Impact of New Technology in Increasing Cyber Crime in Rwanda

By: ***UWINAGANYE Vedaste[1], Dr. Nyesheja M. Enan[2], Dr. RWIGEMA James[3]***

Abstract

The ICT sector in Rwanda has grown rapidly in recent years, with access to information and communication technologies available to the government, private sector, communities, and international organizations. The rate of the population mobile users was 76.6% in March 2018 according to the report published by Rwanda Utilities Regulatory Agency (RURA). Also in March 2018, the number of mobile money transactions was 692.5 billion Rwandan francs. Due to this information provided, above we decided to carry out research of assessing the impact of technology in increasing cybercrime in Rwanda and set measures that can be used to avoid cybercrime.

Keywords: *cybercrime, ICT, New technology, impact, Criminal activities*

Introduction

In almost all human endeavors, information and communication technology (ICT) has emerged as a driving force. This global wave's major component, the Internet, has become a double-edged sword, offering individuals and businesses numerous opportunities while also significantly increasing the risk to information security. The internet, in particular, has changed both formal and informal business dealings.(1) The international information market was developed through the process of economic globalization with new technology, not only proving new profitable opportunities but also raising the problem of criminal activities.

Any illegal activity carried out via one or more internet components, such as websites, social media chat rooms, online transactions, or email, is considered cybercrime.(1) A larger number of people do their own activities at home using an internet connection including work, school, shopping, health services, and entertainment in general.(2) Due to the expansion of cyber functionalities, criminal acts can now be carried out online, and the internet serves as the medium through which they accomplish their objectives. In order to locate, target, and harm their targets, hackers, criminal organizations, and spies from all over the world have access to powerful and constantly evolving tools. They even have established markets for the purchase and sale of cyberattack targeting and execution tools and expertise.(3)

New Technological Crime in Rwanda

As a foundation for economic growth, the government of Rwanda (GoR) has made significant investments in ICT infrastructure and applications. As expected, this enables economic expansion and social mobility to improve Rwandans' standard of living, social economic policy, and plan.(4) Nowadays in Rwanda, most of the institutions, organizations, businesses, schools, and universities have digitized their services and they deliver different services online. This implies the use of new innovative technology and new opportunities which promoted the development of the population and the country in general.

In general, the government, the private sector, and international organizations have funded development in the ICT sector in Rwanda, which has experienced rapid expansion. The distribution of internet bandwidth to rural communities for the purpose of accessing education, health, and public services like Irembo services, Rwanda Revenue Authority (RRA) services, and Rwanda Social Security Board (RSSB) Services in a rural and remote area of Rwanda has resulted in high levels of improved access to information and communication technology (ICTs) in Rwanda. (4)(5)

Is the Web Beneficial or Negative?

The merging of communications and computing has brought about wonderful technological change that has a significant influence on numerous aspects of everyday life. Information technology and telecommunications are essential to education, the stock market, welfare, and banking. Sadly, unprecedented opportunities for criminal activity have emerged as a result of the convergence of communications and computing technologies. One of the biggest problems we'll face with the new technologies is figuring out these weaknesses and taking the right measures to fix them. (1)

This article demonstrates that the internet is a powerful force for positive change. It is altering the nature of commerce and government and providing us with inexpensive and simple access to a vast reservoir of information and entertainment for every moment of our daily lives. In a different way, people claimed that internet communication is inferior to traditional face-to-face interaction in terms of social exchange and will result in negative outcomes. Over time, media coverage of the effects of internet use has emphasized this negative perception.(1)

However, there are three main ways that the internet has affected harmful or criminal activity: One is that harmful patterns of behavior like drug trafficking, bomb-talk, stalking, and so on are being perpetuated by the internet as a means of communication. Second, the global nature of the internet has opened up new opportunities for harmful behavior that are already covered by civil or criminal law. Thirdly, other harmful behavior, such as the unauthorized appropriation of images, software tools, and music products, has been encouraged by the nature of the virtual environment, particularly in terms of the distances between time and space. (5) Due to this in 2016, Rwanda was attacked by more than 1000 cyber-attacks daily before they could affect targeted individually, company, and institutions and the bank registered 80 hacking cases

according to the central bank.(5) Even those internet has played a big role in service delivering and encouraged more innovation for problem solving in ICT sector.(6)

Cybercrime in Rwanda

In 2017, 70% of the population in Rwanda had mobile subscription while 20% had activated mobile broadband subscription as reported by international telecommunication union (ITU). Rwanda as developing countries tend to lack of infrastructure, economics and social political framework for developing e-Commerce compared to the developed countries.

