Cyber Security and Cyber Crimes in India

Project Report

Jaswinderpal Singh, Hitika, Jasmeen Sharma,
Kartik Setia, Kanishka Jaggi, Kajol
M.Sc. Statistics II Year - 2023
.
Under the Guidance of: Prof. Narinder Kumar
Department of Statistics, Panjab University, Chandigarh

23 March 2023

Contents

Chapter 1

Introduction

1.1 Cybersecurity

Cybersecurity refers to the practices and technologies used to protect computers, networks, and electronic data from unauthorized access, use, disclosure, disruption, modification, or destruction. It includes a range of security measures such as firewalls, encryption, intrusion detection and prevention systems, and incident response plans. The goal of cybersecurity is to secure and protect sensitive information, maintain the availability of critical systems, and ensure the integrity of data and communications. It also includes educating employees and users on safe practices to minimize human error.

1.2 Cyber Crimes

Cybercrime refers to any criminal activity that involves the use of computers, networks, or the internet. Examples include hacking, identity theft, phishing scams, and distributing malware etc.

Cyber crimes are a new class of crimes rapidly increasing due to extensive use of Internet and I.T. enabled services.

1.2.1 Major Cyber Crimes in India

Some major cyber crimes in India include:
1. *Hacking:* Unauthorized access to computer systems, networks, or websites to steal sensitive information or disrupt operations.
2. *Phishing:* Attempts to trick individuals into providing personal or financial information through fake emails or websites.
3. *Identity Theft:* Using someone else's personal information to commit fraud or other crimes.
4. *Fraud:* Using the internet to scam people out of their money or personal information.
5. *Cyberstalking:* Harassment or bullying through electronic means.
6. *Child pornography:* Using the internet to distribute or view child pornography.
7. *Ransomware:* A type of malware that encrypts a victim's files and demands payment to restore access.
8. *Crypto jacking:* Unauthorized use of someone's computer or device to mine cryptocurrency.
9. *Distributed Denial of Service (DDoS) attacks:* Overwhelming a website or network with traffic to make it unavailable.
10. *Spamming:* Sending unsolicited messages through email or other means.

These are some major cyber crimes reported in India, but there can be various other types of cyber-attacks that are emerging with technology advancements.

1.2.2 Biggest Recent Cyber Breaches in India:

AIIMS ransomware attack: what it means for health data privacy

Date: November 2022
Impact: 1.3 TB data encrypted and five servers affected in AIIMS ransomware attack

Details: As per the preliminary analysis, servers were compromised in the information technology network of the AIIMS by unknown threat actors due to improper network segmentation, which caused operational disruption due to

non-functionality of critical applications. CERT-In and other stakeholder entities have advised necessary remedial measures.
No specific amount of ransom was demanded by the hackers though a message was discovered on the server suggesting that it was a cyberattack.
Earlier, investigations into the cyberattack, which had crippled the functioning of the premier health institution in New Delhi, had revealed that "the IP addresses of two emails, which were identified from the headers of files that were encrypted by the hackers, originated from Hong Kong and China's Henan province".
The report said these two addresses, 'dog2398' and 'mouse63209', were generated in the first week of November in Hong Kong. Another encrypted file was sent from Henan in China.
Investigations also revealed that the targeted servers were infected with three ransomware: Wammacry, Mimikatz and Trojan.
Most of the functions of e-Hospital application such as patient registration, appointment, admission, discharge etc. had been restored after two weeks of the attack.

Air India data breach highlights third-party risk

Date: May 2021
Impact: personal data of 4.5 million passengers worldwide

Details: A cyberattack on systems at airline data service provider SITA resulted in the leaking of personal data of passengers of Air India. The leaked data was collected between August 2011 and February 2021, when SITA informed the airline. Passengers didn't hear about it until March, and had to wait until May to learn full details of what had happened. The cyber-attack on SITA's passenger service system also affected Singapore Airlines, Lufthansa, Malaysia Airlines and Cathay Pacific

CAT burglar strikes again: 190,000 applicants' details leaked to dark web

Date: May 2021

Impact: 190,000 CAT applicants' personal details

Details: The personally identifiable information (PII) and test results of 190,000 candidates for the 2020 Common Admission Test, used to select applicants to the Indian Institutes of Management (IIMs), were leaked and put up for sale on a cybercrime forum. Names, dates of birth, email IDs, mobile numbers, address information, candidates' 10th and 12th grade results, details of their bachelor's degrees, and their CAT percentile scores were all revealed in the leaked database.

The data came from the CAT examination conducted on 29 November 2020 but according to security intelligence firm CloudSEK, the same thread actor also leaked the 2019 CAT examination database.

Hacker delivers 180 million Domino's India pizza orders to dark web

Date: April 2021

Impact: 1 million credit card records and 180 million pizza preferences

Details: 180 million Domino's India pizza orders are up for sale on the dark web, according to Alon Gal, CTO of cyber intelligence firm Hudson Rock.

Gal found someone asking for 10 bitcoin (roughly $535,000 or Rs. 4 crore) for 13TB of data that they said included 1 million credit card records and details of 180 million Dominos India pizza orders, topped with customers' names, phone numbers, and email addresses. Gal shared a screenshot showing that the hacker also claimed to have details of the Domino's India's 250 employees, including their Outlook mail archives dating back to 2015.

Jubilant FoodWorks, the parent company of Domino's India, told IANS that it had experienced an information security incident, but denied that its customers' financial information was compromised, as it does not store credit card details. The company website shows that it uses a third-party payment gateway, PayTM.

Trading platform Upstox resets passwords after breach report

Date: April 2021

Impact: All Upstox customers had their passwords reset

Details: Indian trading platform Upstox has openly acknowledged a breach of know-your-customer (KYC) data. Gathered by financial services companies to confirm the identity of their customers and prevent fraud or money laundering, KYC data can also be used by hackers to commit identity theft.

On April 11, Upstox told customers it would reset their passwords and take other precautions after it received emails warning that contact data and KYC details held in a third-party data warehouse may have been compromised.

Upstox apologised to customers for the inconvenience, and sought to reassure them it had reported the incident to the relevant authorities, enhanced security and boosted its bug bounty program to encourage ethical hackers to stress-test its systems.

Police exam database with information on 500,000 candidates goes up for sale

Date: February 2021

Impact: 500,000 Indian police personnel

Details: Personally identifiable information of 500,000 Indian police personnel was put up for sale on a database sharing forum. Threat intelligence firm CloudSEK traced the data back to a police exam conducted on 22 December, 2019.

The seller shared a sample of the data dump with the information of 10,000 exam candidates with CloudSEK. The information shared by the company shows that the leaked information contained full names, mobile numbers, email IDs, dates of birth, FIR records and criminal history of the exam candidates.

Further analysis revealed that a majority of the leaked data belonged to candidates from Bihar. The threat-intel firm was also able to confirm the authenticity of the breach by matching mobile numbers with candidates' names.

This is the second instance of army or police workforce data being leaked online this year. In February, hackers isolated the information of army personnel in Jammu and Kashmir and posted that database on a public website.

COVID-19 test results of Indian patients leaked online

Date: January 2021

Impact: At least 1500 Indian citizens (real-time number estimated to be higher)

Details: COVID-19 lab test results of thousands of Indian patients have been leaked online by government websites.

What's particularly worrisome is that the leaked data hasn't been put up for sale in dark web forums, but is publicly accessible owing to Google indexing COVID-19 lab test reports.

First reported by BleepingComputer, the leaked PDF reports that showed up on Google were hosted on government agencies' websites that typically use *.gov.in* and *.nic.in* domains. The agencies in question were found to be located in New Delhi.

The leaked information included patients' full names, dates of birth, testing dates and centers in which the tests were held. Furthermore, the URL structures indicated that the reports were hosted on the same CMS system that government entities typically use for posting publicly accessible documents.

Niamh Muldoon, senior director of trust and security at OneLogin said: "What we are seeing here is a failure to educate and enable employees to make informed decisions on how to design, build, test and access software and platforms that process and store sensitive information such as patient records."

He added that the government ought to take quick measures to reduce the risk of a similar breach from reoccurring and invest in a comprehensive information security program in partnership with trusted security platform providers.

User data from Juspay for sale on dark web

Date: January 2021

Impact: 35 million user accounts

Details: Details of close to 35 million customer accounts, including masked card data and card fingerprints, were taken from a server using an unrecycled access key, Juspay revealed in early January. The theft took place last August, it said.

The user data is up for sale on the dark web for around $5000, according to independent cybersecurity researcher Rajshekhar Rajaharia.

BigBasket user data for sale online

Date: October 2020

Impact: 20 million user accounts

Details: User data from online grocery platform BigBasket is for sale in an online cybercrime market, according to Atlanta-based cyber intelligence firm Cyble.

Part of a database containing the personal information of close to 20 million users was available with a price tag of 3 million rupees ($40,000), Cyble said on November 7.

The data comprised names, email IDs, password hashes, PINs, mobile numbers, addresses, dates of birth, locations, and IP addresses. Cyble said it found the data on October 30, and after comparing it with BigBasket users' information to validate it, reported the apparent breach to BigBasket on November 1.

Unacademy learns lesson about security

Date: May 2020

Impact: 22 million user accounts

Details: Edutech startup Unacademy disclosed a data breach that compromised the accounts of 22 million users. Cybersecurity firm Cyble revealed that usernames, emails addresses and passwords were put up for sale on the dark web.

Founded in 2015, Unacademy is backed by investors including Facebook, Sequoia India and Blume Ventures.

Hackers steal healthcare records of 6.8 million Indian citizens

Date: August 2019

Impact: 68 lakh patient and doctor records

Details: Enterprise security firm FireEye revealed that hackers have stolen information about 68 lakh patients and doctors from a health care website based in India. FireEye said the hack was perpetrated by a Chinese hacker group called Fallensky519.

