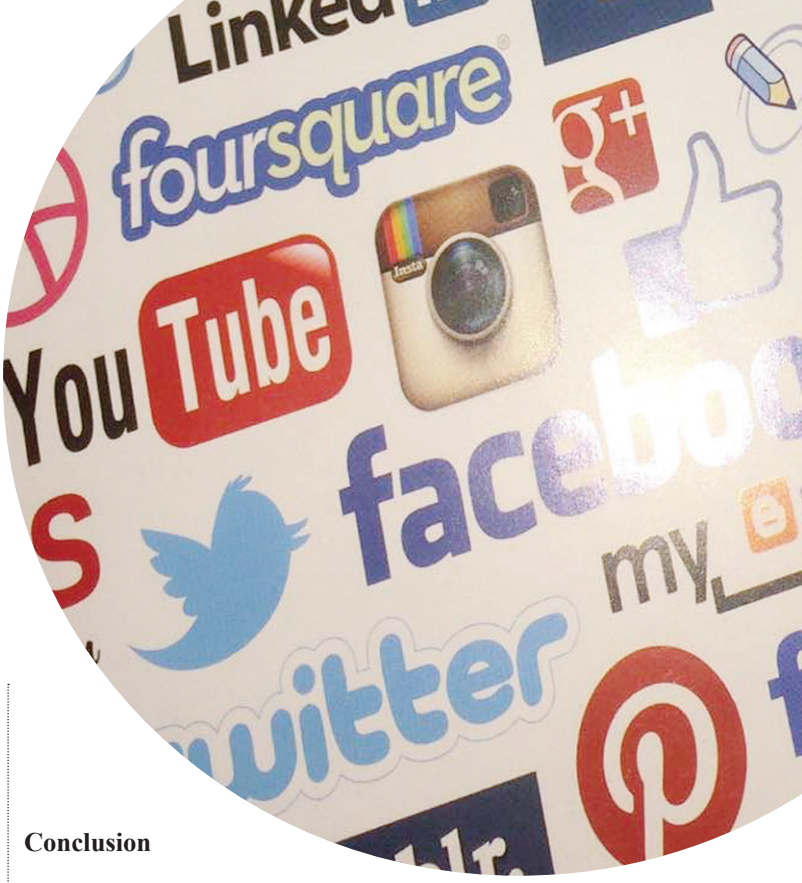
The Modern War: Cyber in the Equation

"It is change, continuing change, inevitable change, that is the dominant factor in society today. No sensible decision can be made any longer without taking into account not only the world as it is, but the world as it will be. . . . This, in turn, means that our statesmen, our businessmen, our everyman must take on a science fictional way of thinking." —Isaac Asimov.

In the 2015, the USA Director of National Intelligence named cyber threats as the number one strategic issue facing the United States (Hughes & Colarik, 2016). If cyber security is a concern to the USA with its level of sophistication in technology, I bet it may be a more bugling issue in the third world countries. Although we have different enemies as nations, we cannot take cyber security issues for granted because no nation is immune from such attacks.

In the early 2017, it came into public attention that Russians may have interfered with the USA presidential elections (BBC, 2017a). France Defense Minister, Jean-Yves Le Drian revealed that France was the subject of 24,000 cyber-attacks against its defense targets in the year 2016 alone. The Minister said such attacks were doubling every year and the 2017 presidential elections may be targeted (BBC, 2017b). Furthermore, Mr. Le Drian said cyber attacks in France have increased substantially in the last three years and have become a serious threat to the country's infrastructure (BBC, 2017b).

The former U.S. Vice President Joe Biden warned France, Germany and the Netherlands before their elections that Moscow may try to sway the results (Petroff, 2017). However, the



voting infrastructure for Germany, France and Netherlands is expected to be relatively secure since all three countries use paper ballots (Petroff, 2017). Mr. Biden tried to point out that the decision of who is going to be the leader of a country might be decided by another country or a small group of people through some computer technology.

Germany, France and the Netherlands, which in the 2015 recorded populations of 81.68 million, 66.54 million and 16.94 million respectively (World Bank, 2017) and are all well advanced in technology, are still on paper ballots! This shows the criticality of the matters with regards to threats in the cyberspace.

