Chapter 12
Cyber Criminals on the Internet Super Highways: A Technical Investigation of Different Shades and Colours within the Nigerian Cyber Space

Edwin Agwu
University of Wales, Cardiff, UK

ABSTRACT

The internet has impacted the lives of individuals, organisations, and governments all over the world. However, it is now viewed and adopted with caution due mainly to the criminal tendencies of some misguided elements within the society. The internet technology has evolved to become a weapon of "mass robbery" in the hands of criminals. Fraudulent mails emanating from Africa, in general and Nigeria in particular have received world wide attentions. These and more have dented the image of the country home and abroad. This study presents the various ways in which the internet is used for criminal purposes within the Nigerian polity. It further examined the various crime related laws, their adequacies, and implications. Findings revealed the interplay of different methods through which vulnerable individuals and organisations are defrauded. The strategies proposed for addressing these crimes with a view to giving the country a clean bill of health in the international community are as well applicable to other developing countries. The findings also lay solid foundations for further research within different strands of crimes. It also concludes with recommendations for policy makers, businesses, and internet services providers with emphasis on the need for greater awareness creation.

INTRODUCTION

Cyber or online crimes, a crime, hitherto committed over the internet highway, have assumed a gargantuan status. CIA (2010) estimated that two to three billion are made from this per year. The internet since its inception and subsequent adoption by businesses and individuals has provided a viable platform or channel for genuine business transactions, communications, socialization, as well as for frauds. The next section examined the various definitions of crime, followed by a review

DOI: 10.4018/978-1-4666-5942-1.ch012

of the internet services in the sub-Saharan Africa in general and Nigeria in particular. The Nigerian crime related laws were further examined with specific emphasis on its adequacies. The implications of the study are highlighted in the last section and recommendations drawn from the findings. Furthermore, the scope for further research and practice forms part of the conclusions.

WHAT IS CYBER CRIME?

Crime has been around long before the advent of the internet; however, since the introduction of the internet and its wide adoption, frauds migrated to cyberspace and have now advanced at a much faster rate ranging from the use of famous names of individuals and organisations to defraud as well as organised attacks. The United Kingdom Home Office (2010) defined cyber crime as "offences that can be committed through communication technology". While the United State Department of Justice (2000) defined internet fraud as: any type of fraud scheme that uses one or more components of the internet, such as chat rooms, e-mails, message boards, or web sites to present fraudulent solicitation to prospective victims, to conduct fraudulent transactions, or to transmit the proceeds of fraud to financial institutions or to others connected with the scheme.

Furthermore, cyber crimes have also been viewed as any form of criminal activities that involves the use of computers and the internet (Council of Europe 2007). These includes but not limited to theft, child pornography, harassment, threatening behaviours and other anti-social activities (De Schrijver et al., 2004). The internet, undoubtedly, provides a fertile ground for criminals to plan, hatch and execute their criminal activities across geographical and jurisdictional boundaries. This poses a serious challenge to both local and international law enforcement agencies (London's Metropolitan Police Service 2007). This is because, some offences such as the use of emails for financial solicitation (usually emanating from one country) can be distributed to many countries at the same time and these may be viewed differently based on the respective laws of each country.

It is however, worthy to note that crimes and fraudulent acts are as old as man. It is often touted as having its roots biblically in the Garden of Eden. However, the first recorded fraudulent act within the world most read holy book, The Bible, was the deception by Abraham when he denied his own wife. Another was Jacob against his big brother Esau and his subsequent collection of the blessing hitherto meant for Esau based on seniority. And in the New Testament, was the denial by Peter that he never knew who Jesus was in order to save his own life. Fraud therefore is an age-long act that has come to stay.

Within the sub-Saharan Africa, Nigeria tops the list in fraud related activities, and a well known key player in the international community (Adomi & Igun 2008). The activities cover a wide range of activities; from the use of expertise or highly technical and technological tactics with which victims' personal details are obtained. Others include but not limited to bank account details, ATM pin numbers, and credit card details, among others (Longe et al., 2008). The hues and cries about these and more have driven these perpetrators to widen their scope to dating websites where vulnerable singles (bachelors and spinsters) engage in discussions leading to exchange of personal details which includes, full name, telephone numbers, email accounts, Skype names, facebook IDs, twitter, etc; the combined effects of these and more serves as a serious problem to internet users all over the world (Okugbule, 2006). Unfortunately, cybercrimes, viewed as an entity, have since been engulfed in very serious controversies. While some cybercrime activities are acceptable within a country, it is illegal in another country. Digital surveillance or censorship is another boiling point of controversy with respect to cybercrimes. The right to freedom of expression has therefore