Furthermore, it was revealed that healthcare records were being sold on the dark web – several being available for under USD 2000.

Local search provider JustDial exposes data of 10 crore users

Date: April 2019

Impact: personal data of 10 crore users released

Details: Local search service JustDial faced a data breach on Wednesday, with data of more than 100 million users made publicly available, including their names, email ids, mobile numbers, gender, date of birth and addresses, an independent security researcher said in a Facebook post.

SBI data breach leaks account details of millions of customers

Date: January 2019

Impact: three million text messages sent to customers divulged

Details: An anonymous security researcher revealed that the country's largest bank, State Bank of India, left a server unprotected by failing to secure it with a password.

The vulnerability was revealed to originate from 'SBI Quick' – a free service that provided customers with their account balance and recent transactions over SMS. Close to three million text messages were sent out to customers.

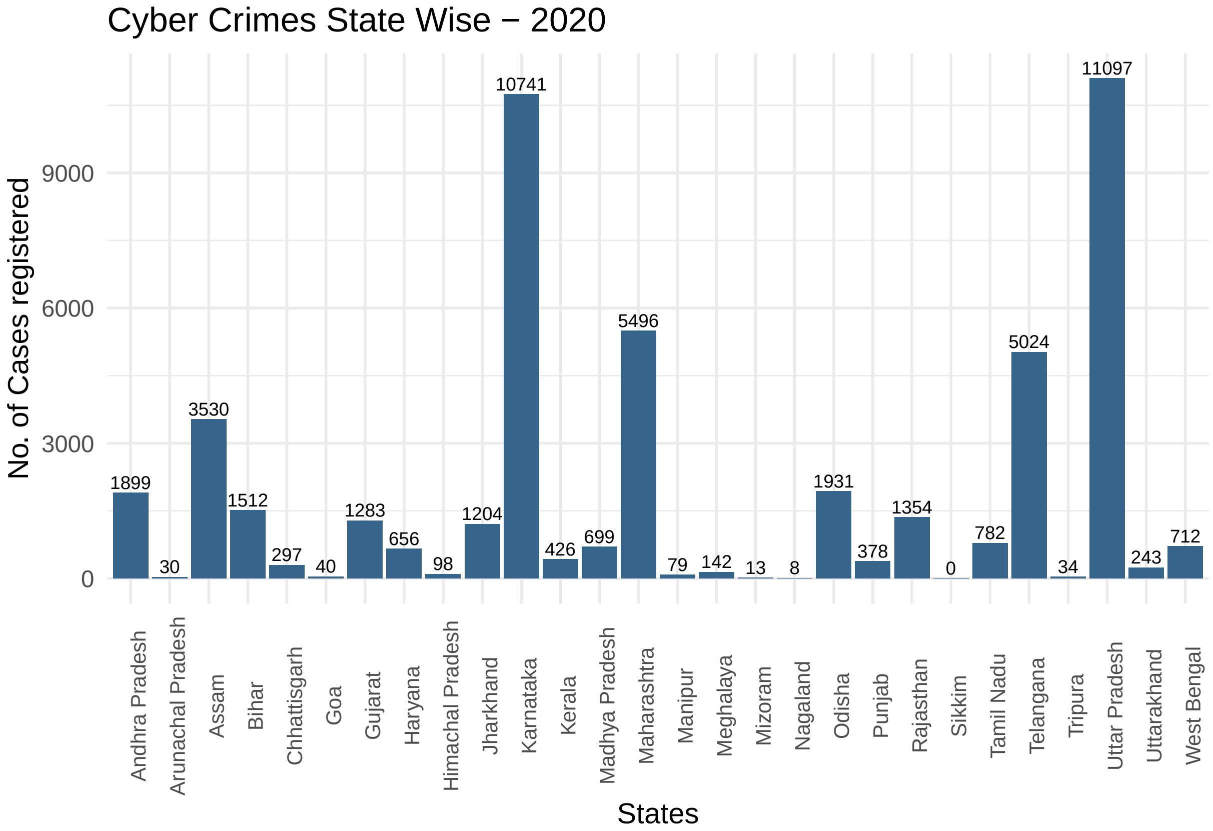
Chapter 2

Cyber Crimes in India: Statistics and Data Visualization

2.1 Cyber Crimes State-Wise:

2.1.1 Year 2020

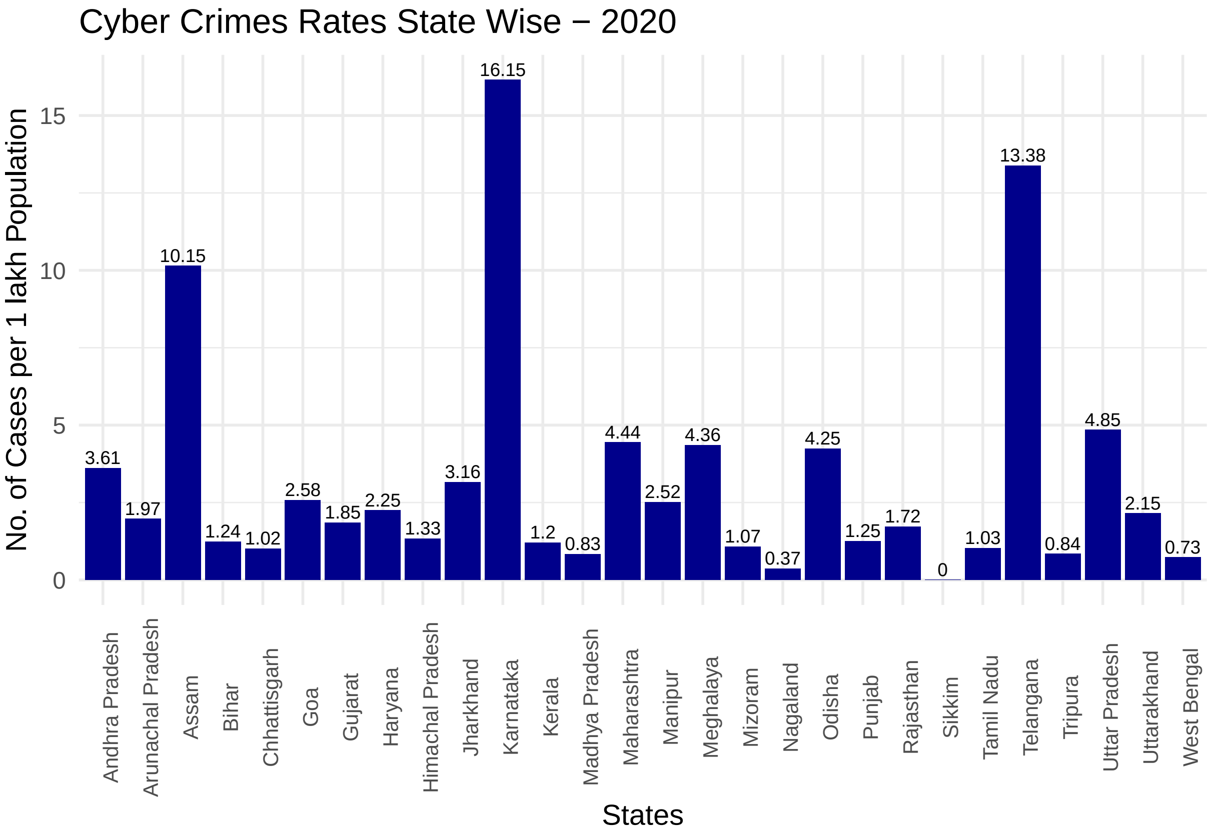
```
rm(list = ls())
source("viz2021.R")

barst2020
```



The above figure shows the highest number of cases being registered in Uttar Pradesh, followed by Karnataka, Maharashtra and Telangana. But one must note that the population in these states may vary. So to get a better comparison, rates can be calculated, which gives the cyber crime cases registered in the state per 1 lakh population. Mid year projected population for each state for the year 2021 is available. Hence the Cyber Crime Rate can be calculated as:

$$Rate = \frac{No.\,of\,cases\,registered}{Mid\,year\,projected\,population\,(in\,lakhs)}$$

```
barst2020r
```



As far as the rates are concerned, Karnataka and Telangana emerged as the states with highest cyber crime rates followed by Assam, Uttar Pradesh and Maharashtra.

