International Journal of Leading Research Publication (IJLRP)
E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

"Telangana Police: Forefront in Cybercrimes Resilience"

S. Ravi Chandra[1]
Deputy Superintendent of Police (Dy SP),
Police Computer Services and Standardization (PCSS)
DGP office, Lakadikapool, Hyderabad, Telangana

Prof. S.V.M. Kama Sai[2]
Professor of law
KL University, Vijayawada, Andhra Pradesh.

Manda Buchi Ramulu[3]
Police Computer Services and Standardization (PCSS)
DGP office, Lakadikapool, Hyderabad, Telangana

Abstract:
Technology has touched many spheres of our lives all over the world. Today, it is part and parcel of business, education, banking, agriculture, communication, medicine, government, private services, and other sectors that make people's lives easier. On the other hand, it has simultaneously led to an increased threat of online crimes, in particular cyber fraud. Cyber criminals are posing a challenge/hazard to the economic and security system of our country. According to the "Indian Cyber Threat Report-2025," India is facing 11 cybercrimes every second. The NCRB report 2022 reported 65,893 (28 states and 8 UTs) cases, and SCRB 24,643 (till November 2024) were registered under cybercrimes/cyber fraud, respectively. Telangana state is in the top three states (Karnataka, Maharashtra) in registering cybercrime cases in the last three years. In this situation, Telangana police extensively use technology and SMART Policing to reach the expectations of the police and people to provide law & order and justice. This article tries to throw light on how the Telangana police resist the national and international cyber criminals with the objective of a crime-free society.

Keywords: Cybercrimes, technology, Online transactions, Cyber stalking, Phishing attacks, pharming, Carding, etc.

I. Induction to Cyber Crimes:

The objective of technology innovation is always the betterment of human life. It is the misuse of technology that has a detrimental effect in multiple ways. A crime which involves a Personal Computer (PC) and an internet connection is known as a Cybercrime. Cyber-crime combines the term "Crime" and "Cyber", which comes from the Greek word "kubernan", which means to 'lead' or to 'govern'.[1]

Cyber stalking, Phishing attacks, pharming, Carding, Identity theft, theft of confidential information, intellectual property theft, financial fraud, extortion, cyber warfare, cyber espionage (hacking), etc., are several prevalent cybercrimes. The scourge of cyber fraud is plaguing the netizens and institutions with an increased potency and frequency. In cyber fraud, it is very difficult to identify a virtual identity with the real world. This type of crime could be orchestrated from any part of the world. That is why it is also known as a "White collar crime". Cybercrime is classified into two types. The first category of Crimes is committed/ directed on computers and can be committed in the online world. The second category of cybercrime involves computers or relevant information technologies. E-virus, e-worms, malware, Trojan horse (destructive

program) are examples of cyber-crimes. NCRB data has been witnessing a sharp increase in cybercrimes in India annually. USA's Internet Complaint Center (IC3) of the FBI, in its Internet Crime Report for 2019, has placed India in 3rd place with 2,901 amongst the top 20 countries based on the victims of internet crimes. (UK 93,796 victims, followed by Canada 3,721).

II. World-first "Cybercrime Index":

It has been prepared by the University of Oxford, the University of New South Wales, and Monash University, gathering researchers through a survey of 92 leading cybercrime experts from around the world. They are involved in cybercrime intelligence gathering and investigations. The survey asked the experts to consider five major categories of cybercrime.[2]

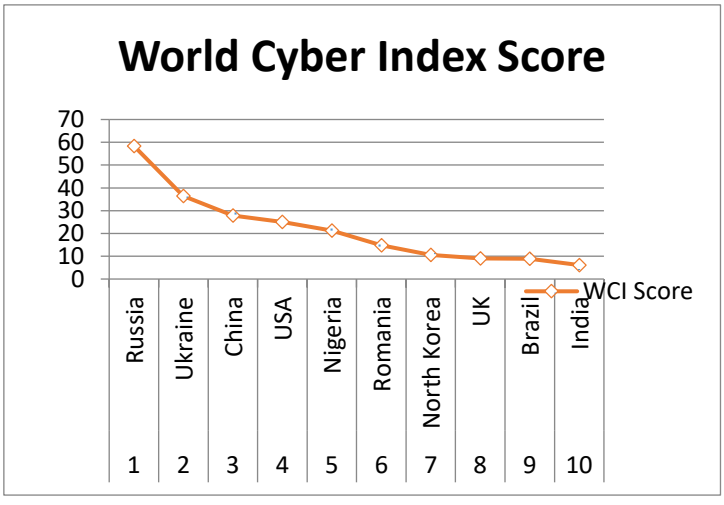
The World Cybercrime Index has been published in the journal *PLOS ONE*. The five major categories of cybercrime assessed by the study were:

i. Technical products/services (e.g., malware coding, botnet access, access to compromised systems, tool production).
ii. Attacks and extortion (e.g., denial-of-service attacks, ransomware).
iii. Data/identity theft (e.g., hacking, phishing, account compromises, credit card compromises).
iv. Scams (e.g., advance fee fraud, business email compromise, online auction fraud).
v. Cashing out/money laundering (e.g., credit card fraud, money mules, and illicit virtual currency platforms).

III. World 1st Cybercrime Index:

Ranking	Country	WCI Score
1	Russia	58.39
2	Ukraine	36.44
3	China	27.86
4	USA	25.01
5	Nigeria	21.28
6	Romania	14.83
7	North Korea	10.61
8	UK	9.01
9	Brazil	8.93
10	India	6.13

Source: Image credit: Pippa Havenhand.



World Cybercrime Index Report reveals that Russia and Ukraine are the top high-tech cyber hubs for cybercrimes. Most of the cybercrimes are based in Nigeria. The USA and Romania are under the category of

high-low tech cybercrimes (more crimes). India is in 10th place with a not high and lower category, in which more scope for scammers. According to the report, in 2023 alone $ 8 trillion, and in 2024 $ 9.22 trillion in damages due to cybercrime losses worldwide. By 2028, it will reach $ 13.8 trillion.

IV. Cyber Crimes in India:

The 2022 NCRB reported that cybercrimes against women totaled 14,072 registered across our country. The case's main cyber blackmailing, threatening under section 506,503,384 IPC r/W IT Act, cyber pornography, publishing obscene sexual materials under section 67 A/ 67 B (girl child) of IT Act, etc., Karnataka topped with 3,904 (27.74%), Maharashtra 2,530 (17.97%). Telangana, with 1,262(8.96) cases, was registered. 2022 NCRB report - Cyber-crimes against Children total 1823, including 28 states and 8 UTs. Karnataka topped with 239, Kerala and Rajasthan 182, and Tamil Nadu is in 11th place with 33 cases registered.[3]

