Global Scientific JOURNALS

GSJ: Volume 9, Issue 8, August 2021, Online: ISSN 2320-9186
www.globalscientificjournal.com

East African Countries in World of Technology Gap in the Context of Cyber Threat

IHIMBAZWE Paul

Current masters student in Faculty of computing and information Science,

University of Lay Adventists Kigali

Abstract

In general many of the African countries has improved their well-being in most past five years and this countries have enjoyed growth in income per person of more than 5% a year since 2007, there might be Claire understanding the impact of the technology in this development as the industrial firms which import, master uses and improve technology to enable effective technology strategies. Since 2015, due to different government website are created with existing template instead of creating their own from scratch , security expert have forecasted government and online commercial services as the next frontier for illegal activity in Africa.

Section III of UA about convention on cyber security and personal data protection shows that the supplier of goods shall allow his/her clients to make payments using electronic payment methods approved by the state according to the regulations in force in each state party [5], with starting (creating) the website from existing template will impact negatively to the security with this online payment.

The main objective of this paper is to identify the gap found in technology in the context of cyber threat for EAC by identifying the main groups and actors countering cyber-attacks as this threats might hinder the development of this countries.

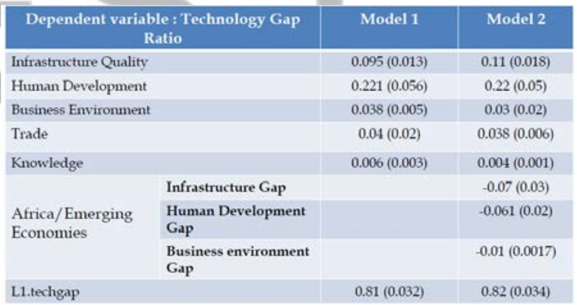
Keywords: EAC (East Africa Country), Cyber threats & Cyber security, UA, Cyber Gap, Cyber-attack.

1. Introduction

Cyber security involves protection of computer system from damage, theft or manipulation to the hardware, software, or the data contained on them [8]. To understand just how technology becomes vulnerable to cybercrime, it helps to first understand the nature of threats and how the exploit technological systems [9] more than 500,000 attacks against fortune every minute. A cyber or cyber security threat means a malicious act that seeks to damage data, steal data, or disrupt digital life in general. Cyber threats include computer viruses, data breaches, denial of service attacks and other attack vectors [10]. Globally the development of the African counties focuses on the Investment and savings, External financing and debt, internal trade majors [11], hence the developed countries invest too much in technology as the future world will relay on the advanced technology. Also member of EAC such Rwanda, Tanzania, Burundi, Kenya and south Sudan that cover a land area of 1.82 million square kilometers (km^2) and it is home to 149.7 million people[7] in the way toward their development need to invest in technology too.

One of the EAC target is to accelerate economic growth and reducing widespread poverty, to achieve this social development and improvements in the welfare of its citizen need to be considered, trade performance sets the limit to which investments and growth can be expanded without encountering balance of payments and debit repayment problem [6]. Enhancing the extend of trade scope to overcome poverty, technology will come into play , within internet technology many professional service like medical, accounting, education, legal will become tradable across this countries. With this technology the code of conduct that means set of rules formulated by the processing official with a view to establish the correct use of computer resources, networks and the electronic communication of the structure concerned and approved by the protection authority[5] need to be taken into account. Hence ICT has become the way of criminals, where posing incalculable threats to the world through cyber criminality [8].

A couple of factors can be examined to define EAC technology cyber gap, like Knowledge Infrastructures quality, Human development, Trade, Business environment, and emerging economies[2]. Each of the stated above factors will be discussed to prove how EAC member are target to cyber threat that might affect the development of their countries.



