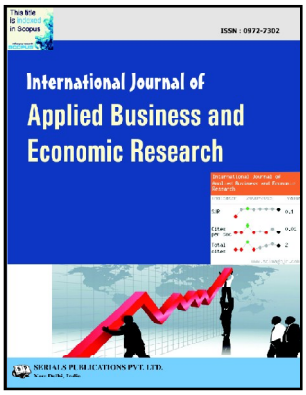

International Journal of Applied Business and Economic Research

ISSN : 0972-7302

available at http: www.serialsjournal.com

Volume 15 • Number 17 • 2017

Exploring Cyber Crime Patterns in India

Dinesh Yadav[1], Gurinder Singh[2] and R.S. Rai[3]

[1] *Research scholar, Amity International Business School, Amity University Uttar Pradesh*
[2] *Group Vice Chancellor, Amity Universities, Director General Amity International Business School, Amity University Uttar Pradesh*
[3] *Deputy Director, Research Planning & Statistical Services, Amity University Uttar Pradesh*

Abstract: There has been enormous growth of Internet and mobile smart phone in the recent years. This has made the information access very easy for the end user and hence has emerged as medium of tremendous amount of information and communication worldwide. The exponential growth of internet, usage of communication devices and I.T. enabled services has led to growth of cybercrimes across the world. This research paper provides an overview of patterns in cyber-crime data. This paper explored the patterns of cybercrime in India using time series and regression analysis. Analysis is based on National Crime Record Bureau, Ministry of Home Affairs, Govt. of India data on cyber-crime collected under the heads of offences registered under IT act, 2000, IPC related to cyber-crimes and Special and Local Laws (SLL) related to cyber-crimes. An attempt was made to see the patterns and trends of Cyber-crimes and their relationship with growth in Internet users in India.

Keywords: Cybercrime, Cyberspace, I. T. Act 2000

1. INTRODUCTION

The use of computer and information technology makes human life easy and fast. The penetration of cheap, powerful, user-friendly computers in human life has enabled more and more people to use them and, more importantly, rely on them as part of their normal way of life. As businesses, government agencies, and individuals continue to rely on accessing them for services more and more, so do the criminals. The misuse of computer, information technology and Internet gave rise to new type of crimes, called Cybercrimes.

Cybercrime may be defined as any illegal act in cyber space that uses computer as a tool or a target or both. Cyber space is referred to as mere virtual space, where computer-mediated communication takes place but which is not spatially located. Jaishanker (2011) defined cybercrime as; "Offences that are committed

against individual or a group of individual with the criminal motive to intentionally harm the reputation of victim, cause mental or physical harm or loss to the victim directly or indirectly using communication devices". As cybercrime is continuously evolving and no single definition can include all the facets and manifestations of cybercrimes in totality, there is no standard definition of cybercrime globally accepted by researchers and academia. There is no other crime alike cybercrime which affects people from all walks of life irrespective of their age, education, income and social status. Cybercrime may include anything and everything such as no delivery of goods or services ordered online, computer intrusions, intellectual property rights abuse, economic espionage, online extortion, international money laundering, and a growing list of other Internet facilitated crimes. List of cybercrime also includes distributing viruses and worms, illegally downloading files, phishing and pharming, and stealing personal information like bank account details.

Cybercrime is different from the traditional crimes as; (1) to commit a cybercrime, the offender is not required to be present at the scene of crime as it can be committed remotely from any part of the world, (2) most of the evidence in cybercrime cases is digital evidence which is invisible and fragile and can be altered easily unlike physical evidence, (3) specialized hardware and software tools are required to collect or extract the digital evidence. As most of the personnel working in police and other law enforcement agencies, prosecutors and even judicial officers are not aware of the use of specialized tools for digital evidence collection, they are not able to comprehend causes of many cases related to cybercrime. In conventional crime investigation, physical evidences such as finger print, foot print etc. collected from the scene of crime are of great importance but for cybercrime investigation these evidences are irrelevant and hence the traditional methods of crime investigation have become outdated in investigating cybercrimes. Thus prevention, detection and investigation of cybercrimes is a constant challenge to the police and other law enforcement agencies.

The Information Technology Act 2000 (Amended 2008), attempts to provide ways to deal with cybercrimes. This Act has made it possible to have legal status to intangible electronic and digital records and therefore digital information got validity and enforceability. It empowers the authentication of the digital records through digital signature.