The Strategy

In the course of addressing the new trend of cyber attacks, where the political arena is invaded, I tried to figure out the Tanzanian scenario and put forward the three questions above: As a nation, are we prepared to fight in the cyberspace?; If not fighting, do we have machinery and capability to protect our internal affairs?; and since military work has never been a part time job, as a county, do we have a full time cyber brigade?

From a citizen's standpoint, all these questions are difficult. However, I find them important for pondering and for further research. Nonetheless, they may serve as indicators to gauge our stance on cyber war.

I had a chat with an official in the military and he said that it is customary for defense departments to put up a budget for buying or maintaining artillery and ammunition, hiring and training people for specific skills, evaluating the threats from other countries, etc. Then I remembered the National Service (JKT) training, where we were told that before confronting an enemy, there should be some sort of intelligence work to determine the enemy's capability, etc. In this regard, I asked, "in the past, people used to travel physically to gather intelligence information but in this era of science and technology where we have such things like unmanned aircraft, drones, spywares, hacking, etc. are we good?" The official stared at me and gave a short answer, "Bro, we have a long way to go." Period

The Way Forward

Anything of a strategic nature starts with a budget, framework of execution and assessment, etc. War in the cyberspace is real, and has real effects. The technology is growing rapidly and the adversaries are aggressive.

The stochastic nature of cyber attacks requires teamwork that may include cross-border experts, collaborations of government and individuals or private companies, etc. It is also possible for the state to hire an independent company from a foreign county for this work (RT, 2013b).

Conclusion

The article has, in a nutshell,
examined the cyberspace and the new trend of politically motivated hacking. The aim is to provide food for thought rather than answers. There are few questions put forward; though important, but not explicit. More research and work is needed to address cyber security issues in our context.

Reference

1. Aljazeera, (2017). "Two Russian spies indicted over massive Yahoo hack" found at http://www.aljazeera.com/news/2017/03/russian-spies-indicted-massive-yahoo-hack-170315184949612.html
2. BBC, (2017a). "Was Russia involved in the US presidential election?" found at http://www.bbc.com/news/world-us-canada-39325046
3. BBC, (2017b). "France thwarts 24,000 cyber-attacks against defence targets " found at http://www.bbc.com/news/world-europe-38546415
4. Hughes, D and Colarik, A. M., (2016). "Predicting the Proliferation of Cyber Weapons into Small States", JFQ 83, 4th Quarter 2016 found at file:///Users/frankpseth/Desktop/Joint%20Force%20Quarterly_Vol.%2083_%204th%20Quarter%202016.pdf
5. Petroff, A., (2017). "How Europe's elections could be hacked" found at http://money.cnn.com/2017/01/25/technology/hacking-elections-europe-germany-france/
6. RT, (2013a). "Hackers-for-hire: Chinese group accused of economic espionage against US companies" found at https://www.rt.com/usa/hackers-china-hidden-lynx-092/
7. RT, (2013b). "NSA contracted French cyber-firm for hacking help" found at https://www.rt.com/usa/nsa-vupen-exploit-hack-978/
8. World Bank, 2017. "Where we Work", found at http://www.worldbank.org/

Social Media Identity Theft

By Victoria Rutakara, TCRA

IF a person pretends to be someone else to obtain goods, services or cash in the victim's name that is identity theft. Identity theft is fraud.

Identity theft can be used in many ways to achieve many things. For example, medical identity theft can be used to access services, consuming benefits that the victim has paid for. Identity theft can be used to obtain loans or take out contracts in the victim's name thereby damaging their credit record. Criminals are able to access a victim's bank accounts by obtaining details about a person to enable them to pass for the intended victim in the eyes of a bank, creditor, insurance company and so on. Criminals can also obtain your personal information through third-party applications.

Most social media sites have apps that ask for permission to access your account information before you can install them. This is one way hackers steal your details to commit fraud. Unconsciously (or sometimes, consciously), you provide personal details you would not share otherwise on your social media accounts. Information such as your full name (including your middle name), date of birth, hometown, pet names, interests and hobbies, nature of work, and home or office address are just some of the personal details you post on your profile. Criminals can easily manipulate these details to commit fraud.