Dependent variable : Technology Gap Ratio		Model 1	Model 2
Infrastructure Quality		0.095 (0.013)	0.11 (0.018)
Human Development		0.221 (0.056)	0.22 (0.05)
Business Environment		0.038 (0.005)	0.03 (0.02)
Trade		0.04 (0.02)	0.038 (0.006)
Knowledge		0.006 (0.003)	0.004 (0.001)
Africa/Emerging Economies	**Infrastructure Gap**		-0.07 (0.03)
	Human Development Gap		-0.061 (0.02)
	Business environment Gap		-0.01 (0.0017)
L1.techgap		0.81 (0.032)	0.82 (0.034)

a. ICT Infrastructure quality

As discussed above, African need to adjust the ICT infrastructure to meet the stated objectives, Threats spread easily because many servers and computers are not properly protected [13] and African is vulnerable to different online criminal activities such as drugs & Human trafficking, financial fraud and terrorism as well, and for example US$245 million have been lobed from Tanzania, Zambia, Uganda, Rwanda and Kenya to cyber fraud.

b. Business environment

By the year of 2015 in banking sector, mobile financing threats become one of the top main malware programmes aimed at money theft in Africa [1], access to the internet is also growing too fast in EAC as 206,534,800 users subscribed to Facebook with 496,039,381 people access to the internet [12] and this media remains a preferred target for scammers, falsified link and fishing are used [1].

Over 400 companies business targeted on a daily basis and their business email compromise scams was successful in African

2. Methods

This paper interrogate the EAC technology gap in the context of cyber threats. The research judge the critical factors that create opportunities for cyber threat in EAC.

2.1 EAC technology gap in the context of cyber threats

The result have been showed that many email user account click on links in emails from strangers even when they are aware of the risky. Every one need to have basic understanding of cyber threat because cyber threats is not all about technological defenses instead, it's all about people, from home user through industry to government contrary this is not what is done in EAC where information security is a duty of ITs only, much effort is channeled to small number of people who are doing ICT and related field.

2.2 Critical factors that create opportunities for cyber threat in EAC

Existing of week infrastructures to fight cybercrime, in the world of today data (information) is new gold, if you do not safe guard it, you are likely to lose everything that you own from the money in your bank, votes during presidential voting, new business idea stored in your machine (computer), new formula stored in your system, and etc.. Though computers were created for good but bad guys are inventing every day, now computer has become also target to them. Here down is a table showing how internet servers are secured per 1 million people. We compare EAC member with some of western countries.

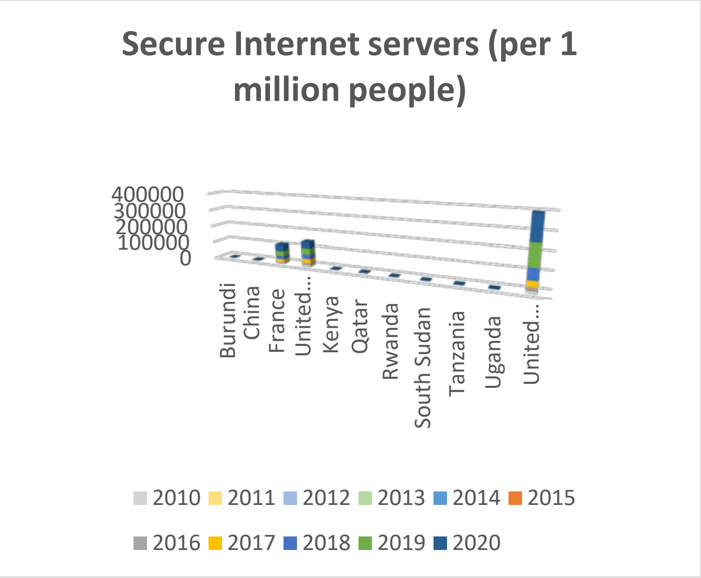


Figure 1: Secure internet server per 1 million, comparison is made between EAC with other developed countries

When you look at the country rank and value in the ICT development index for EAC comparing with some western country (USA, United Kingdom, china, France, and Qatar) have been used as example in this paper.

It is clear understanding that the EAC still have a long journey to go for covering this gap in technology in terms of infrastructure.