2. LITERATURE REVIEW

The global Internet penetration (user percentage of total population) rose at a compound annual growth rate of 10% from 23.2% in 2008 to 38.1% of the global population in 2013. This represents a global base of Internet users of 2.7 billion in 2013. International Telecommunication Union (ITU) predicted that 3 billion users were likely to have been surpassed in May 2015 and mobile penetration will reach to 71% by 2019 (Internet Society Global Internet Report, 2015, pp. 42,44). Ashish Kalsi, strategist, search quality of Google India stated that here are 350 million Internet users in India, of which 152 million are mobile users. This number is projected to increase to 500 million in 2017, of which 400 million are going to be mobile users. (Google: Internet users in India to touch 500 million by 2017, 2016).

(KPMG Cybercrime Survey Report, 2015) states that 72% Companies of India have faced some sort of a cyberattack over the past year and 83% of the respondents said that there is external involvement in cyber-attacks cyber incidents have not only risen sharply in 2015, the trend is more towards cybercrime with financial motives. 61 percent respondents indicated that malware, and 41 per cent stated that social engineering, are the nature of cyber-attacks faced by companies. This report further states that potential

intentions/motives behind cyberattacks are illicit financial gain (65%), malicious damage to business operations (54%), use system for further attacks (30%), espionage by competitors (46%), act of war/ terrorism by other country (18%) and others (4%). The survey also states that as per 74% respondents, a detailed annual IT and cyber risk assessment is not carried out and furthermore 78% respondents stated that they do not have a cybercrime response plan, while 62% do not have a governance process to log or monitor IT events on their critical systems.

According to Global Economic Crime Survey 2016, the rapid changes in technology and the advent of the Internet of things (IoT), there has been a sharp increase in attack activity involving interconnected devices in the cloud and 56% of the Indian respondents felt that the risk of cybercrime had increased in the last two years, as compared to 53% globally. Moreover, as per 50% of the respondents the local law enforcement agencies are not adequately resourced and skilled to investigate the cybercrimes. (Global Economic Crime Survey 2016, An India Edition).

The total number of Internet users in India was 233,152,478 (18% of the total population) and estimated up to 354,114,747 (27% of the total population) by 2015. The number of Internet users has increased tenfold from 1999 to 2013. The first billion was reached in 2005, the second billion in 2010 and the third billion in 2014. Around 40% of the world population has an Internet connection today. (Internet Users by Country, 2017)

3. TYPES OF CYBERCRIME

Comprehensive Study on Cybercrime states that cybercrime cannot be described as a single definition, it is best considered as a collection of acts or conduct – these acts are based on the material offence object and modus operandi that affect computer data or systems. (Comprehensive Study on Cybercrime, 2013). Further, this study classified cybercrime acts in the following categories-

(A) Acts against the confidentiality, integrity and availability of computer data or systems

- Illegal access to a computer system
- Illegal access, interception or acquisition of computer data
- Illegal interference with a computer system or computer data
- Production, distribution or possession of computer misuse tools
- Breach of privacy or data protection measures

(B) Computer related acts for personal or financial gain or harm

- Computer related fraud or forgery
- Computer related identity offences
- Computer related copyright or trademark offences
- Sending or controlling sending of Spam
- Computer related acts causing personal harm
- Computer related solicitation or 'grooming' of children

(C) Computer content related acts

- Computer related acts involving hate speech
- Computer related production, distribution or possession of child pornography
- Computer related acts in support of terrorism offences

(D) Other Cyber Crime Acts

- computer-related tools for facilitating illegal acts related to financial instruments and means of payment
- online gambling
- use of an information technology device for the purposes of trafficking in persons
- computer-related drug trafficking
- computer-related extortion
- trafficking in passwords and
- access to classified information

4. METHODOLOGY

4.1. Purpose of the Study

The study aims to explore the trends of cybercrimes in India over the period 2004-2015. The purpose of this study is to investigate whether a relationship between the growth of Internet users and growth of cyber-crime exists. At the outset, the study undertakes a detailed examination of time pattern of incidences of cybercrime and growth of Internet usage in India.

