AN OVERVIEW OF TOP STATES COMMITTED CYBER FRAUD IN INDIA

Dr.G.Ramesh Pandi ,Assistant Professor of Commerce,
Kalasalingam University, Krishnankoil,
Virudhunagar Dist. Tamilnadu
India

Mr.Sathrukkan Babu, Assistant Professor of Commerce,
MGR College, Hosur, Tamilnadu
India ,

Dr.M.Anbalagan,Assistant Professor of Commerce
Kalasalingam University, Krishnankoil,
Virudhunagar Dist.
Tamilnadu,

ABSTRACT

Cyber fraud or Cybercrime, or **computer crime**, is crime that involves a computer and a network. The computer may have been used in the commission of a crime, or it may be the target. Debarati Halder and K. Jaishankar define cybercrimes as: "Offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm, or loss, to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)". Such crimes may threaten a nation's security and financial health. Issues surrounding these types of crimes have become high-profile, particularly those surrounding hacking, copyright infringement, child pornography, and child grooming.

There are also problems of privacy when confidential information is intercepted or disclosed, lawfully or otherwise. Debarati Halder and K. Jaishankar further define cybercrime from the perspective of gender and defined 'cybercrime against women' as "Crimes targeted against women with a motive to intentionally harm the victim psychologically and physically, using modern telecommunication networks such as internet and mobile phones".

Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes. Activity crossing international borders and involving the interests of at least one nation state is sometimes referred to as cyber warfare. In India cyber crimes are increasing day by day.

STATEMENT OF THE PROBLEM

Recently the usage of technology is rapidly increasing in all the fields. Our central government is insisted the same through their programmes like digital India, e-commerce, etc., As a consequence, their crime rate is also increasing. It is our duty to find such crimes and take necessary precautionary steps to avoid cyber crimes. In this article the researchers try to analyse the cases registered and persons arrested under cyber crimes. Very rare articles are published in this field. This research gab is filled up by the researchers through this study.

OBJECTIVES OF THE STUDY

- To analyze the cyber crime cases registered
- To point out the measures taken by Indian government to reduce cyber crimes

TYPES OF CYBER CRIME

Cyber Crimes in India are registered under three broad heads, the IT Act, the Indian Penal Code (IPC) and other State Level Legislations (SLL). The cases registered under the IT Act include

- Tampering computer source documents (Section 65 IT Act)
- Loss /damage to computer resource/utility (Section 66 (1) IT Act)
- Hacking (Section 66 (2) IT Act)
- Obscene publication/transmission in electronic form (Section 67 IT Act)
- Failure of compliance/orders of Certifying Authority (Section 68 I T Act)
- Failure to assist in decrypting the information intercepted by Govt Agency (Section 69 IT Act)
- Un-authorised access/attempt to access to protected computer system (Section 70 IT Act)
- Obtaining licence or Digital Signature Certificate by misrepresentation / suppression of fact (Section 71 IT Act)
- Publishing false Digital Signature Certificate (Section 73 IT Act)
- Fraud Digital Signature Certificate (Section 74 IT Act)
- Breach of confidentiality/privacy (Section 72 IT Act)
- Others

On the other hand, cases are also registered under the IPC and those include

- Offences by/against Public Servant (Section 167, 172, 173, 175 IPC)
- False electronic evidence (Section 193 IPC)
- Destruction of electronic evidence (Section 204, 477 IPC)
- Forgery (Section 463, 465, 466, 468, 469, 471, 474, 476, 477A IPC)
- Criminal Breach of Trust (Section 405, 406, 408, 409 IPC)
- Counterfeiting Property Mark (Section 482, 183, 483, 484, 485 IPC)
- Tampering (Section 489 IPC)
- Counterfeiting Currency / Stamps (Section 489A to 489E IPC)
- Cyber Crimes up by more than 3 times in 5 years

CYBER CRIME CASES REGISTERED UNDER IT ACT

With increasing mobile and internet penetration in the country, cyber crimes have also increased proportionately. Between 2011 and 2015, more than 32,000 cyber crimes were reported across the country. More than 24,000 of these cases are registered under the IT Act and the remaining under the various sections of IPC and other State Level Legislations (SLL). The following table shows the statistical facts about cyber crimes.