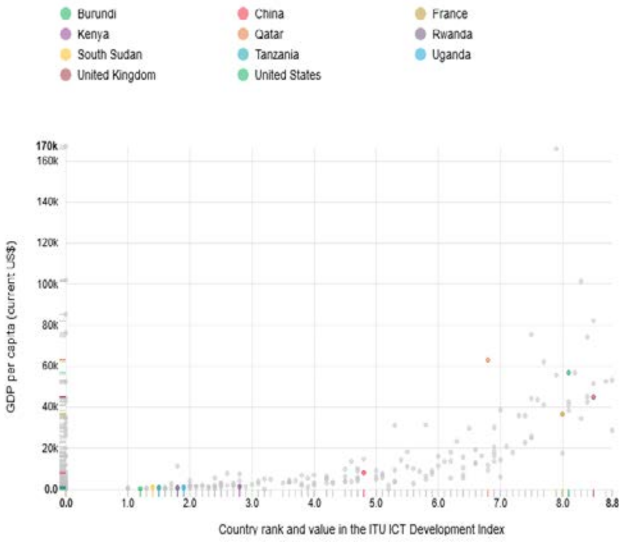


Figure 2: Country Rank and value in ITU ICT development index, index (--100))

Digital infrastructure as all elements that capable of providing support for urban management like fiber cable, IoT object etc…The internet play huge role, let look at individual (%) using internet in EAC comparing with other developed countries

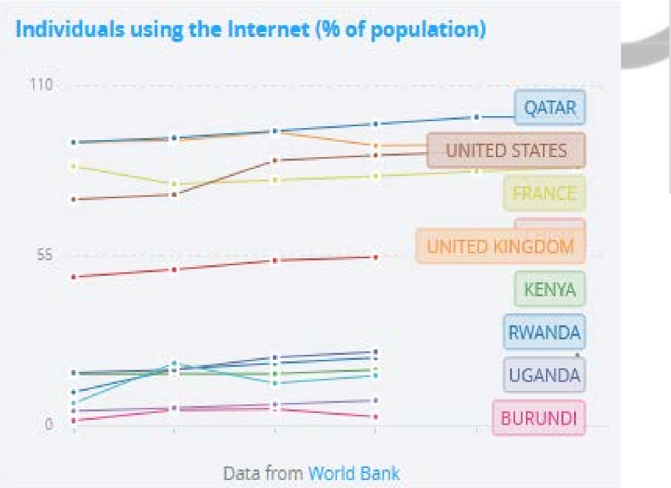


Figure 3: Individual using the internet (% of population) comparison for EAC with developed countries

Lack of expert in Information security and related field, many of students who got scholarship to study abroad remain there and find & get job from those countries especial in western countries where technology is advanced and salary is high too, this make those countries to keep maintaining stability of their technology security comparing to the rest countries, also comparing the monthly salary of computer experts from EAC each member's GDP is too expensive to higher the experts from outside. Here down is an example where comparison of the monthly salary of a system administrator salary and Information security analyst change by experience were made from EAC members to some of the western country.