This pattern of online theft and fraud is caused by a combination of factors, namely:

a) Lack of users' knowledge regarding online identity protection;
b) Growing comfort with, and trust in, social platform providers;
c) The need for social platforms to generate revenue;
d) Lack of standards or police for these platforms. Although this issue is not yet in the mainstream consciousness, it likely will be sooner rather than later.

Why social media?

A great number of people are on social media and have been registered using their confidential information. Users of social media are encouraged to provide as much information as possible during registration. Social media have been the place for generating revenue with targeted advertising, based on personal information. With limited government oversight, industry standards or incentives to educate users on security, privacy and identity protection, users are exposed to identity theft and fraud. Additionally, these platforms have tons of confidential user information, and are likely vulnerable to outside (or inside) attack.

With the increased global use of social media, there are more opportunities than ever before to steal identities or perpetrate fraud online. Many social networks may ask for driving licence, give opportunity to share videos and photos, these provides detail information about the user, their families, friends, house, hobbies and interests. Having said that social media gives the greatest potential of abuse.

The profile elements can be used to steal or misappropriate your identity:

- Full name (particularly your middle name)
- Date of birth (often required)
- Home town
- Relationship status
- School locations and graduation dates
- Pet names
- Other affiliations, interests and hobbies

Why should you care?

Users may be wondering why sharing the above information on public is a potential dangerous move. There are a variety of reasons why you should keep personal information confidential, or at least closely managed. Below are just a few examples of how this information can be used to compromise your identity:

- Phishing attempts using this information can be used to gain trust in order to obtain non-public information through online conversations.
- GPS-enabled phones sharing your location can reveal sensitive information like your home address, work address and the places you visit.
- Ninety-five percent of Facebook profiles have at least one application, many of which are not reviewed and can be used for malicious and criminal purposes.

False profiles can be used to fuel resume fraud or defamation of character.

Potential of abuse

For example users of social media may update their status posted on social media Facebook, Twitter etc., that they are out of town or away on business for a weekend. Unknowingly this may leave your family open to assaults or robbery.

Best Practices

User may still get the benefit of using social media without making themselves a target for criminals. Before you jump online and cancel all of your social media accounts, consider that there are ways to be smart about what you share and with whom you share it.

These are the best practices:

- Never, ever give out your National ID number or driver's license numbers.
- Consider unique user names and passwords for each profile.
- Vary your passwords and change them regularly.
- Don't give out your username and password to third parties (even if it helps you connect to others and build

Social Media Identity Theft

your network).
- Assuming you plan to be active in social media, minimize the use of personal information on your profiles that may be used for password verification or phishing attacks.
- Avoid listing the date of birth, hometown, home address, year of high school or college graduation, primary e-mail address.
- Only invite people to your network that you know or have met, as opposed to friends of friends and strangers.
- For password security verification questions, use a password phrase for all answers (rather than the answer to the specific question, like "What is your mother's maiden name?").
- When age-shifting to protect your real birthday, keep the date close; otherwise, you may expose yourself to age discrimination.
- Watch where you post and what you say, as it can be used against you later.
- Google yourself regularly.
- Always check your privacy settings and configure it accordingly to restrict releasing too much information to the public.

References:

1. https://www.eonetwork.org/octane-magazine/special-features/social-media-networks-facilitate-identity-theft-fraud
2. http://www.lifehack.org/articles/technology/identity-theft-through-social-networking-lessons-take-now.html
3. http://www.anvilmediainc.com/marketing-resources/articles/social-media-id-theft-article/

CALL FOR ARTICLES, CONTRIBUTIONS

The Editor invites articles and contributions in all areas of Electronic and Postal Communications for the next issue of the newsletter. Topics include, but are not limited to:

- Recent Advances in Communications Technology
- Mobile Payments and Financial Inclusion
- Enabling Communications Technologies for Smart Cities and Villages
- Audience attitudes to TV and radio
- The future of digital terrestrial TV and mobile broadband
- Quality of the regulated Communications services
- Cybersecurity and Cyber war
- Security, privacy and trust in ICTs
- Issues on Mobile and Internet services
- Consumer protection issues
- The Economy of Broadband Communications
- Capacity Building in the ICT Industry
- Big Data Analytics and Internet of Things (IoT)
- Over-The-Top Content Services and Media System
- Block chain technologies
- The Future of Television
- Consumer use of digital communications
- The importance of communications services and affordability
- The leverage of video on demand in the community
- Development of GIS and its impact on National Addressing and Postcode System
- National Addressing and Postcode System as an economic enabler

Submission of articles, contributions
Contributors are invited to submit full-length articles, including figures and possible references, font size 12, single-spacing, up to four A4 pages.