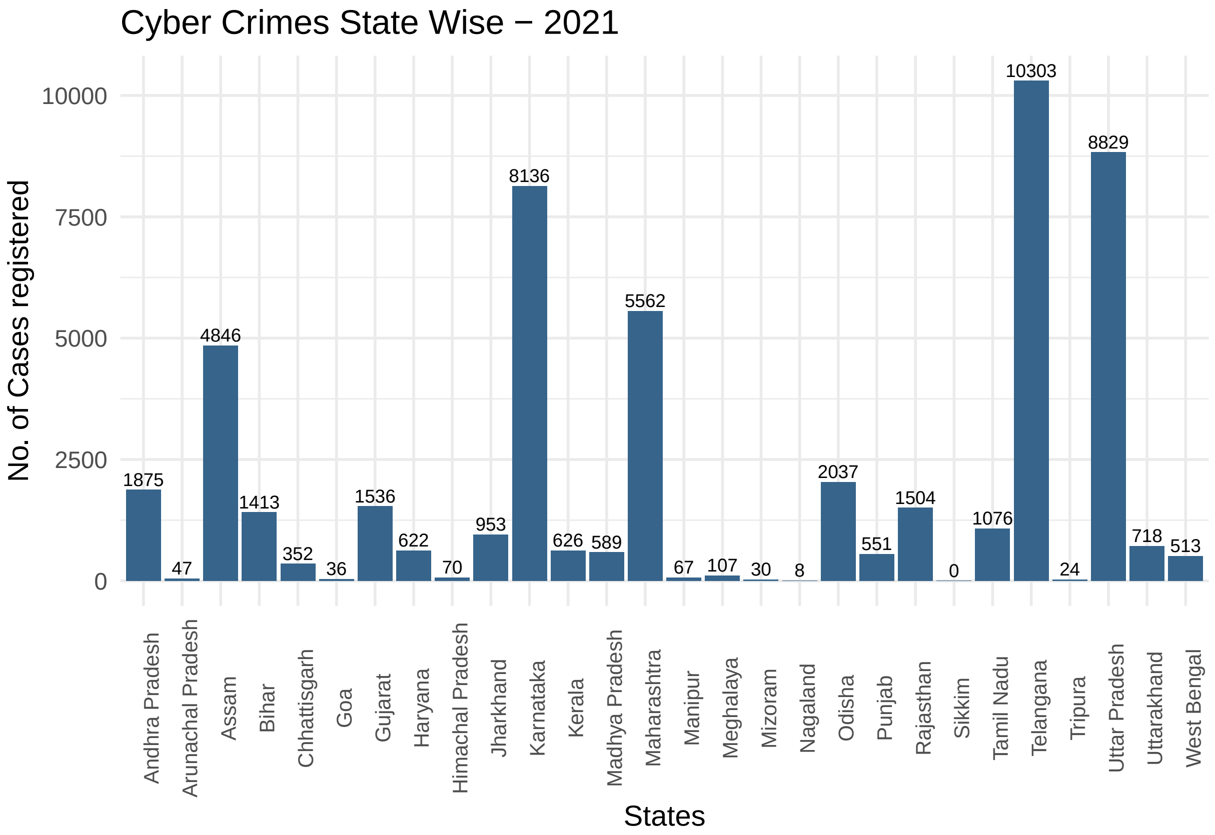
```
major_states20 = df$cases_reg2020[ which(df$state %in% c("Telangana", "Assam",
                                  "Uttar Pradesh", "Karnataka", "Maharashtra") ) ]
sum(major_states20)/df[40,4]
```

```
## [1] 0.7172579
```

The above value indicates that almost 71.72579 % of the total cyber crimes reported in the country India in 2021 came only from the five states: Telangana, Uttar Pradesh, Karnataka, Maharashtra and Assam.

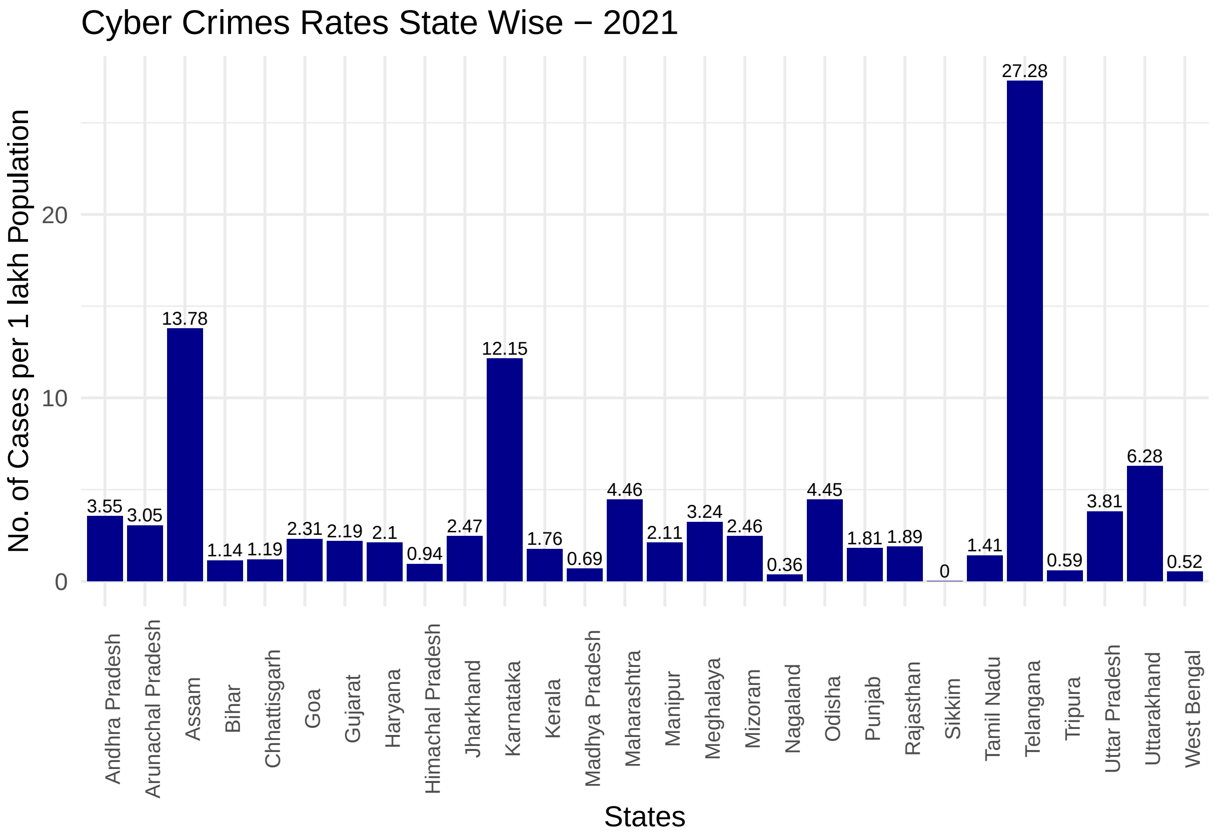
2.1.2 Year 2021

```
barst2021
```



From the above figure it looks like Telangana tops the Cyber Crimes tally followed by Uttar Pradesh and Karnataka in 2021. But for better comparison, let us see the Cyber Crime Rates, i.e. Cyber Crimes in a State per 1 lakh population.

```
barst2021r
```



Now, from here it is evident that infact Telangana is the state with highest cyber crime rate of 27.28 cases per 1 lakh population, followed by Assam and Karnataka with rates 13.78 and 12.15 respectively.

```
major_states21 = df$cases_reg2021[ which(df$state %in% c("Telangana", "Assam",
                             "Uttar Pradesh", "Karnataka", "Maharashtra") ) ]
sum(major_states21)/df[40,5]
```

