# Chapter XVIII
# Cyber Crime Control in Developing Countries' Cybercafés

**Stella E. Igun**
*Delta State University, Nigeria*

## ABSTRACT

*This chapter discusses the challenges and problems governments and other stakeholders are facing in fighting and controlling cyber crimes in developing countries cybercafés. The chapter's main focus is on the developing countries vulnerability to cyber crimes; these countries lack major infrastructural devices for controlling cyber crimes at the moment. The nature of cyber crime and Internet in developing countries is pathetic, in that the cyber crime rate is high and transnational (affecting the developing countries all the same) and the developing countries are still very low in Internet connection. Furthermore, the chapter reveals reasons for the increase in the incidences of cyber crimes in developing countries; cyber crime laws that have been enacted to control and tackle the problem of cyber crimes are also highlighted.*

## INTRODUCTION

The Internet has grown explosively over the past few years. Compared to only 20 million in 1995, over 200 million now communicate, shop, settle bills, engage in business transactions, and even meet with their doctors online (United Nations Office on Drugs and Crime, 2000). The capabilities and opportunities provided by the Net have transformed many legitimate business activities augmenting the speed, ease, and range with which transactions can be conducted while also lowering many of the costs (Williams, 2002). As the Internet has expanded so has its misuse (United Nations Office on Drugs and Crime, 2000). Criminals have discovered that the Internet can offer them new opportunities and multiplier benefits for *illicit business*. The dark side of the Net involves

not only *fraud* and theft, pervasive pornography and pedophile rings, but also drug trafficking and criminal organizations and individuals that are more concerned about exploitation than the kind of disruption that is the focus of the intruder community. In the *cyber space*, as in the real world, most *criminal activities* are initiated by individuals or small groups and can best be understood as "disorganized crime" (Williams, 2002).

Cybercafé could be described as a virtual market where all kinds of business transactions take place. Due to high cost of Internet connectivity and access, they are used by most Net users in developing countries as access points to the Internet (Adomi, Okiy, & Ruteyan, 2003; Mutula, 2003). They were originally set up to carryout genuine activities such as browsing, faxing, making Internet calls, and scanning and printing material, but now most cybercafés are known for *dubious activities*, especially at night. At the moment, cybercafés have attracted scammers (Abodurin, 2004) and pornographic activities by students and youths. Abodurin (2004) further lamented that the youths are supposed to be our future and yet are wasting valuable time doing wrong things. Cybercafés thus provide safe haven for *cyber criminals*.

Cyber crime can be referred to as *criminal activity* committed on the Internet. It describes everything from electronic cracking to denial of service, attacks that cause cyberspace owners and electronic sites to run at a loss. Cyber crimes may be committed against individuals, property, and government. Crime waves against information on computers have become a problem in the cybercafés in the world. The developing countries cybercafés lack legal protection, they rely mostly on technical security measures built into the system to protect the system's information and businesses and government from those who steal, defraud, and destroy important information. Since the developing countries depend only on system-in-built protection and self protection, cybercafés in developing countries are becoming dens for *fraudsters* and dangerous criminals. The advanced countries have put in place rules and laws guiding *cyberspace* to make it a safe place. Even at this stage, these countries still need to evaluate and examine their current laws to see that the laws are meeting with current cyber crime waves that are always on the increase.

Since cyber crimes pose challenges that have arisen from the development and use of *information technology*, the problems associated with cyber crimes should be dealt with by all stakeholders and the governments. Developing countries should establish risk management policies on cyber crimes because of their limited resources. It should be noted that cyber security technology vary from country to country in terms of infrastructures and complexities, while cyber attacks may be the same for all countries because of the nature of globalised (Internet) computer networks.

The relationship between the growth of the Net and attempts to control it can reveal a lot about the democratic potential the Internet offers in developing countries. Observers of the Internet should note that the terrorist attacks of September 11, 2001 (911) have accelerated efforts to control the previously free space provided by the Internet (Gomez, 2004). The need to stem negative effects of terrorist acts and other cyber related crime have driven governments, non government organizations, and individuals in industrialized and developing nations to devise measures to control the tide of cyber crime. Some of these measures are directed at control of cyber crime in several developing countries (Hasan, 2002; Glaser, 2003; AsiaMedia, 2004; Gomez; 2004; Federal Republic of Nigeria, 2006).

The objectives of this chapter are to explore the vulnerability of developing countries to cyber crimes; the categories of cyber crimes that are prevalent; the steps taken by the developing countries and their governments to control cyber crimes; the laws that have been enacted and the acts put into action to control crimes; the action