TABLE 1
Cyber Crimes Registered under IT Act

Year	Cases Registered under IT Act	Increase / Decrease in Numbers	Increase / Decrease in Percentage
2011	1,791	-	-
2012	2,876	1085	60.58
2013	4,356	1,480	51.46
2014	7,201	2,845	65.31
2015	8,045	844	11.72

Source: https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/

Table 1 has explained the increase or decrease of the cyber crime cases registered under Information Technology Act. The annual increase in numbers ranged from 1,085 in 2012 to 844 in 2015. The increasing rate fell down to 11.72 per cent in 2015 from 60.58 per cent in 2012

TABLE 2

No. of Persons Arrested under IT Act

Year	Persons Arrested under IT Act	Increase / Decrease in Numbers	Increase / Decrease in Percentage
2011	1,184	-	-
2012	1,522	338	28.55
2013	2,098	576	37.84
2014	4,246	2,148	102.38
2015	5,102	856	20.16

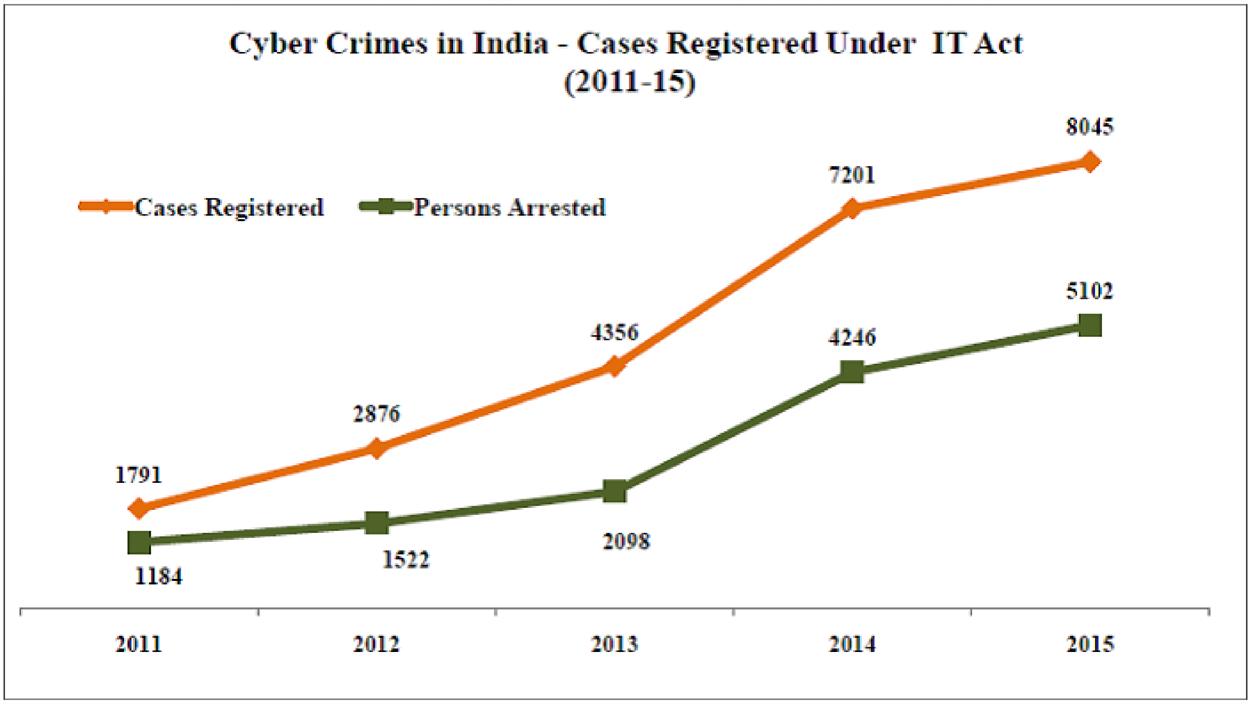
Source: https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/

Table 2 shows that the result of persons arrested for committed cyber crime under the IT Act. It reveals that maximizing or minimizing the persons arrested for cyber crime under the Information Technology Act. The annual rate is increased in quantitatively from 2,148 in 2014 to 856 in 2015. The growing rate fell down to 20.16 per cent in 2015 from 102.38 per cent in 2014.

CYBER CRIME IN INDIA – CASES REGISTERED AND ARRESTED UNDER IT ACT

The following chart explains the cases registered and arrested the persons those who involved in cyber crime under the Information Technology Act.

CHART 1



CYBER CRIME CASES REGISTERED UNDER IPC

Table 3
Cases Registered under IPC

Year	Cases Registered under IPC	Increase / Decrease in Numbers	Increase / Decrease in Percentage
2011	446	-	-
2012	601	179	42.42
2013	1,337	730	121.46
2014	2,272	935	69.93
2015	3,422	1,150	50.62

Source: https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/

Table 3 has highlighted the increase or decrease of the cyber crime cases registered under Indian Penal Code. The annual increase in numbers ranged from 730 in 2013 to 935 in 2014, 1,150 in 2015. But the increasing rate fell down to 50.62 per cent in 2015 from 121.46 per cent in 2013.