Deadlines
Paper submission: 29th June 2017 (Hard deadline)
Notification of acceptance: 8th July 2017
Final camera-ready paper due: 16th July 2017
Submit your article to: regulator.magazine@tcra.go.tz.
The Editor, Regulator Magazine, TCRA, Tanzania Communications Regulatory Authority,
Mawasiliano Towers, 20 Sam Nujoma Road, P. O. Box 474,
14414 Dar es Salaam.

For more information and clarifications please contact the Editor on: regulator.magazine@tcra.go.tz

The Communication Sector's Potential for Youth Employment

By Semu Mwakyanjala

TACKLING unemployment needs concerted efforts by stakeholders in the communication sector, taking advantage of the Tanzania Communications Regulatory Authority (TCRA's) motto of "Creating A Level Playing Field"

The TCRA Director General Eng. James M. Kilaba told scholars from higher learning institutions during workshop on employment opportunities held in Mwanza recently that exchange of ideas and sharing of experiences provides one of the best platforms for discussing abundant opportunities associated with challenges in tackling youth unemployment in Tanzania. The forum provided an opportunity to review past, present and project on future challenges for unemployed youth in the country, he said.

Unemployment occurs when learned and skilled people actively seeking job opportunities go without work. The well-known definition of unemployment by the International Labour Organization (ILO) is "People above a specified age who, during the reference period, are without work, currently available for work, and seeking work."

By this definition, the unemployed usually account for a small percentage of the working-age population, especially in countries with informal sectors or a large rural population. Underemployment refers to an employment situation that is insufficient for the worker, relative to a standard.

Eng. Kilaba said that empowering young Tanzanians to live their dreams is the way to achieve Africa's potential. The dynamism of young Tanzanians will spearhead the economic and social transformation across Tanzania, he added.

"Our country faces demographic challenges as the population of young people increases and access to secure jobs continues to be problematic. Beyond economic costs, high rates of youth unemployment and underemployment have social ramifications. Some youth with few job prospects and little hope of future advancement may see no alternative and may consequently be lured into engaging in criminal acts", he stated.

High rates of youth unemployment represent both widespread personal misfortune for individuals and a lost opportunity for critical national and global economic development. It has been shown to have lifelong effects on income and employment stability, because affected young people start out with weaker early-career credentials, and show lower confidence and resilience in dealing with labour force challenges.

Tanzania's demographic trends show a population structure that is eminently young. Long-term population changes and long-lasting economic stagnation have in turn resulted in a large informal sector and strong pressures on the labour market in the form of youth unemployment.

High youth unemployment is a problem affecting many developed and developing economies. Young people represent, by far, the bulk of unemployed Tanzanians.

Relatively few of the young people joining the labour market can find a job in the formal sector, and many cannot readily find an adequate occupation in the informal sector.

Most youth in Tanzania have tried to seek better opportunities in urban areas, but too often find themselves stuck in slums with little or no way to earn a survival salary. Many of them end up being paid as thugs by suspected criminal leaders or joining militias – not because of an ideological compatibility, but because they need to eat for their survival. Criminal enterprises also recruit hopeless youth from this pool of unemployed. This large, desperate and restive population poses a great danger for many African countries.

Youth are three times more likely to be unemployed than their elders, so there are veritable armies of unemployed youth eager to make a living doing whatever they have to do to survive. An increasing number of unemployed youth are college graduates.

The TCRA DG observed that employment opportunities had cropped up from the exponential growth of the Communication sector in the past few years. The developments in the sector offer many opportunities for employment and entrepreneurships. Applications, retail, support and value added services have many areas which need to be explored for self-employment. Another area is e-waste management. Hundreds of youths have now secured employment due to the abundant employment opportunities available in the country's communication sector.

