Chapter 13
Prevention and Regulation of Cyber-Crimes in the Age of Terrorism:
The Legal and Policy Model from India

S.R. Subramanian
Hidayatullah National Law University, India

ABSTRACT

India is the 12th nation in the world to have a special system of laws addressed to the information technology sector. Besides the general criminal law of the country, the Information Technology Act, 2000 incorporates a special legal framework relating to cyber-crimes. Looking differently, India is also a global hub of information technology and its allied services. Accordingly, the growth and development of the information technology sector and its contribution to national economy is phenomenal. It is in this context, the chapter examines and analyses the Indian ICT laws and policies in the backdrop of cyber-crime prevention and regulation, with the aim of offering a comprehensive model of ICT policy. It will discuss the extent of legal framework in the light of classification and criminalization of various cyber-crimes. Also, while examining the policy instruments, it will bring out the public and private initiatives on protection of information infrastructures, incident and emergency response and the innovative institutions and schemes involved.

INTRODUCTION

The unprecedented growth and development of information and communication technology (ICT) along with the open and hitherto unregulated nature of the internet and the anonymous feature of internet activities acted as the 'safe heaven' for criminal purposes. Besides a new range of technological offences, a number of traditional crimes such as theft, fraud and conspiracy can also be committed via the internet. In other words, internet can be the subjects of crime, it can be the site of a crime and it can also be a tool through which crimes can be committed (Kamath (2005). With the exponential increase in internet-related crimes, both in terms of number and sophistication, cyberspace present new challenges to the security and stability of the

DOI: 10.4018/978-1-61692-012-8.ch013

internet and raise serious concerns for policymakers and other stakeholders at all levels.

However, cyber-crime is a new discipline and hence the legal response to these rapidly growing illegal activities is still in the process of emerging. The dilemma of cyber-crime regulation is that it is caught between two diametrically opposite legal approaches (Gelbstein and Kurbalija (2005). The 'real law' approach, on the one hand, considers the internet as a natural evolution of existing technologies like telegraph and hence extends the application of prevalent legal rules to the internet. On the other hand, the 'cyber law' approach treats the internet as *sui generis* development and believes that it can only be regulated by special laws. Nonetheless, the practice of most government is that the existing law can be applied to the problems of internet, with varying levels of modifications.

However, the major challenge in regulating the cyber-crime is not the multiple categories or the magnitude of crimes, but that the law is inadequate to deter and prevent further violations. Hence, the investigation, prosecution and enforcement of cyber-crime is an enormous challenge for any criminal justice machinery. Moreover, the global phenomenon of the cyberspace also adds to the jurisdictional quagmire of the internet (Rao, (2004). This underlines the significance of the continual update of law and policies to keep pace with the latest technological developments to prevent it from being obsolete.

India is a global IT player and is a pioneer in the field of cyber-law, having brought the Information Technology Act in the year 2000. However, the Information Technology Act, 2000 was heavily criticized for improper treatment of cyber-crime. Even as the Statement of Objects and Reasons of the enactment claim, the law creates an enabling environment for electronic commerce and only incidentally addresses the issues of cyber-crime. Until the passage of Information Technology (Amendment) Act, 2008 (Act No. 10 of 2009), the law was woefully inadequate to deal with the vital issues like 'cyber-terrorism', not to speak of the onerous challenges of use of internet for terrorist purposes.

It is in this context, the chapter examines and analyses the Indian ICT laws and policies in the backdrop of cyber-crime prevention and regulation, with the aim of offering a comprehensive model of ICT policy. It will discuss the extent of legal framework in the light of classification and criminalization of various cyber-crimes. Also, while examining the policy instruments, it will bring out the public and private initiatives on protection of information infrastructures, incident and emergency response and the innovative institutions and schemes involved.

CYBER-CRIMINAL LAW IN INDIA

India is the 12th nation in the world to have a special system of laws addressed to the information technology sector (Regulatory norms, 2006). Recognizing the potential contributions the information technology sector can make to the socio-economic development of the country, the legislation sought to create an environment for electronic commerce. It also incidentally criminalizes and punishes certain conduct prohibited under the law. These provisions are in addition to the general criminal law contained in the Indian Penal Code, 1860, itself amended by the Information Technology Act, 2000. Most importantly, a thorough overhaul of cyber-criminal law, inter alia, has taken place through the Information Technology Amendment Act, 2008[1].

Contraventions

The law vertically classifies the cyber-crimes into two types: contraventions and 'information technology offences'. While contraventions will attract financial sanctions in the form of com-