As a result, the use of the internet has grown rapidly in the majority of Rwanda's urban areas, as has the use of mobile phones. Financial crime is a big problem in Rwanda, and the impact it has on the country's economic growth cannot be overstated. However, while there are many interesting and important articles on this topic, broad accounts of Rwandan related crime are harder to come by. Although email phishing, online banking fraud, brute force attacks, network scanning, viruses, worms, and other forms of fraud can occur in Rwanda.

According to the mission statement, "The mission of the national cyber security policy is to ensure Rwandan cyber space is secure and resilient," Rwanda is aware that threats to cyber security pose a global threat to information integrity, safety, and privacy. Rwanda will safeguard its cyberspace in the coming generations to safeguard its citizens.(4)

Impact of cybercrime in Rwanda

Since nearly every part of the country is connected to the internet, cybercrime has become a global problem that necessitates the full cooperation of the public and private sectors in all provinces, including Kigali City. A nation's ability to identify and prosecute cybercriminals is a crucial aspect of information and infrastructure security. These areas' weaknesses have the potential to jeopardize security worldwide, not just in Rwanda. The risk of cybercrime has become a global issues and now affecting almost all country wide. In 2018, Rwanda become in country where users faced the highest risk of local infection with 46%.

The oboe makes it abundantly clear that cybercrime is a novel threat to society, that it can occur at any time and from any location, and that authorities tasked with investigating it need to devote a greater amount of time and effort than they do to locating and identifying the perpetrators of traditional crimes. For instance, policy and security officers must be able to locate electronic evidence and deal with cross-border challenges when tracing suspected hackers and crackers.(1)

Consider a hypothetical case like online credit card fraud to illustrate the cross-border issues that can investigate cybercrime cases. The ease with which a global network of victims can be reached without ever having to know their names, visit the bank that issues the cards, or even set

foot in their countries is one of the reasons why this type of fraud has skyrocketed. This indicates, from the perspective of law enforcement, that suspects and victims may be scattered across the globe. Dues to this it's duties for every one either personal, private organization, public organizations, to share information for any element which can suspected to commit a cybercrime. (1)

Conclusion

This article concludes that organizations and individuals have a responsibility to ensure their own protection because the impact of cybercrime is an unavoidable consequence of the convergence of ICT. While I concur that cybercrime is prevalent in both developed and developing nations, as well as in Rwanda as a whole, its impact appears to be greater in developing Rwanda due to a lack of adequate technology and enforcement expertise.

Despite the major obstacles Rwanda faces as a result of its low literacy rate and lack of suitable resources, the internet continues to provide an endless supply of opportunities. We end up suggesting that the security of new technology will depend on the efforts of all organizations and institutions as well as on the degree of self-help by potential victims of cybercrime. In a similar vein, public and private security agencies cannot effectively combat cybercrime alone. The role that the communications and information technology industries play in creating products that are resistant to crime.

Last but not least, it is important to note that one of the biggest threats to the widespread use and development of ICT in Rwanda is cybercrime. Hacking, economic espionage, web defacement, data sabotage, viruses, fraud, unauthorized access, and other acts against computer networks are all examples of cybercrime. Data can affect anyone, including businesses, the government, and citizens in general.

REFERENCES

1. Salifu A. The impact of internet crime on development. J Financ Crime. 2008;15(4):432–43.
2. Monteith S, Bauer M, Alda M, Geddes J, Whybrow PC, Glenn T. Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. Curr Psychiatry Rep. 2021;23(4).
3. Lagazio M, Sherif N, Cushman M. A multi-level approach to understanding the impact of cyber crime on the financial sector. Comput Secur [Internet]. 2014;45:58–74. Available from: http://dx.doi.org/10.1016/j.cose.2014.05.006
4. ICT RM of. National Cyber security Policy 2016. Rwanda Minist ICT [Internet]. 2016;(August):15. Available from: https://www.minict.gov.rw/index.php?eID=dumpFile&t=f&f=14149&token=e52639123cc23fbb644ea5b6b7a21212abef6c31
5. Mugisha D. METHODS AND IMPLEMENTATION TO COMBAT CYBER CRIMES IN 8 th Annual INTERPA Conference Theme : Cyber Security and Combating Cyber Crime. 2019;(February).
6. Kosanke RM. 済無No Title No Title No Title. 2019.