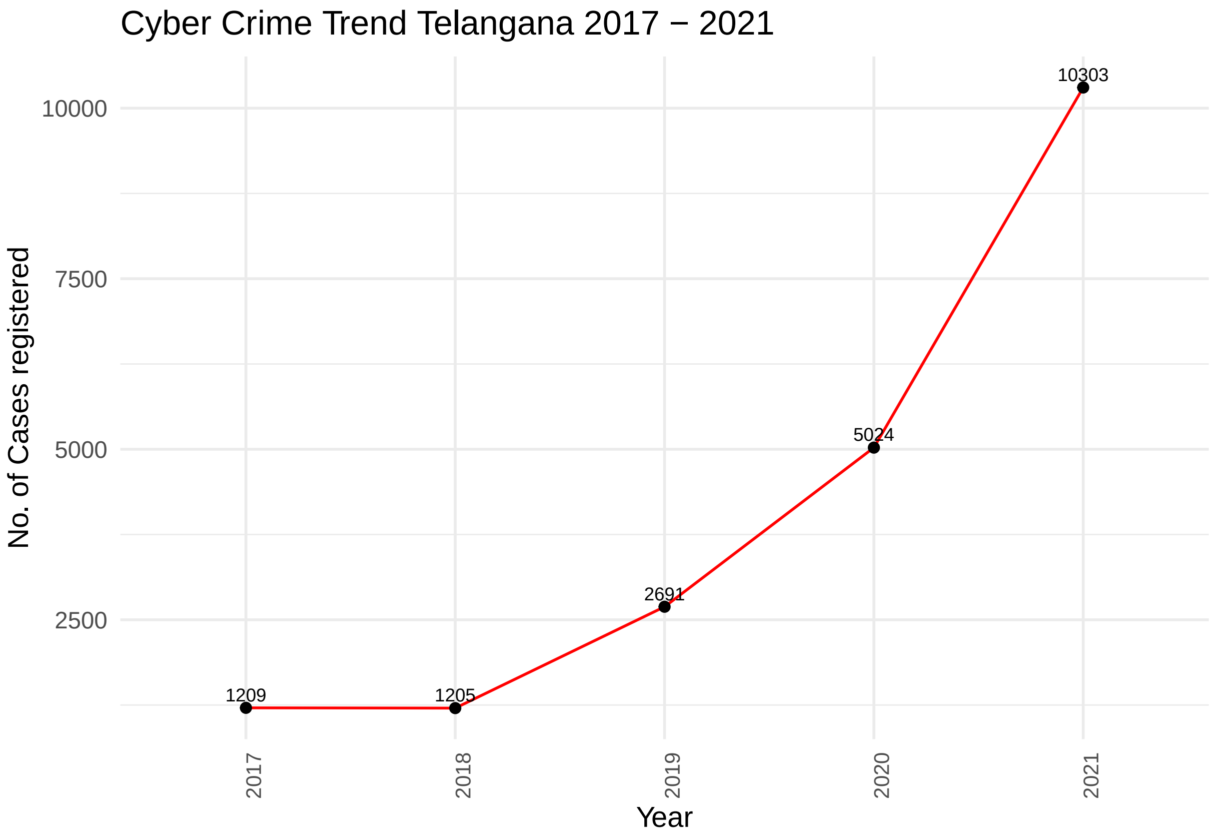
```
## [1] 0.7112168
```

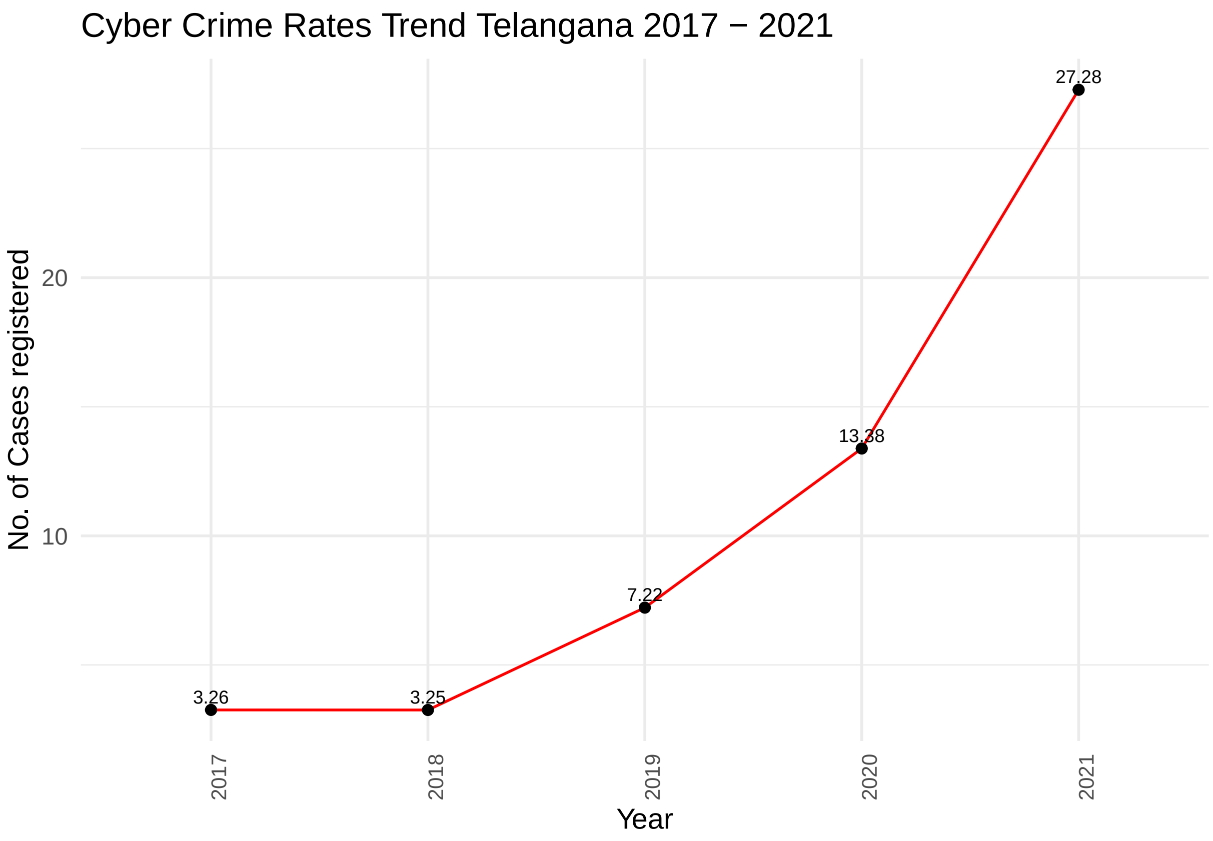
The above value indicates that almost 71.12168 % of the total cyber crimes reported in the country India in 2021 came only from the five states: Telangana, Uttar Pradesh, Karnataka, Maharashtra and Assam. However, they together contributed almost 36% of the Indian Population

These States can be analyzed further based on last 5 years as follows:

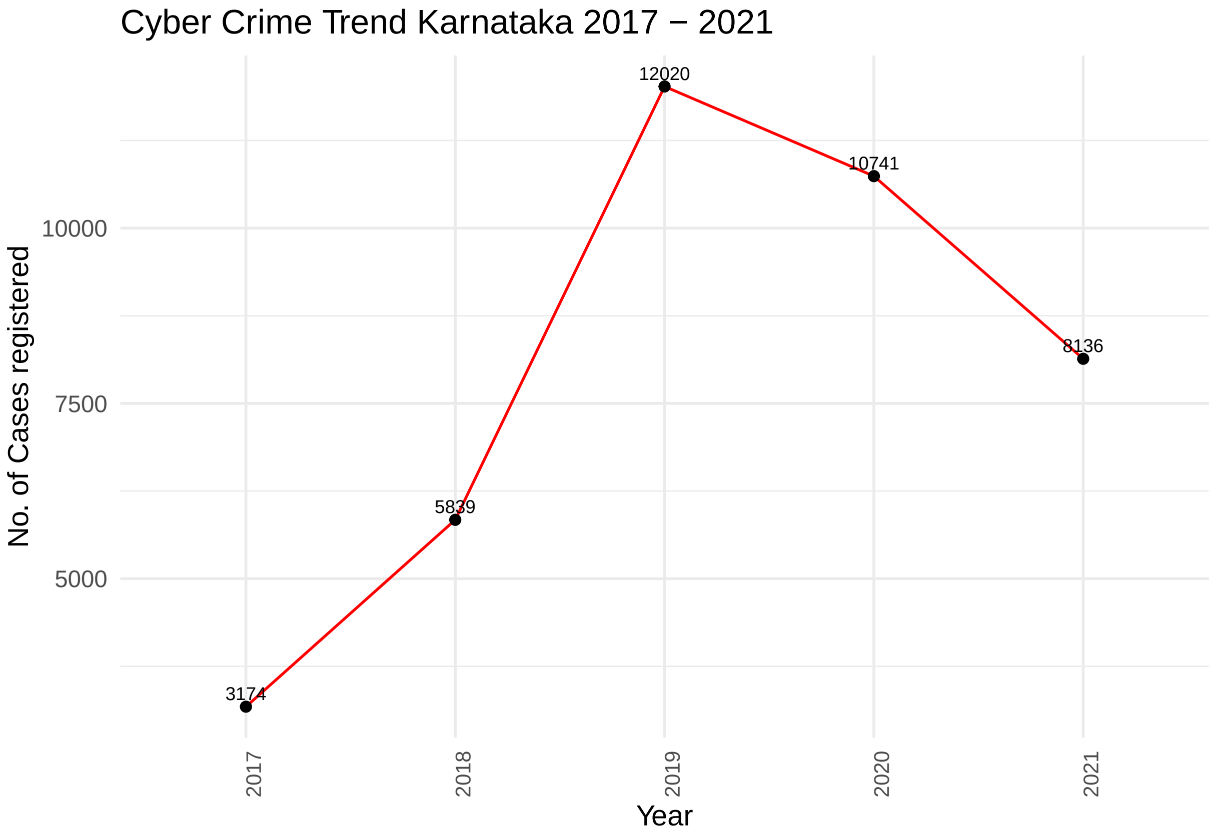
```
j = 1
for (i in statelist) {
  cat("\n",nam[j],"\n")
  show(trend_plot(i,  paste("Cyber Crime Trend",nam[j],"2017 - 2021"), i$cases) )
  cat("\n")
  show(trend_plot(i,  paste("Cyber Crime Rates Trend",nam[j],"2017 - 2021"), i$rates) )
  cat("\n")
  j = j+1
}
```