CYBER CRIME CASES – PERSONS ARRESTED UNDER IPC

Table 4
Persons Arrested under IPC

Year	Persons Arrested under IPC	Increase / Decrease in Numbers	Increase / Decrease in Percentage
2011	446	-	-
2012	549	103	23.09
2013	1,203	654	119.13
2014	1,224	21	1.75
2015	2,867	1,643	134.23

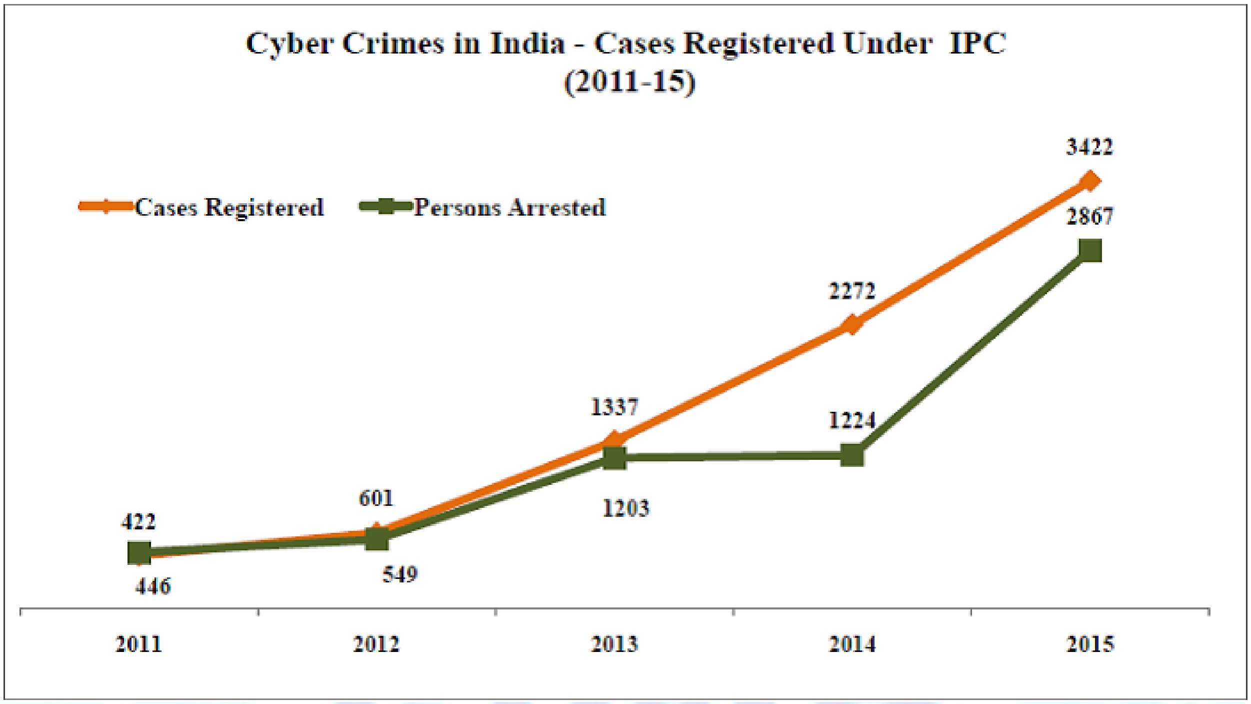
Source:https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/

One can understand from Table .4 that persons arrested for committed cyber crime under the Indian Penal Code. It reveals that maximizing or minimizing the persons arrested for cyber crime under the Indian Penal Code, the annual increase in quantitatively from 103 in 2012 to 1643 in 2015. The growing rate increased from 23.09 per cent in 2012 to 134.23 per cent in 2015.

CYBER CRIME IN INDIA – CASES REGISTERED AND ARRESTED UNDER IPC

The following chart shows the cases registered and arrested the persons those who involved in cyber crime under the Indian Penal Code.

