Chapter 7
Cybercrime Regulation:
The Nigerian Situation

Alex Ozoemelem Obuh
Delta State University, Nigeria

Ihuoma Sandra Babatope
Delta State University, Nigeria

ABSTRACT

This chapter discusses cybercrime and cybercrime regulation in the Nigeria. It gives the meaning to cybercrime, types of cybercrimes (of which advance fee fraud is the most prevalent in Nigeria), means of perpetrating cybercrimes, the current situation and efforts towards combating cybercrime in Nigeria.

INTRODUCTION

Advancements in information and communication technologies (ICTs) have led to the representation of different types of information in electronic formats. The consequence is that currently text, pictures and voice can all be digitised. Along with these geometric changes in information presentation and distribution are tandem demands in user expectations for more rapid, open, and global access to information than has been available in the past. However, this migration from traditional communication medium to the new mediat seems to constitute a threat to the existence of a number of traditional print institutions and has provided a platform for fraudulent (criminal) Internet activities. Computers are increasingly more affordable and Internet connectivity is also becoming commonplace. The introduction and embracement of the Global System for Mobile Communication (GSM) in Nigeria and the influx of digital and online services such as the MP3 players, Ipod, cell phones with internet access and blogs (instant news reporting on personal and corporate web pages) (Longe & Chiemeke, 2008)

Cybercrime is a major concern to the global community. The introduction, growth, and utilisation of information and communication technologies (ICTs) have been accompanied by an increase in criminal activities (Parker, 1998). With respect to cyberspace, the Internet is increasingly used as a tool and medium by transnational organised crime (Lyman & Potter, 1998). Cybercrime is an obvious form of international crime that has been

DOI: 10.4018/978-1-61692-012-8.ch007

affected by the global revolution in ICTs (Parker, 1998). As a recent study noted, cybercrimes differ from terrestrial crimes in the following four ways (McConnell, 2000):

- They are easy to learn how to commit;
- They require few resources relative to the potential damage caused;
- They can be committed in a jurisdiction without being physically present in it; and
- They are often not clearly illegal.

On such a basis, cybercrimes present new challenges to lawmakers, law enforcement agencies, and international institutions. This necessitates the existence of an effective supra-national as well as domestic mechanisms that monitor the utilisation of ICTs for criminal activities in cyberspace.

Nigerian 419 scam has become a major concern for the global community. The introduction, growth and utilization of information and telecommunication technologies (ICTs) have been accompanied by an increase in illegal activities. With respect to cyberspace, anonymous servers, hijacked emails and fake websites are being used as a tool and medium for fraud by cyber scammers. Nigerian advance fee fraud on the Internet is an obvious form of cybercrime that has been affected by the global revolution in ICTs. This form of crimes is not exclusive to advance sums of money to participate into business proposals but also covers romance, lottery and charity scams. The term '419' is coined from section 419 of the Nigerian criminal code (part of Chapter 38: Obtaining Property by false pretences; Cheating) dealing with fraud. Currently, the axiom '419' generally refers to a complex list of offences which in ordinary parlance are related to stealing, cheating, falsification, impersonation, counterfeiting, forgery and fraudulent representation of facts (Tive, 2006).

According to 2007 Internet Crime Report prepared by the National White Collar Crime Centre and the FBI, Nigeria currently ranks third in the world with 5.7 per cent of perpetrators of cybercrime (2007 Internet Crime Report). The Nigerian government has over the years enacted far-reaching laws aimed at checkmating transnational organized crime and punishing the perpetrators of these crimes. Efforts in regulating cybercrimes such as advance fee fraud and 419 are reflected in the Criminal Code Act, Economic and Financial Crimes Commission Act 2004, Computer Security and Critical Information Infrastructure Protection Bill 2005 and Advance Fee Fraud and other Fraud Related Offences Act 2006.

This chapter is aimed at explaining the concept of cybercrime especially as it relates to Nigeria, issues relating to cybercrime legislation and suggests ways of getting out of these problems in the present days of internet usage and applications.

BACKGROUND

Cybercrime is generally regarded as any illegal activity conducted through a computer. Cybercrime is any criminal activity employing an information system (which may not be computerized) as the channel through which it is committed (Parker, 1998). It is illegal computer -mediated activities which often take place in the global electronic networks (Thomas & Loader, 2000). Cybercrime is when criminals use computers or networks as a tool, place, or target for criminal activity and behavior. The evolvement of cybercrime has affected law enforcement agencies and society. Enforcement has led to the creation of laws, policies, and legislature. Law enforcement agencies must vigorously fight and prevent cybercrime in order to help create a society that is safer (Thomas, 2006).

Cybercrime is a major problem faced by businesses attempting to establish and maintain an online presence (Smith & Rupp, 2002), and cybercrime attacks can potentially be just as damaging to a nation's infrastructure as attacks by classical criminals. Computer-related crime includes theft of telecommunications services or