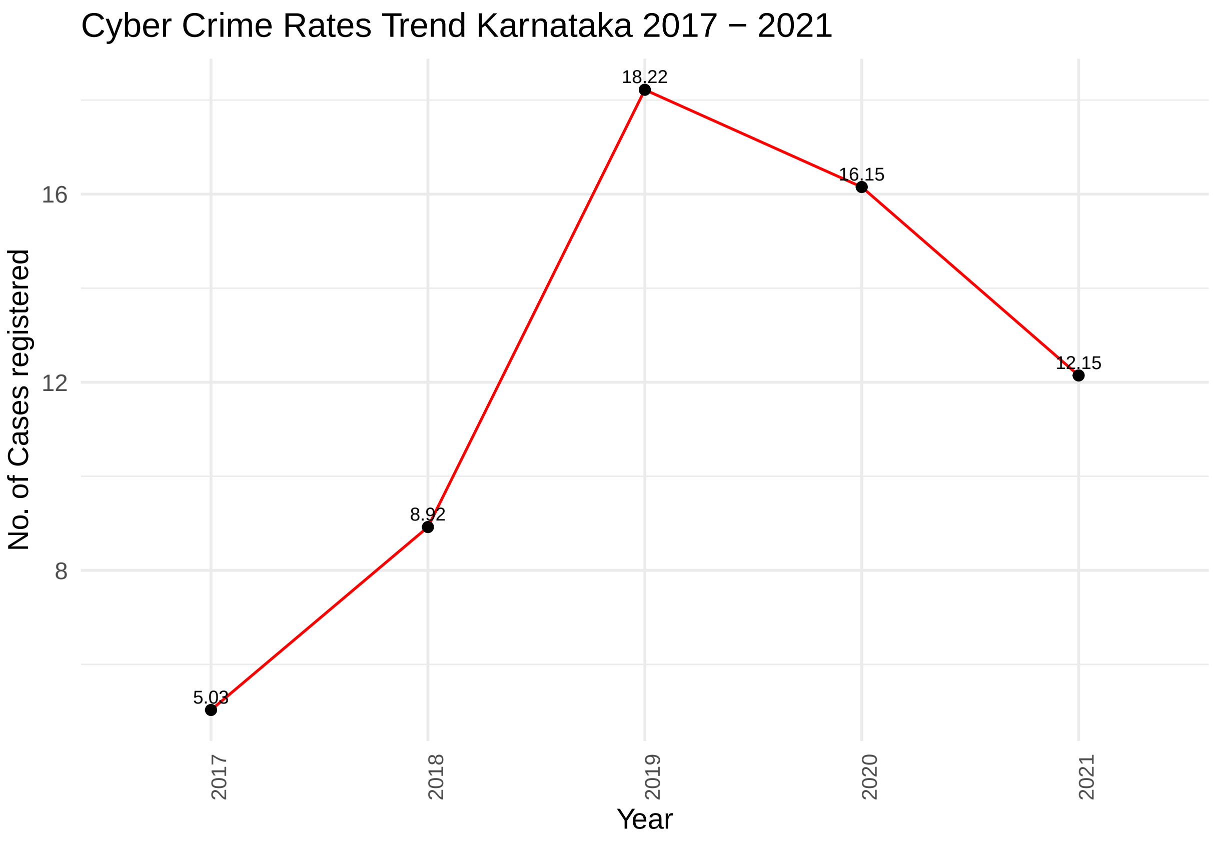
```
##
##  Telangana
```



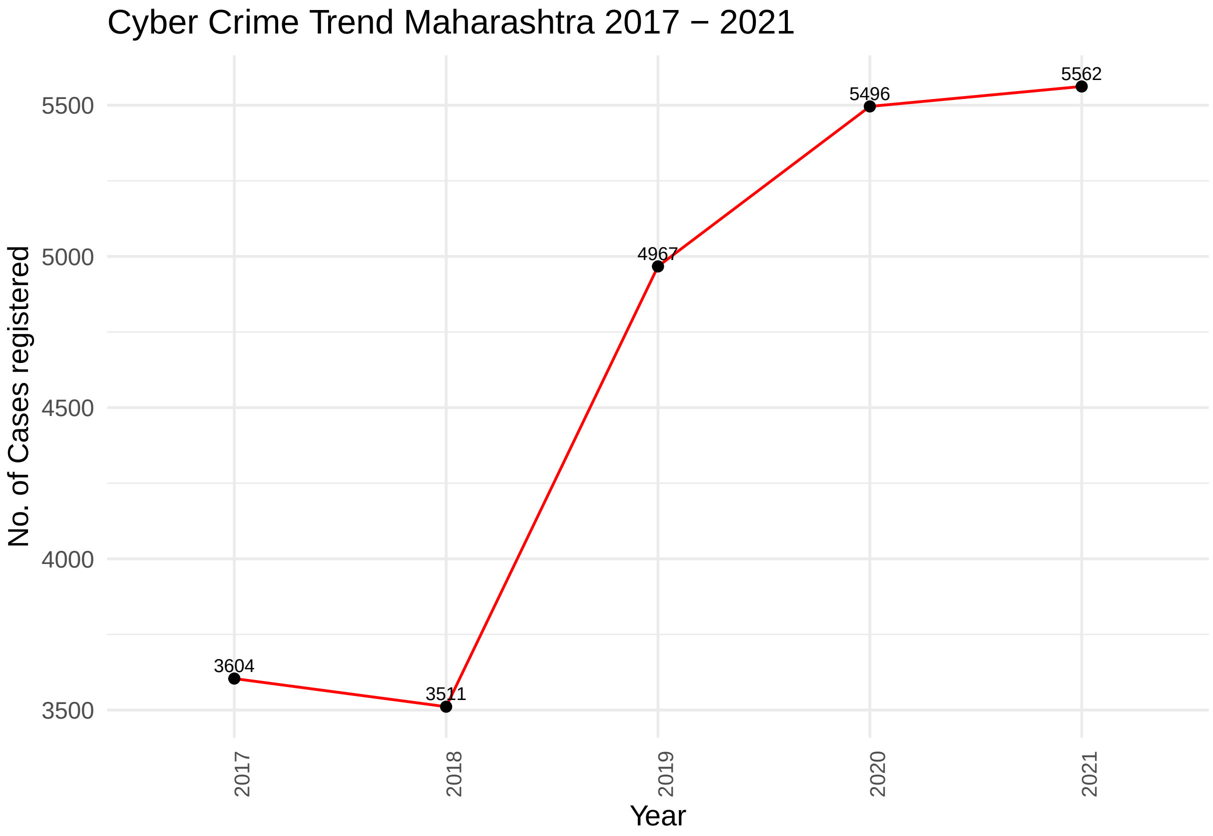

Cyber Crime Rates Trend Telangana 2017 − 2021
No. of Cases registered
Year
10
20
2017
2018
2019
2020
2021
3.26
3.25
7.22
13.38
27.28

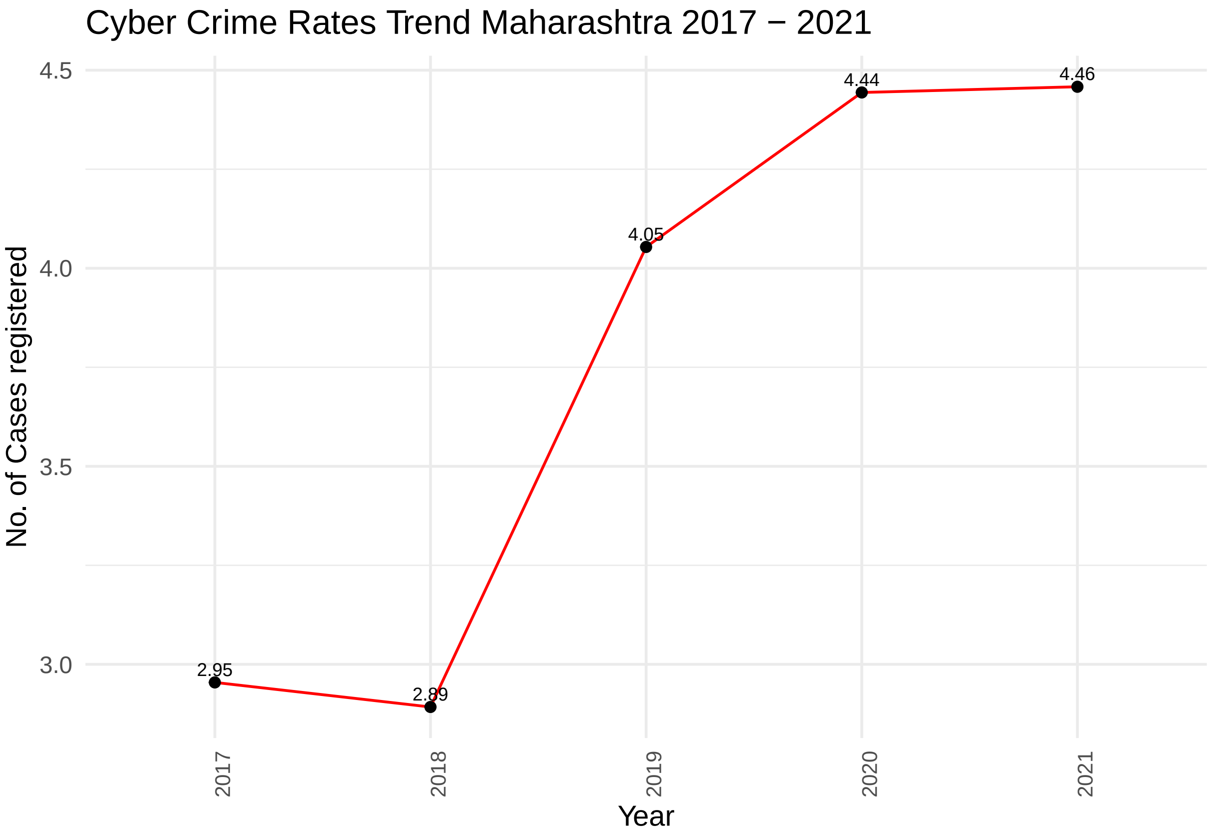
```
##
##
## Karnataka
```


Cyber Crime Trend Karnataka 2017 − 2021
No. of Cases registered
Year
5000
7500
10000
2017
2018
2019
2020
2021
3174
5839
12020
10741
8136

