Cyber Crime Regulation, Challenges, and Response

Sachin Tiwari
https://orcid.org/0000-0001-5526-129X
Jawaharlal Nehru University, India

INTRODUCTION

The cyberspace emergence has created a new reality with transnational connection providing a venue for growth and also for contestation (Chourci, 2012). Defining the characteristics of the cyberspace includes various attributes such as; diffusion of power, ease of accessibility, low cost of entry, attribution, i.e., anonymity (Nye, 2011). The cyber domain position is characterized as a “transnational domain for information and economic exchange, which contemplates the transnational nature of the internet and the problem of global governance” (Kiggins, 2014). Definition of cybersecurity has constantly shifted to reveal the growing number of threats and new areas affected by the attacks. The case of UNGA resolution 53/70 where the modification of definition from the phrase ‘may adversely affect the security of the state’ in 1999 to ‘may adversely affect States in both civil and military fields’ in 2002 reflects the change in definition due to evolving nature and increased threats (Radu, 2014). Effectively, cybercrime was seen majorly as a technical issue, however, the course changed with the increase in incidents and the need for regulating it. The effective cost of cybercrime has increased with sophisticated tools being employed for a criminal purpose especially with the rise of ransomware as an industry. The concern arises from the fact that the average cost for the enterprises was $11.7 million of cybersecurity due to cybercrime, with an increase of 27.4 percent each year (Accenture, 2017). Platforms like Convention on Cybercrime in 2001, World Information Society in 2003, have pushed for a ‘global culture of cybersecurity’ and laid the foundation for the effective policymaking at the international, regional, and national level. Moreover, the international scenario is constantly molded by the sophisticated cyberattacks, global geopolitical shifts, and social media empowered by political move with the divergent position of the states. The variance is visible in the cyber legislation with varying definitions, development with one paternalistic group of countries advocating state sovereignty while other members promoting freedom of internet and role of private companies

In this perspective, the article aims at presenting and analyzing the state of the growing threat of cybercrime and the resultant laws being enacted at the international, regional and national level by the countries to counter it. The first section includes the background, including an overview of cybercrime being defined in the various literature. The second section includes various efforts presented on cybercrime legislation including the multilateral instruments such as the convention on cybercrime by Council of Europe, United Nations resolution apart from regional and national efforts. The third section analyzes the challenges of jurisdiction, sovereignty, and privacy and the various responses in the form of legislation being laid out. The fourth section proposes a model for the effective cooperation in the form of balanced multi-stakeholder in light of growing internationalization of the cybercrime.

DOI: 10.4018/978-1-5225-9715-5.ch025

BACKGROUND

Literature Review

The research on the cybercrime has focused on analyzing it from various perspective, including the technological, sociological, criminology, psychology, and economic perspective. David Wall (2001, 2007) in one of the early analysis puts cybercrime on the basis of behavior lists (i) Cybertrespass/ hacking (ii) Cyberpiracy (theft of intellectual property) (iii) Cyberpornography (iv) Cyber violence (harassment/ hate speech) as the problem exists on the nature and extent. Later an addition was made to the computer-assisted crime by Susan Brenner (2010) as a social practice with the addition of the cyberspace to all aspects of crime. Due to this addition; cybercrimes are defined on the basis of the "computer enabled" and "computer facilitated" activities. It is similar to the difference earlier categorized by Brenner (2007) of traditional crimes and more specifically defined cyber offenses. The UK investigation agencies make the distinction between the *cyber-dependent crimes* committed through computers directed against computers and other as *cyber-enabled crimes* (Wall 2007). Similarly, (McGuire, 2012) described the cybercriminal groups in the form of "swarms and aggregators" with three types, ranging from the almost virtual conducting illicit activities, hybrid criminal groups and as facilitators mainly traditional organization criminal groups involving in trafficking, gambling, etc.

The definition includes the cybercrime as a form of social practice, which was further articulated by Yar (2013) considers the debates cybercrime not as a single crime but as a broad range of illegal and illicit activities that have effects on societal, political, economic effect. Emilio Viano (2015) in evaluating cybercrime from a societal perspective, considers it as a vastly unregulated field presenting the challenge among policymakers for effective cybercrime regulation. Holt and Bossler et al. (2016) make the distinction that the early computer crime till the 1990s was referred to computer misuse and later with the development of computer and internet, the focus is on offenses in an online environment. What is constructed as an association of crime with cyber is related to the usage of this emerging domain for the traditional criminal activities plus some emerging from the cyber domain. The term "cybercrime" is used to describe a range of offenses, including traditional computer crimes, as well as network crimes (ITU, 2014). Gabriel Weimann (2015) considers the association of terrorism with the cybercrime, where the terrorist has exploited the internet for various means ranging from propagating radical messages to financial gains. Many authors have attempted to look at the extent of the harm caused by the cybercrime empirically which have varied across the reports and limited the real extent in the policy-making (Klahr 2017; Markus Rieke, Rainer Bohme 2018). From a psychological perspective (Kirwan, 2018) in quantifying cybercrimes and propose the effective policing, deterrence means and introduction of a capable guardian to deter the criminal activities. Susan Brenner (2012) identifies the association of the migration of the traditional crime into the cyberspace along with new distinct cybercrime and the need for developing new law for it. Several national laws globally are outdated and face the unique challenge to prosecute them.

Cybercrime Development and Law

The cybercrime originated early on with the spread of networked computers and the legislation for the prevention of it. One of the first legislation was enacted in the US was the *Access device fraud Act* of 1984 for stopping counterfeiting using electronic devices, including computers. The first major cybercrime incident originated in form of Morris Worm which affected computer system in 1988 in the US was