4.2. Research Design

The scope of the study is to explore the cybercrime patterns in India over the period 2004-2015. The research design of the study is exploratory. The variables of the study were time (2004-2015), incidences of cybercrimes, number of Internet users over the period and penetration of Internet as a percent of total population of India.

The study relies on secondary data compiled from various published reports of National Crime Records Bureau (NCRB), Ministry of Home Affairs, Government of India, United Nations Statistical Division and International Telecommunication Union, United Nations. The data on incidences of case registered under cybercrime were taken from the publication of NCRB, viz. 'Crime in India' of the period 2004 to 2015. (Crime in India, 2004-2014) Number of Internet users was taken from Internet Live Stats (Internet Users by Country 2017).

5. RESULTS AND DISCUSSION

National Crime Records Bureau publishes crime data of India which is publicly available through its yearly publication viz. Crime in India. This data is based on the police recorded criminal cases on annual basis. From these publications, we downloaded the cybercrime data from Chapter 18 (Cyber Crimes) from 2004 to 2015, which includes cases under Information Technology Act, offences under related sections of IPC

and offences under Special and Local Laws (SLL). Particularly we downloaded the data regarding cases registered under cybercrime in states and union territories and Cases registered under cybercrimes by motives and suspects. We wanted to see the impact of growth of Internet (X) on incidences of cybercrime (Y). We assumed that with the growth of Internet users, the cybercrime incidences will also grow and will show some trend vis a vis time. Firstly, we drew scatter plot of the dependent variables viz. Incidences of Cyber Crime (Y) and Growth in number of Internet Users (X) against time. Through the scatter plot, it became evident that exponential fit would be the best for the data. Ignoring spatial variation, we used curve estimation feature of SPSS-20.0 to fit exponential curves for the variables Incidences of Cyber Crime (Y) and Growth in number of Internet Users (X) against time. The fit, and components of our model are shown in Figures 1 and 2. Our model fits the data quite well, suggesting that a large degree of variation in incidences of cybercrime rates and growth in Internet users is explained by long-term trends composed of an exponential trend. These initial results suggest that our model is well-suited to modeling long-term trends. We achieved full coverage with our 95% uncertainty forecasting intervals.

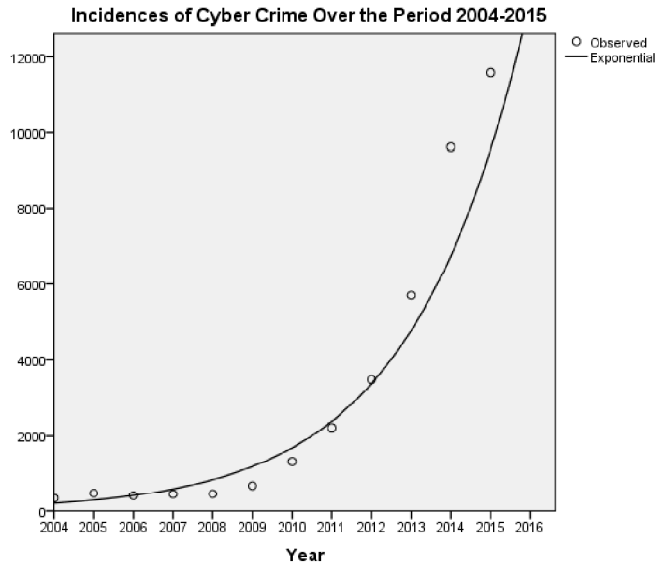

Figure 1

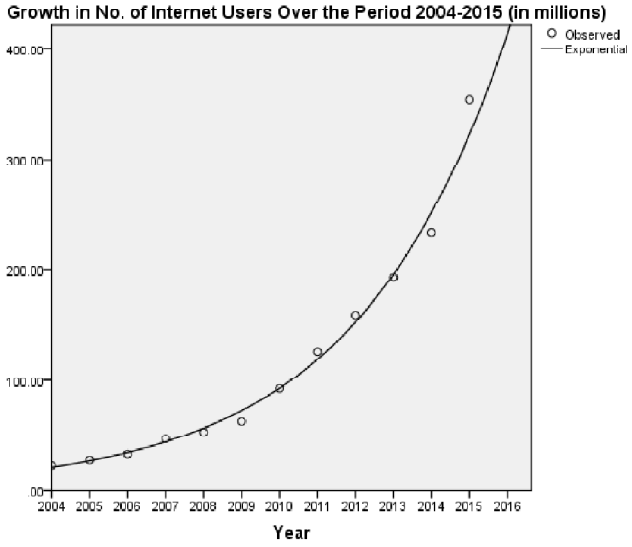

Figure 2

Further, R^2 (.921) for the incidences of cybercrime against time suggests that 92.1% variations in the incidences are explained by the change in time. Also, R^2 (.994) for the growth in number of Internet users against time suggests that 99.4 percent variations in the growth of Internet users are explained by change in time.