CHART 2



TOP STATES COMMITTED CYBER FRAUD IN INDIA 2015

TABLE 5

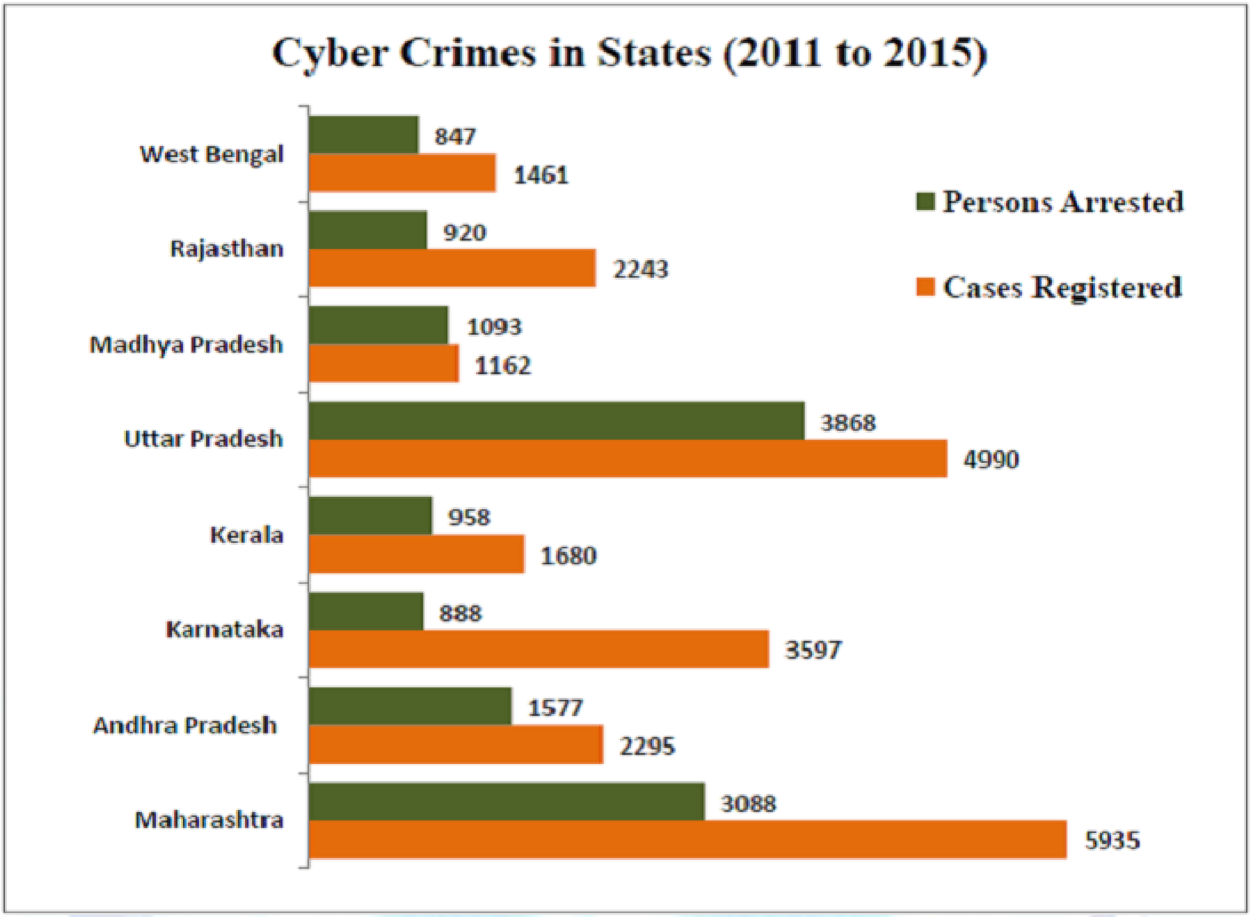
Top states Committed Cyber Fraud in India 2015

States	Cases Registered	Persons Arrested
West Bengal	1,461	847
Rajasthan	2,243	920
Madhya Pradesh	1,192	1,093
Utra Pradesh	4,990	3,868
Kerala	1,680	958
Karnataka	3,597	888
Andra Pradesh	2,295	1,577
Maharastra	5,935	3,088
Total	23,363	13,239

It is understood from Table 5 indicates that the various states of India involved in cyber crime in the period from 2011 to 2015 among the states , Maharashtra and Uttar Pradesh are the tops states involved in the cyber crime during above mentioned period.

The list of states with the highest incidence of cyber crime for the period 2011 to 2015 throws no surprises. Maharashtra tops the list with more than 5900 cases in the 5 years followed by Uttar Pradesh with close to 5000 such cases. Karnataka is third with more than 3500 cases. The top states in this list are the ones with a greater internet subscriber base. The bottom 10 is relatively smaller states with lower population & lower internet penetration. The results are shown in the following chart.