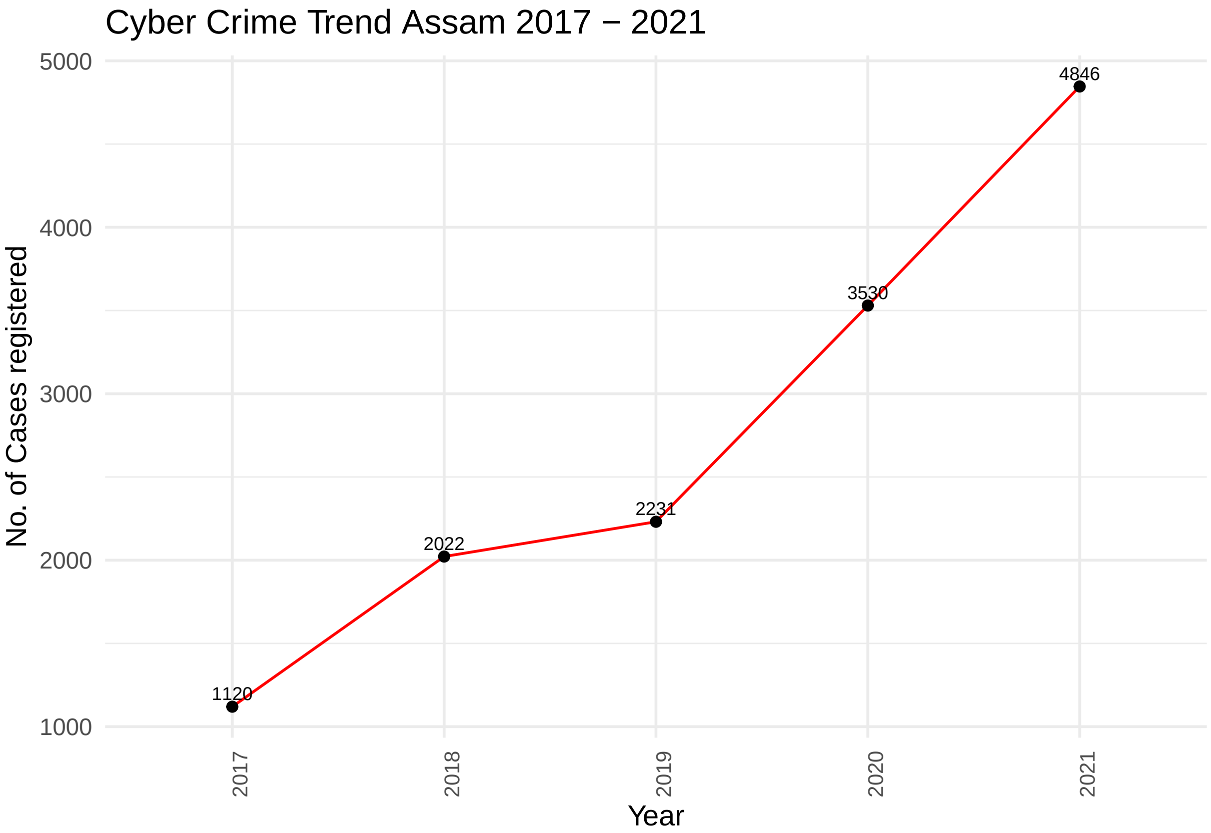


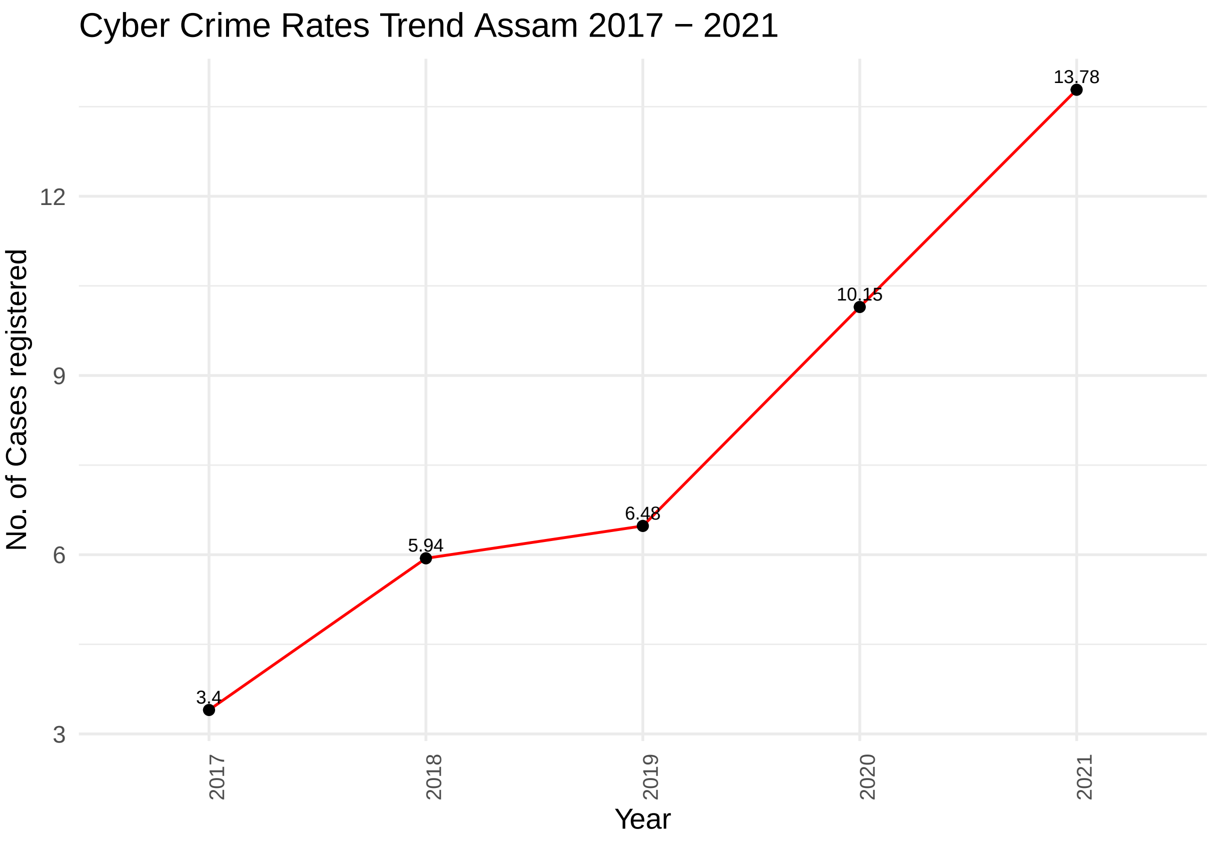
```
##
##
##  Maharashtra
```



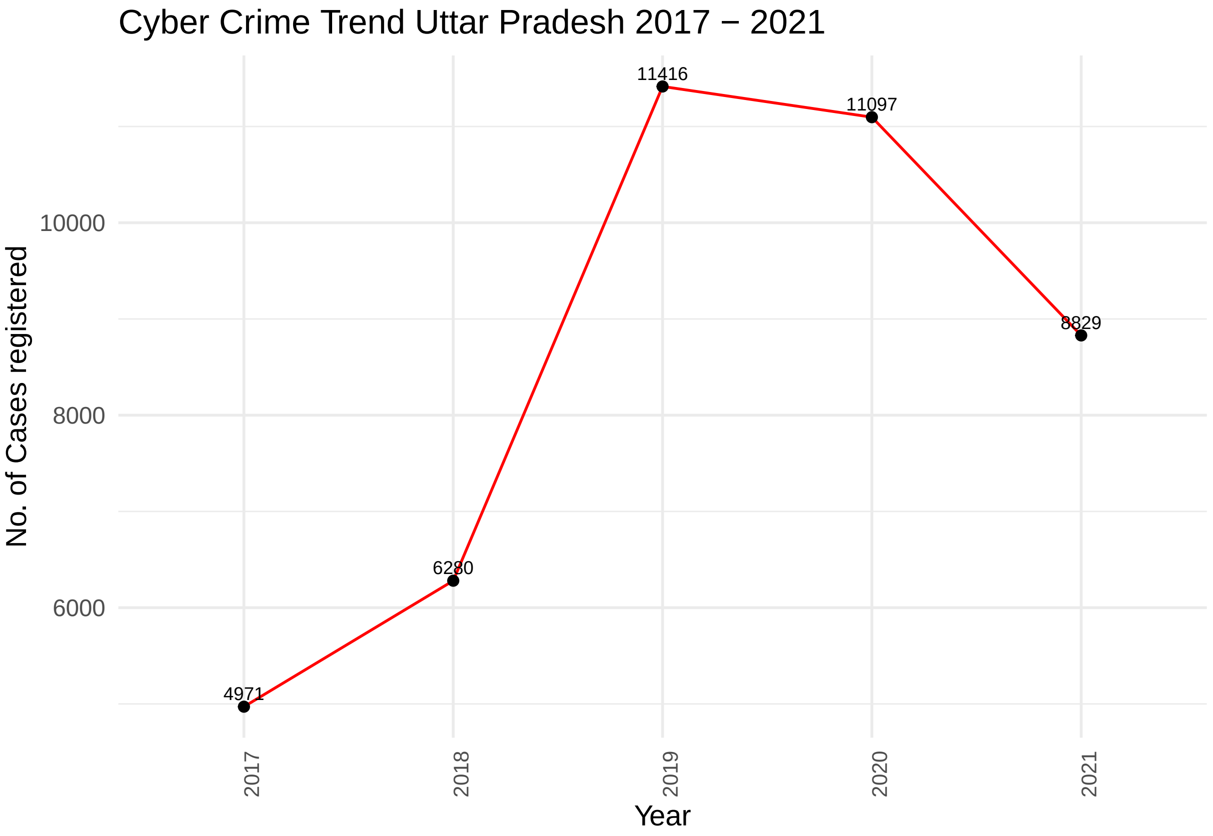

Cyber Crime Rates Trend Maharashtra 2017 − 2021
4.5
4.0
3.5
3.0
No. of Cases registered
2.95
2.89
4.05
4.44
4.46
2017
2018
2019
2020
2021
Year

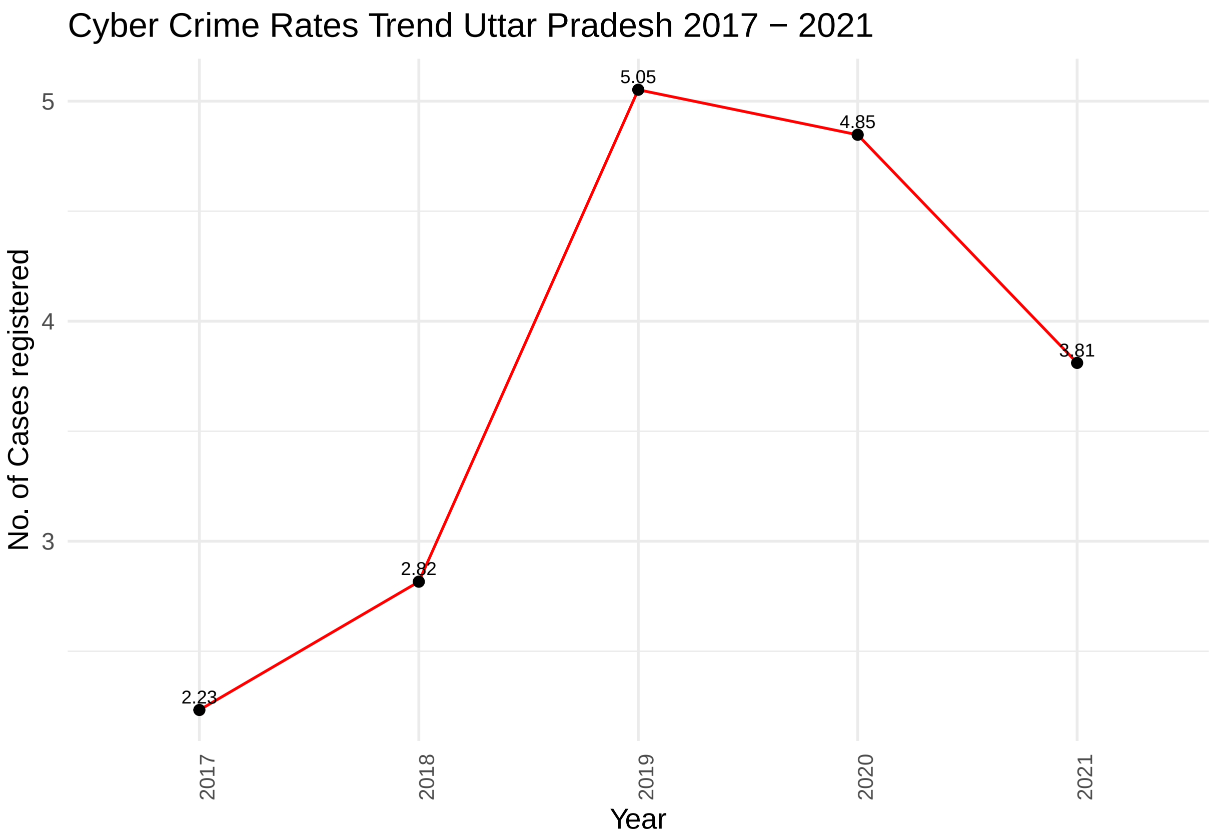
```
##
##
##  Assam
```


Cyber Crime Trend Assam 2017 − 2021
5000
4000
3000
2000
1000
No. of Cases registered
1120
2022
2231
3530
4846
2017
2018
2019
2020
2021
Year



```
##
##
##  Uttar Pradesh
```



