Chapter XVI
Cybercafés of Nepal:
Passage to Cyber Crime?

Deepak Rauniar
South Asia Partnership International, Nepal

ABSTRACT

The chapter introduces the cybercafés of Nepal and explores the prospect of someone (persons, criminals) exploiting them to commit global cyber crimes. Cybercafés are public places of Internet and are considered important tools of society for access to information and e-services of all kinds. However, by the virtue of being public places, they also stand vulnerable to misuse in terms of cyber crimes. The chapter discusses cybercafés and cyber crimes and introduces them with specific reference to Nepal—a country in south Asia nestled between two information technology giants, India and China. The chapter also discusses the cyber law of the country. Based on research carried out with the objectives of assessing the scenario in which the cybercafés operate in Nepal, it has been argued that they can be easily exploited to commit cyber crimes. Further, in terms of the facts that have emerged from the research, appropriate recommendations have also been derived and presented.

INTRODUCTION

Bordered by the People's Republic of China to the north, and by India to the south, east and west, Nepal is one of the most beautiful countries in the world. Land of the Himalayas, home to Mount Everest, steepest country in the world, rich in culture, diversity, heritage, flora and fauna, are some of the attributes of the country. The total population of the country is around 24 million, GDP per capita of about $270 and a poverty incidence of 38%. The difficult terrain of the hilly and mountainous regions of the country makes development much more difficult, restricting ac-

cess to resources and information to the common man. Sadly, it is also one of the poorest countries in the world.

In terms of information and communication technologies (ICT), the country had its first exposure to computer and computer systems as early as in the 1971. However, despite making such an early start, unfortunately the country could not leverage on the opportunities and prospects of ICT to its potentials and the proliferation of ICT in the country happened slowly.

The real progress in the ICT arena of the country can be considered to have happened only after 1995 onwards (Chapagain, 2006), when a large number of enterprises went for automation. To support this drive, universities and colleges started offering courses in computer science and computer engineering, while the country saw a number of policy initiatives and liberalization by the government. The private sector started to play its anticipated dominant part.

The recent developments in ICT and the according emergence of modern ICT concepts and applications such as e-governance, e-commerce, e-finance, and so forth, have made significant business and social impacts in Nepal as well. In line with the anticipated benefits of ICT, in modern Nepal a wide-spectrum of Nepalese enterprises (from all sectors including the government) exist, which have not only been successful in integrating ICT, including the Internet, with their businesses processes, but have also been successful in exploiting it as an engine of growth.

While it is true that technologies including the Internet open doors to numerous opportunities to enterprises in terms of ease, speed, wider coverage, variety, reduced costs, and so forth, it is also true that like a double edge sword, they also provide significant opportunities and multiplier benefits for illicit businesses as well. The sheer fact is that as brick-and-mortar companies move their enterprises on to the World Wide Web (WWW) seeking new opportunities for profits, so have been criminal enterprises.

The other side, alias the dark side, of the Internet involves not only hacking and cracking, fraud and theft, pervasive pornography, pedophile rings, and so forth, but also extortion, money laundering, pirating, corporate espionage, drug trafficking, and criminal organizations. And these are commonly known as cyber crime. The perpetrators of cyber crime range from teenage "cyber-joyriders" to organized crime operations and international terrorists.

Considering *cyber crimes* to be a special (and often non-traditional) type of crime, many countries have come out with specific laws to deal with them, which are often commonly known as cyber laws.

Given the sheer amount of economic and non-economic (social and national security) impacts associated with *cyber crimes*, today they stand as a challenging and not to be neglected proposition for all countries that intend to benefit from the realms of ICT.

Cybercafés are public places of Internet access that offer networked computers for hire by the hour. They are an important tool of a society for access to information and e-services of all kinds. Patrons have a variety of Internet applications available to them, including Web surfing, e-mail, and chat rooms. Some cafés also provide office-type applications to the visitors (Stohs, 2004). However, being public places and thus the perceived anonymity arising out of it, unfortunately they also stand as one the most vulnerable places to commit *cyber crimes*.

In Nepal, a significant number of *cybercafés* exist. In major cities, a cybercafé can be found in almost all important streets and buildings. However, many of them are not registered and in the absence of a designated authority to monitor and supervise them, all of them remain unsupervised. Further, there are no policy interventions to regulate them.

Accordingly, the *cybercafés* of the country operate with complete freedom with regards to their wish and what they can afford. The same is