These results prompted us to study the relationship between incidences of cybercrime and growth in number of Internet users. We used linear regression analysis. The regression analysis is used because it helps to test on the relationship and the significance of relationship of two phenomena the dependent variable and independent variable. The following table tells about statistic of dependent and independent variables. Sig value shows the relationship between dependent and each independent variable. In accordance with Table 1 it is concluded that growth in number of Internet users have a significant effect on incidences of cybercrimes.

Table 1
Regression Results

Variables	*Coefficients*	*t*	*Sig.*
(Constant)	-1258.944	-2.780	.019
Number of Internet Users (X)	37.038	12.444	.000
R^2	.969	F-statistic	154.841
Adj. R^2	.939	Sig.	.000

The β (coefficient) value (37.038) is positive which shows that there is positive relationship between independent variable (Growth in number of Internet users X) and dependent variable (Incidences of Cyber Crime Y). Which shows that with every million rise in the number of Internet users that incidences of cybercrime will rise with an average of 37.

β value is used to form regression equation, which is:

Y = -1258.944 + 37.038 X

From t- statistics, there is overwhelming evidence to infer that there is a linear relationship between the independent variable (Growth in number of Internet users X) and dependent variable (Incidences of Cyber Crime Y).

From t – test we already know that there is evidence of a linear relationship. R^2 supplies us with a measure of the strength of that relationship. Adjusted R square shows adequacy of model with 0.939, that shows independent variables (Growth in number of Internet users X) can predict 93.9% of variance in dependent variable (Incidences of Cyber Crime Y). Further, F statistic shows that there is overwhelming evidence to infer that the regression model is valid.

6. CONCLUSION

In this study we tried to explore the patterns of cybercrimes in India using time series and regression analysis. Firstly, exponential curve was fitted in incidences of cybercrime data and growth in Internet users' data against time. This showed that the incidences of cybercrime and growth in Internet users both are growing exponentially. Further, an effort was made to find the relationship between incidences of cybercrime and growth in Internet users to confirm the patterns of cybercrimes in India for the period of 2004-2015 using regression analysis. This model can be used by law enforcement agencies and Ministry of Home Affairs to make infrastructural preparation for combating cybercrimes in future. In addition, it is hoped that this study would contribute to the future studies about time series and regression forecasting and could be of use for both researchers in this field.

REFERENCES

——(2013). *Comprehensive Study on Cybercrime.* Vienna: United Nations Office on Drugs and Crime. Retrieved December 21, 2016, from *https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf*

——(2004-2014). *Crime in India.* New Delhi: Natinal Crime Records Bureau. Retrieved December 28, 2016, from http://ncrb.nic.in/

(An India Edition). *Global Economic Crime Survey 2016*. PricewaterhouseCoopers. Retrieved January 20, 2016, from *https://www.pwc.in/assets/pdfs/publications/2016/pwc-global-economic-crime-survey-2016-india-edition.pdf*

Google: Internet users in India to touch 500 million by 2017. (2016, Febuary). Retrieved January 30, 2017, from Gadgets Now Beta: *http://www.gadgetsnow.com/tech-news/Google-Internet-users-in-India-to-touch-500-million-by-2017/articleshow/51077664.cms*

(2015). *Internet Society Global Internet Report.* Internet Society. Retrieved December 22, 2016, from *http://www.internetsociety.org/globalinternetreport/2015/assets/download/IS_web.pdf*

Internet Users by Country. (2017). Retrieved from Internet live stats: *http://www.internetlivestats.com/internet-users/india/*

(2015). *KPMG Cybercrime Survey Report.* Retrieved Febuary 1, 2017, from *https://assets.kpmg.com/content/dam/kpmg/pdf/2016/03/Cyber-Crime-Survey-2015.pdf*