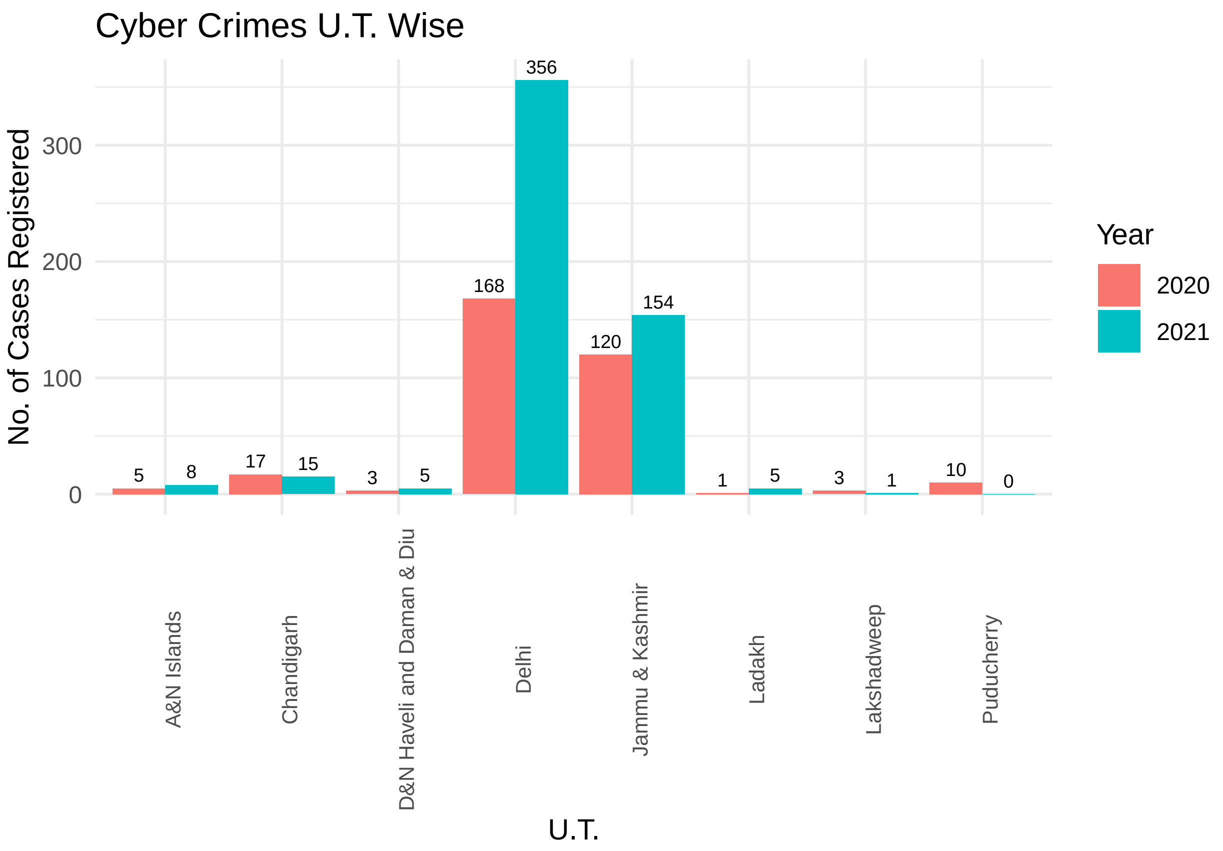


Now, it is evident from that the states of Assam and Telangana are showing rapid increasing trend in Cyber Crimes over the last 5 years. However, Uttar Pradesh and Karnataka are registering some lesser number of cases as compared to previous years. The state of Maharashtra is slowly registering more number of cases as compared to previous years.

2.2 Cyber Crimes U.T. - wise

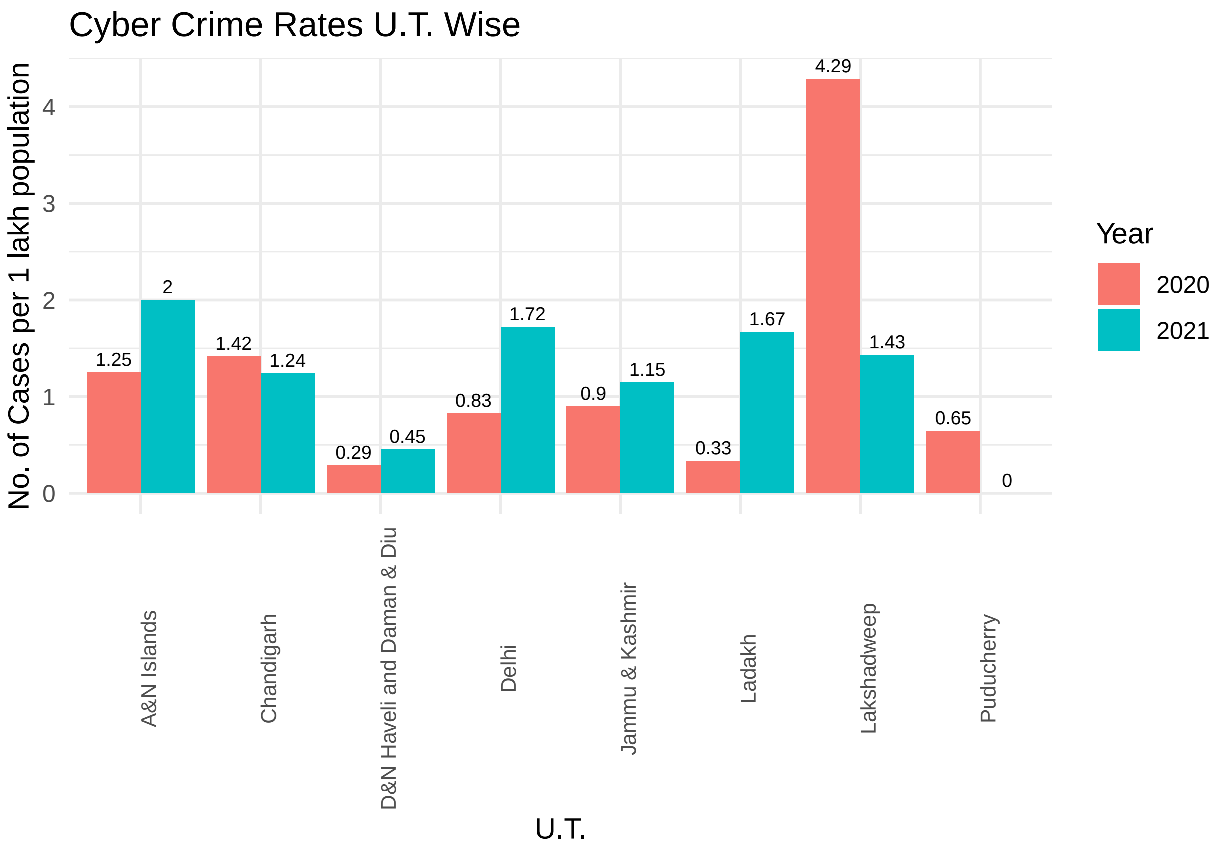
Further, Similar things can be analyzed for the Union Territories also.

```
barut2020_21
```