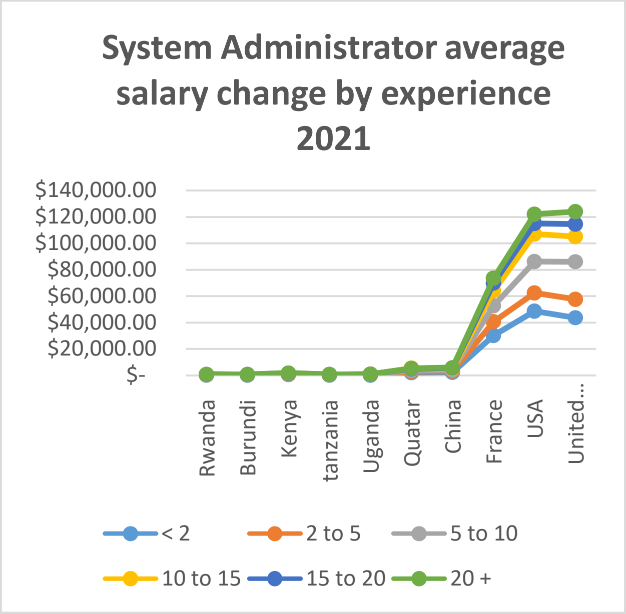


Figure 4: System Administrator average salary change per month

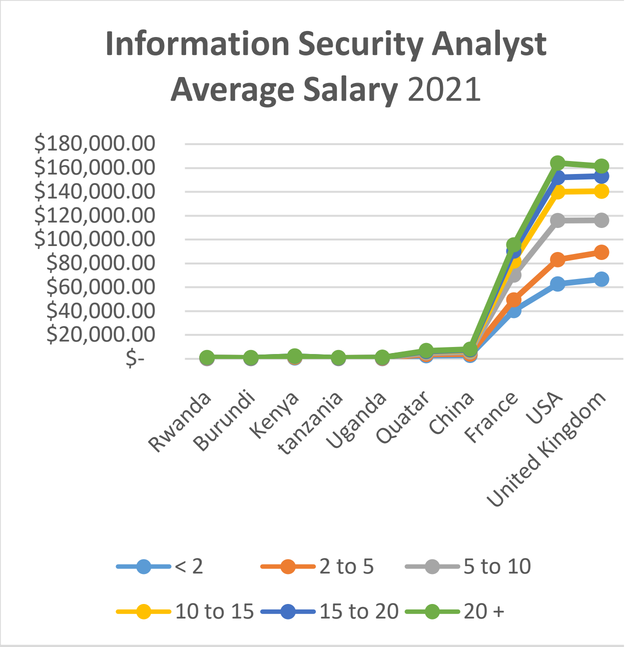


Figure 5: Information Security Analyst average salary change per month

3. Conclusion

Everything start with education with stable politics the East African Country need to invest too much in education where strong Computer Technology and Information Technology institutions need to train more expert in cyber security with a strong expertise in information security field such Security audit, system administration, forensic investigation, software development and information security analyst as well to enable EAC member to overcome technology gap where they will be able to fight with the future challenges of cybercrime.

Advanced technological infrastructure is another strong side to be viewed, technology can be said that it is in its maturity state as new technology borne every single day, for new tech to be compatible with the existing infrastructure sometimes is impossible, for example, recently whatsApp company announce that for android, devices include HTC desire, LG Optimus Black, Motorola Droid Razr and Samsung galaxy S2 will lose whatsapp support by end of 2020[14].With new trend of 5G new infrastructure will be built to be compatible with this internet generation. EAC need to build (have) the quality infrastructure to unable them fight against any cybercrime.

References

[1]Toulu, A (September 2018) Cyber threat on African subjects.

[2]Gouranga, D & Imed, D How far is African from the world technology frontier? Closing the south-south Technology Gap.

[3] UNCTAD, (July 2003) Africa's technology Gap.

[4] Samson, G (December 2020) Dynamics of technology gap between OECD and African countries: A structure estimation.

[5] AU, constitutive Act of the African (2000) African union convention on cyber security and personal data protection

[6] T.W Oshikoya & M. Nureldin, Information technology and the challenge of economic development in Africa.

[7] A.J Mwiburi, (2018) Preventing and Combating Cybercrime in East African. Lessons from Europe's Cybercrime Frameworks.

[8] Hood S. Mukiibi (November, 2019) Cyber security in African: The boring technology story that matters.

[9]ACS, level11 (November2016), Cyber security, threats, challenges & Opportunities.

[10] A.T.Tunggal (Jul 2021), what is a cyber-threat? Also available at: https://www.upguard.com/blog/cyber-threat

[11] United nation conference on trade and development (New York and Geneva, 2001) Economic Development in Africa: Performance, Prospects and Policy issues.

[12] Internet World Stats, Usage and population statistics. Also available at: https://www.internetworldstats.com/stats1.htm

[13] H.O.Quarshie & A.M.Odoom(2012) Fighting cybercrime in Africa.

[14] WhatsApp to stop working on these Android smartphones from tomorrow Jan 1, 2021 – Full list of mobile phones and how to check. Also available at: https://www.zeebiz.com/technology/apps