CHART 3



MEASURES TAKEN BY INDIAN GOVERNMENT

The government says that use of social media has also emerged as a key tool for committing cybercrimes and attacks that affect nation and society and is conscious of increase in cybercrimes. It has taken various steps in the form of awareness, training, legal framework, emergency response and implementation of best practices to prevent occurrence of such cyber crimes

In response to a question in the Lok Sabha, the government mentioned that the following measures are being taken to tackle cybercrimes.

- The Ministry of Home Affairs has issued an Advisory to the State Governments and Union Territory Administrations on Cyber Crime. The State Governments have been advised to build adequate technical capacity in handling cybercrime including technical infrastructure, cyber police stations and trained manpower for detection, registration, investigation and prosecution of cybercrimes.
- A major programme has been initiated on development of cyber forensics tools, setting up of infrastructure for investigation and training of the users, particularly police and judicial officers in use of this tool to collect and analyse the digital evidence and present them in Courts.
- Indian Computer Emergency Response Team (CERT-In) and Centre for Development of Advanced Computing (CDAC) are involved in providing basic and advanced training to Law

Enforcement Agencies, Forensic labs and judiciary on the procedures and methodology of collecting, analysing and presenting digital evidence.

- Cyber forensics training lab has been set up at Training Academy of Central Bureau of Investigation (CBI) to impart basic and advanced training in Cyber Forensics and Investigation of Cyber Crimes to Police Officers associated with CBI. In addition, Government has set up cyber forensic training and investigation labs in the States of Kerala, Assam, Mizoram, Nagaland, Arunachal Pradesh, Tripura, Meghalaya, Manipur and Jammu & Kashmir for training of Law Enforcement and Judiciary in these States.
- In collaboration with Data Security Council of India (DSCI), NASSCOM, Cyber Forensic Labs have been set up at Mumbai, Bengaluru, Pune and Kolkata for awareness creation and training programmes on Cyber Crime investigation. National Law School, Bangalore and NALSAR University of Law, Hyderabad are also engaged in conducting several awareness and training programmes on Cyber Laws and Cyber crimes for judicial officers.
- The Indian Computer Emergency Response Team (CERT-In) issues alerts and advisories regarding latest cyber threats and countermeasures on regular basis. CERT-In has published guidelines for securing the websites, which are available on its website (www.cert-in.org.in). CERT-In also conducts regular training programme to make the system administrators aware about secure hosting of the websites and mitigating cyber attacks.
- Government has decided to provide a centralized citizen portal through Crime and Criminal Tracking Network and Systems (CCTNS) for registering online cyber crime complaints. The Ministry of Home Affairs has also in-principle approved to set up an Indian Cyber Crime Coordination Centre (I4C) to fight against cyber crime in the country and establish an open platform for victims to raise cybercrime complaints with the protocol for resolution such as online crime reporting, to support and coordinate electronic investigations of cybercrime, assist the law enforcement agencies in criminal investigation etc.
- The cyber space is being closely monitored by the Government in respect of the situation of radicalization attempts. The Government has also directed the intelligence agencies to identify potential recruits and keep them under surveillance.

CONCLUSION

The cybercrime is a great threat to the human rights. The number of security attacks being designed to steal personal information is increasing with accelerating pace[7]. The attackers are targeting personal information to make a profit out of their operation and threatening the basic philosophy of 'right to live with dignity. So the Indian Government must tighten the technological security to avoid the cyber. The more number of cybercrime cells and police stations have also been created for detection and investigation of such crimes. A multi-pronged strategy is required to fight along with legal measures.

REFERENCES

1. Moore, R. (2005) "Cybercrime: Investigating High-Technology Computer Crime," Cleveland, Mississippi: Anderson Publishing.

2. Warren G. Kruse, Jay G. Heiser (2002). Computer forensics: incident response essentials. Addison-Wesley. p. 392. ISBN 0-201-70719-5.

3. Halder, D., & Jaishankar, K. (2011) Cybercrime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, PA, USA: IGI Global. ISBN 978-1-60960-830-9

4.Steve Morgan (January 17, 2016). "Cyber Crime Costs Projected To Reach $2 Trillion by 2019". Forbes. Retrieved September 22, 2016.1. http://riverdelfin.blogspot.in/2013/09/an-introduction-to-cyber-crime.html

5. "Cybercrime costs global economy $445 billion a year: report". Reuters. 2014-06-09. Retrieved 2014-06-17.

6. https://factly.in/cyber-crimes-in-india-which-state-tops-the-chart/

7.http://shodhganga.inflibnet.ac.in/bitstream/10603/66825/19/19_conclusion%20and%20suggestions.pdf