The Perpetration and Prevention of Cyber Crime: An Analysis of Cyber Terrorism in India

Poonam Kumar, Asia Pacific Institute of Management, India
Saurabh Mittal, Asia Pacific Institute of Management, India

ABSTRACT

Cyber crime has become an integral part of the transnational threat landscape and conjures up pressing images of nefarious and increasingly complex online activity. More recently, the concept of ‘organized crime’ has been attributed to cyber criminality. There has been subsequent disagreement and confusion concerning whether such crime is a derivation of traditional organized crime or an evolution of such crime within the online space. This paper analyses the opaque state of affairs which has been exacerbated by the relative lack of clear evidence attesting to and supporting either scenario. Technological advances have always been used to the advantage of the criminal fraternity. The crucial question that remains is whether those advances have merely facilitated the commission of physical crime or whether in fact they have led to the creation of a new wave of traditional, but virtual, organized crime. The paper also explores the behavioral ramifications on cyber crime on the informational value of the internet and its usage in consumer with demographic analysis level of its threat and increasing crime rate thus eroding the attractiveness of internet as a viable marketing channel.

Keywords: Crime Terrorism, Cyber Crime, Cyber Space, Online, Organized Crime

INTRODUCTION

Yar argues that ‘it has become more or less obligatory to begin any discussion of “cyber crime” by referring to the most dramatic criminological quandary it raises, namely, does it denote the emergence of a “new” form of crime and/or criminality?’ Grabosky sought at a relatively early juncture to address that question by suggesting that cyber crime was simply a case of ‘old wine in new bottles,’ that is ‘...less a question of something completely different than a recognizable crime committed in a completely different way.’ In a similar vein, Nisbett has argued that ‘cyber crime is on the increase. This does not necessarily mean that there are in fact any new crimes; rather there are new methods of committing existing crimes and better ways of detecting them.’ Interestingly, Wall has noted that ‘...when so-called cases of cyber crime come to court, they often have the familiar ring of the “traditional” rather than the “cyber” about them.’ Crime, like nature, however, abhors a vacuum. It has accordingly always seemed inevitable perhaps that traditional organized crime groups would

DOI: 10.4018/jte.2012010104
positively rush to fill the void for illicit product placement deemed to present itself in the context of cyberspace. It might be assumed, therefore, that an evaluation of the purported involvement of traditional crime groups in cyber crime would be a relatively simple affair. Certainly, the literature, broadly defined, is replete with references to ‘cyber crime’ and more recently to ‘organized’ cyber crime. Unfortunately, the mere assertion in much of that literature that such crime exists (both in a general sense and in an organized form) has been routinely transmuted, as if by osmosis, into tangible fact. Arguably, however, in many cases those ‘facts’ appear to rely as much upon anecdote, hearsay, extrapolation and assumption as they do upon objectively obtained and verified evidence. At the basic level of analysis there is no discernible control mechanism in place insofar as terminology is concerned. Thus, one might speak of ‘cyber crime,’ ‘high tech crime,’ ‘Computer crime,’ ‘technology crime,’ ‘digital crime’ and ‘IT crime’ and be discussing the same and/or different concepts, respectively. Achieving any vestige of comparative analysis of the impact of cyber crime therefore is fraught with difficulties. Beyond that, the increasingly common conflation of cyber crime with the prefix ‘organized’ infers the involvement of traditional organized crime groups but ultimately alludes to ‘ordinary’ criminals who happen to operate in cyberspace in an organized manner.

Equally, it seems common to refer to cyber criminal ‘groups’ as if they were of equivalent size, complexity, ‘stature’ and duration as their traditional, non-virtual counterparts. This effectively allows cyber criminal groups to achieve the semblance of the organizational evolution actually achieved by those traditional organized crime groups they are deemed to emulate. In short, there remains a confused and confusing plethora of terminology, purported parameters and alleged participants of cyber crime as well as concerns over the provenance and quality of evidence elicited in support of such activity. These are certainly subtle differences but they are important differences nevertheless. The number of crimes in cyber space is rapidly multiplying in India. It is important for every citizen of India to know about what is happening in cyber world and how to protect ourselves from these crimes. Each time newer, cunningly plotted plans have been induced by the hackers to harm the users of internet to create a chaos in the cyber world. We have to take measures to lessen it in every little way possible to make our country a better place to live in. In the report we are going to mention about revolution of cyber crimes in India, some recent cases and the statistics in Indian scenario. The cyber crime had emerged in early 1970’s and had very basic cases, because of the advancement of the technology, the cases as increased rapidly and today Indian Cyber crimes are one of the big scandalous crimes which are increasing geometrically in a democratic country like ours – INDIA. According to the research taken by internet crime complaint centre of USA, it was found that our country is ranking 5th position in number of cyber crime cases. It’s not an achievement to tell proudly outside. We should be ashamed of this status and should take necessary actions to reduce the amount of cyber crimes. In the earlier times, crimes were quite easy to detect but after the emergence of criminal activities in the world of cyber space it has become a tedious work to detect such crimes and punish those people who indulge in such malpractices.

The reason for increase in the cyber crime is because of following reasons:

1. The people were feared because of the negative publicity.
2. They were not aware that police had equipped to handle such cyber crimes
3. They were feared of further cyber attack.
4. They were not aware of Cyber Laws.
5. They were fear of false arrest concerns.

THE RISE OF CRIME IN CYBERSPACE

The term “cyberspace” was coined by the science fiction author William Gibson in his 1984