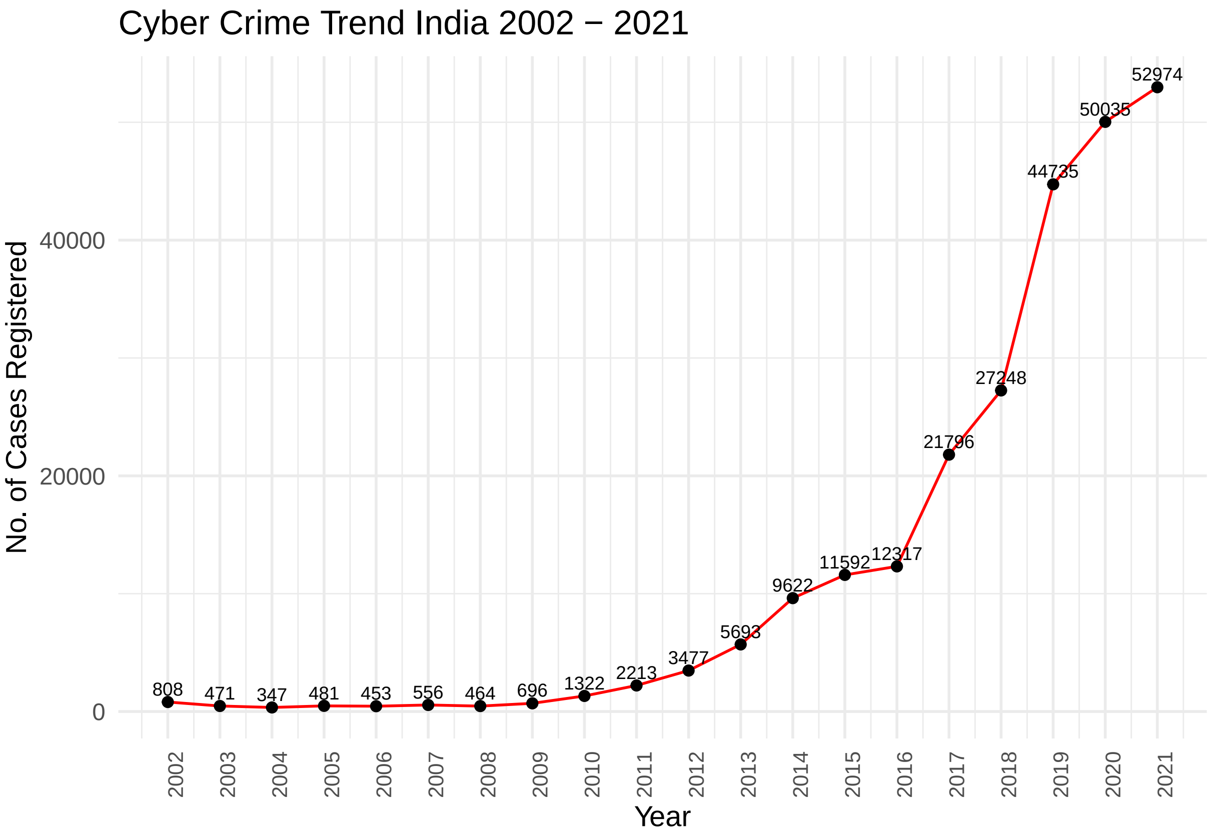
In terms of numbers, the Union Territory of Delhi registered the most 356 cyber crime cases in 2021, followed by Jammu&Kashmir and Chandigarh with 154 ans 15 cases respectively. Also, **the cases in Delhi are more than double in 2021 from 2020.** However, in terms of rates, the picture is somewhat like this in all the Union Territories:

```
barut2020_21r
```



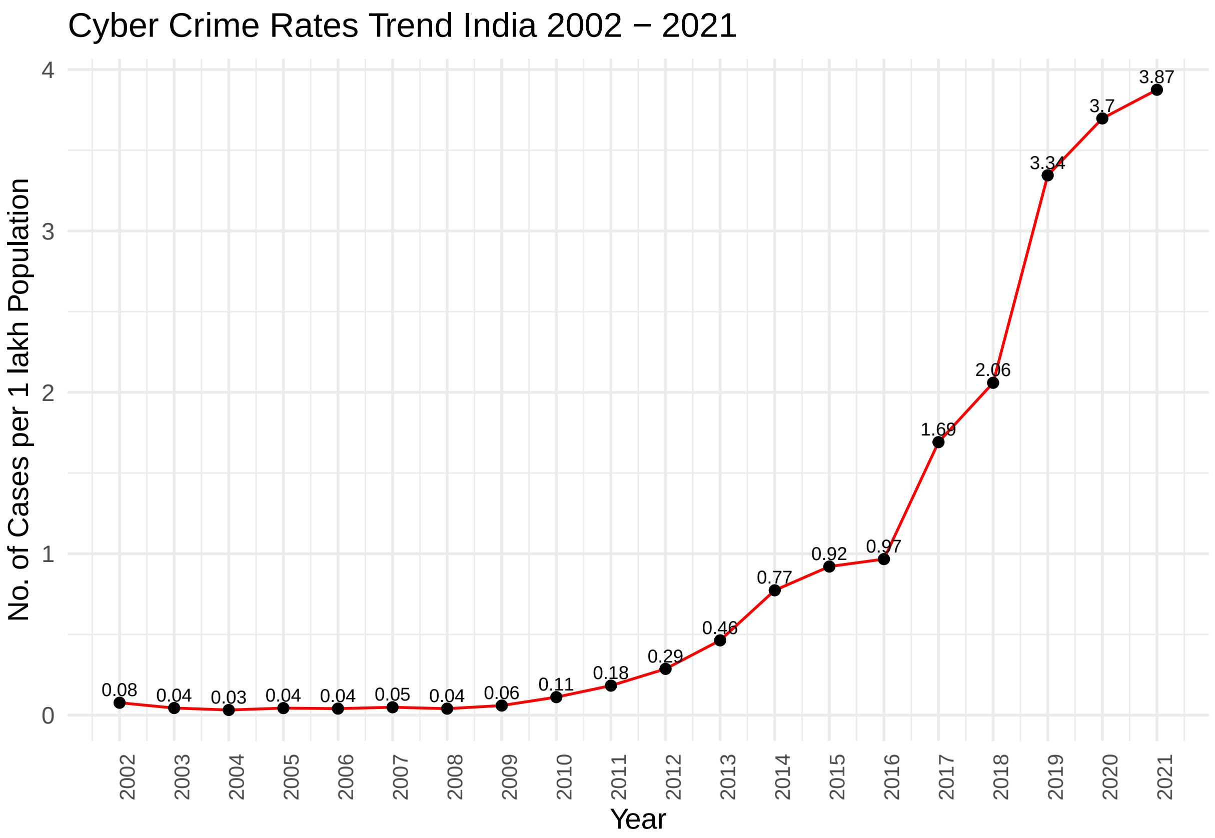
2.3 Cyber Crime Trend India

```r
source("cybertrend.R")
cyber_trend
```



Also, Mid-Year Projected Population of India for each year is available, hence in terms of rates:

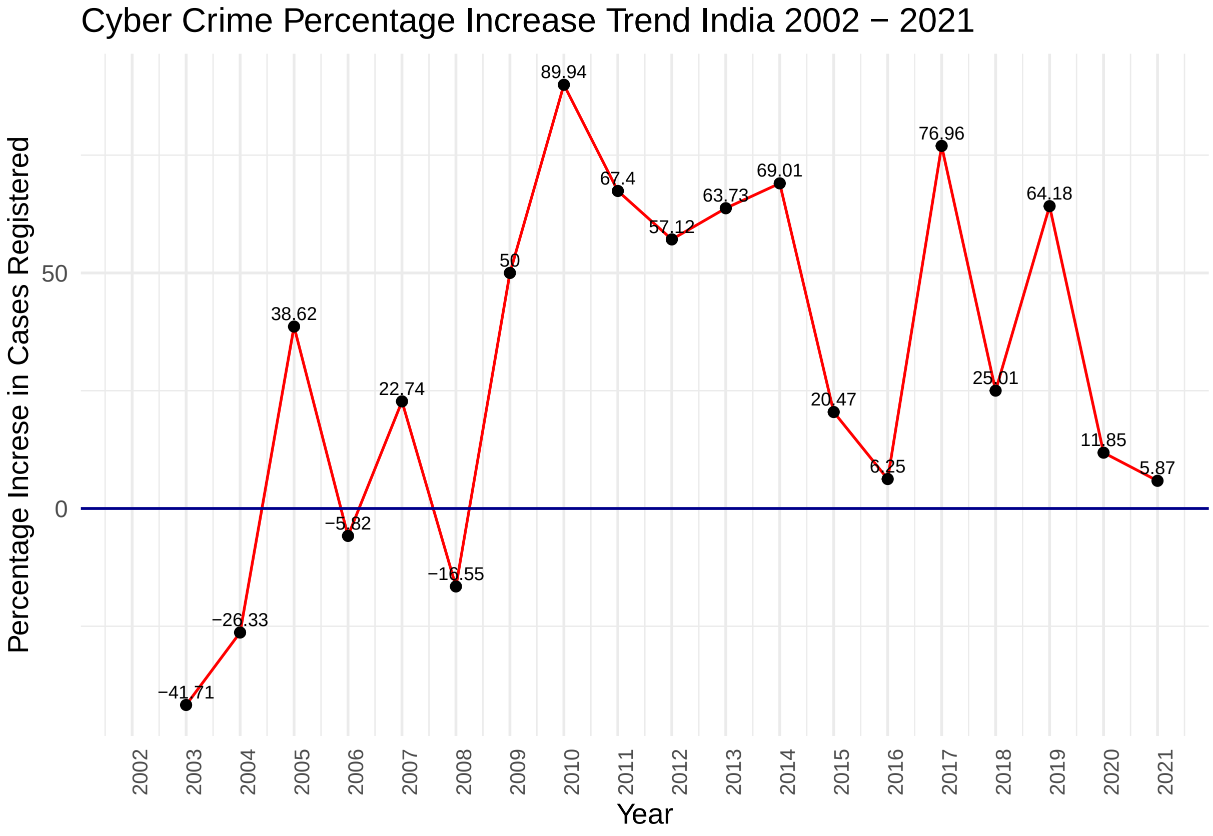
```r
cyber_trendr
```



To get a more clear idea about the previous year comparison, percentage increase in the cases can be calculated using the formula:

$$Percentage\ Increase = \frac{Current\ Value - Previous\ Value}{Previous\ value} * 100$$

```
cyber_trendp
```


Cyber Crime Percentage Increase Trend India 2002 − 2021
Percentage Increse in Cases Registered
50
0
Year
2002
2003
2004
2005
2006
2007
2008
2009
2010
2011
2012
2013
2014
2015
2016
2017
2018
2019
2020
2021
−41.71
−26.33
38.62
−5.82
22.74
−16.55
50
89.94
67.4
57.12
63.73
69.01
20.47
6.25
76.96
25.01
64.18
11.85
5.87