There are 140 radio stations, employing hundreds of youths who would have otherwise been jobless. Several others have been employed in 38 TV Stations.3. Mobile phone companies have similarly transformed the mode of communication and upgraded people's living standards with multiple value added services that enhance employment opportunities.

"The increase in the number of players in the sector has increased competition, which has led to technological, product and service innovations, increased customer choice in terms of services, products and suppliers and increased availability and access to communications products and services", he noted.

He stated that developments in the sector offer many opportunities for employment and entrepreneurships and there was need to acquire necessary skills for employment and self-employment. Young people should be encouraged to take vocational skills.

Stakeholders should explore employment opportunities available in the communication sector, share experiences and find effective and sustainable solutions to the problem. They should explore these opportunities, taking advantage of the Tanzania Communications Regulatory Authority's motto of "Creating A Level Playing Field".

The Education curriculum could be revised to incorporate skills and enterprise development. A special programme could also be designed for low skilled youth in vocational centers. Incentives should be provided to small and medium scale enterprises (SMEs) that promote student internships.

The youth are an asset for families and nations as a whole. Youth in this nation are dynamic, vibrant, resilient and entrepreneurial. The African youth population is projected to expand rapidly, surpassing that of any other continent in the world in the coming few decades.

Once empowered, the expanding youth population will be Africa's strength in the global economy.

TCRA Chairman Dr Jones Kilimbe welcoming the Minister for Works, Transport and Communications, Professor Makame Mbarawa on arrival at TCRA headquarters, Mawasiliano Towers for the the launching of the mobile number portability service. Left is TCRA DG, Eng James Kilaba. (photo by Semu Mwakyanjala)

Stakeholders who participated in the launching of the mobile number portability service.

The Minister for Information, Culture, Sports and Youth, Dr. Harrison Mwakyembe (centre) with the Chairperson of the TCRA Content Committee, Ms. Valerie Msoka (second right) and (from left) Committee members; Mr. Joseph Mapunda. Mr. Abdul Ngarawa and Mr. Derek Murusuri.

ISO 9001:2008 CERTIFIED

TZ-CERT

TANZANIA COMPUTER EMERGENCY RESPONSE TEAM

TANZANIA COMPUTER EMERGENCY RESPONSE TEAM (TZ-CERT)

INCIDENT REPORTING

TZ-CERT addresses all types of computer security incidents, which occur at its constituency. TZ-CERT may act upon requests of one of its constituents or may act if one of its constituents is involved in a computer security incidents.

The level of support given by TZ-CERT will vary depending on the type and severity of the incidents or issue, the size of the user community affected and the TZ-CERT's resources at the time which occurs at its constituency.

Users and System Administrators can report computer security incidents and vulnerabilities to TZ-CERT.

If you encounter any of the violations given below, you may contact TZ-CERT for technical assistance:-

- Attempts (either failed or successful) to gain unauthorised access to your system or data therein
- Disruption or Denial of Service
- Unauthorised use to a system for the processing or storage of data
- Changes to system hardware, firmware, or software characteristics without owner's knowledge, instruction, or constent
- Email-related security issues, spamming, mail bombing, mining, etc
- Attempts for Identity theft such as phishing
- Unauthorised modification of website content, defacement, injection of Malicious link etc

Users of different systems working on various platforms and using different applications may report any vulnerability found in these systems, platforms, applications, services and devices to TZ-CERT. An incident can be reported to TZ-CERT as follows:

- **Website**

The incident can be reported by filling in the incident reporting form on our website (www.tzcert.go.tz) and fill in as many fields as possible to enable TZ-CERT to assess the severity and nature of the incident and assist in recovery, as needed.

- **Electronic Mail**

The TZ-CERT email address for reporting incidents is: ***incidents@tzcert.go.tz***

For all other inquiries and correspondence, write to: ***info@tzcert.go.tz***

- **Telephone**

Occasionally, a compromised system's electronic mail may be under surveillance by the intruder. If that is suspected, you are advised to use a telephone to file your report.

You can contact the TZ-CERT Team on numbers:

Tel: +255 22 2412 039 / +255 22 2199 760-9

Fax: +255 22 2412 038