a) India Cyber Threat Report-2025

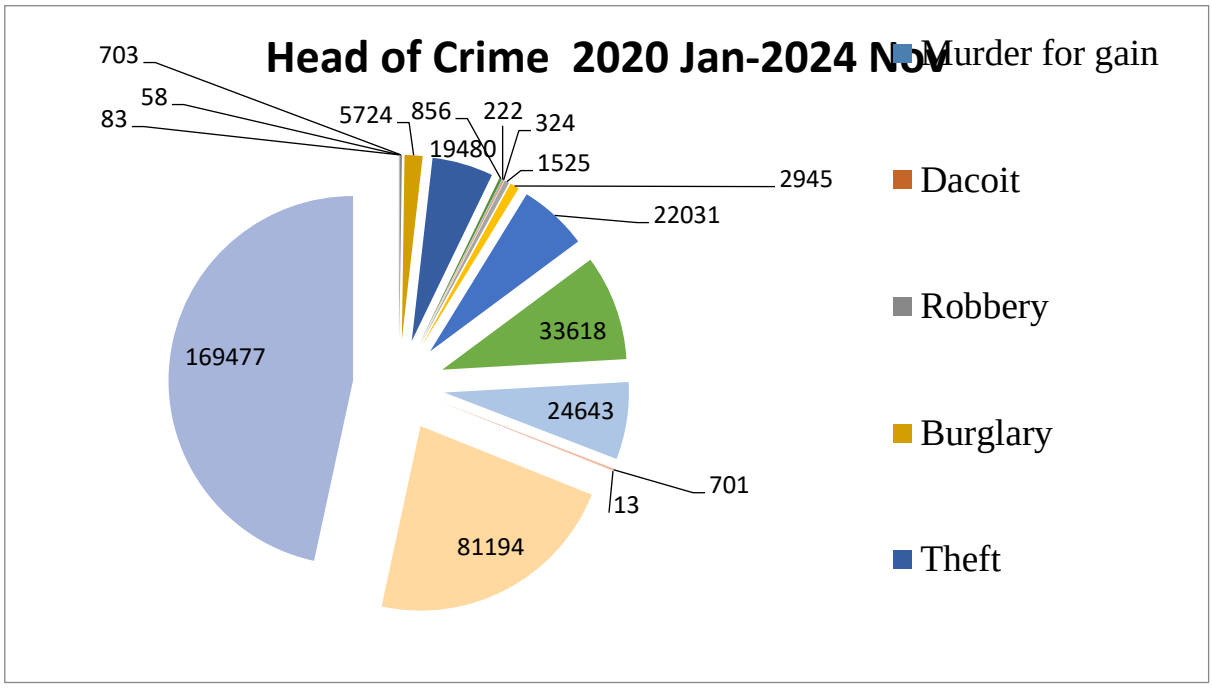
The latest report, 'India Cyber Threat Report-2025 released by Data Security Council of India (DSCI), predicts that cyber-attacks with AI (artificial intelligence) based malware will increase next year. With the same knowledge, it is also possible to control them. It has been found that 11 cyberattacks were committed every second across the country during the past year. According to the report, the impact of these attacks will be carried out through AI-based malware on healthcare and finance. Exploitation of biometric data is expected to increase. Further, it has been said that there is a possibility of committing fraud through fake apps and fake applications targeting the beneficiaries of government schemes. Crimes of massive looting by defrauding investors will increase.

The report suggests that there is a need to improve technology to effectively repel cyber-attacks. DSCI and Secite have prepared a report on cyber-attacks in the country from October 2023 to September this year. Attacks with 36.9 crore malware were detected across 84 lakh endpoints (the center where the crime was detected) across the country. Based on this, it was concluded that in India, an average of 702 cyber-attacks per minute occurs. That means 11 attacks were detected every second. Healthcare (21.82%), 96 (19.57%), Financial Services and Insurance 6 (17.38%), 2 (15.64%), MSME (7.52%), Manufacturing (6.88%), Government sectors (6.1%), / ITES (5.09%) ITES (3.09%) suffered on an average; there is a malware behind every 40,436 frauds. On average, there is a ransomware behind every 595 frauds.[4]

V. State Level Overall Crimes (2020 January- 2024 November)

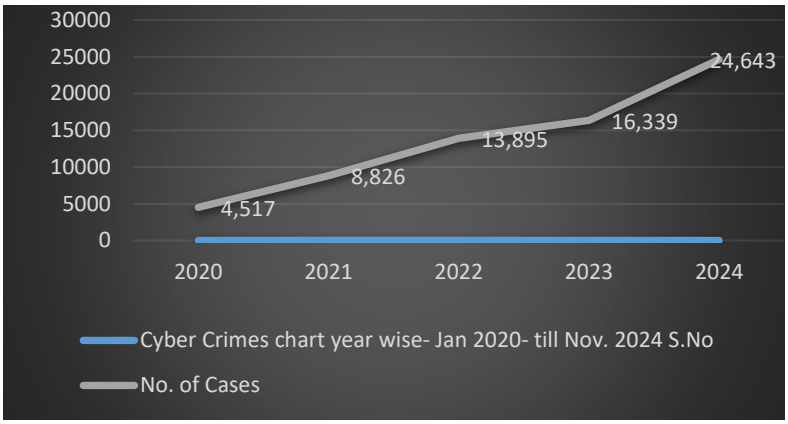
S.No	Head of Crime	As of 2024 Nov (from 2020 Jan to 2024 Nov)
1	Murder for gain	83
2	Dacoit	58
3	Robbery	703
4	Burglary	5724
5	Theft	19480
6	Murders	856
7	Culpable Homicide	222
8	Rioting	324
9	Kidnapping & Abduction	1525
10	Rape Cases	2945
11	Hurt Cases	22031
12	Cheatings	33618
13	Cyber Crime(Including Cheatings)	24643 (in 2024-8304)
14	Cr Br Trust	701

15	Counterfeiting	13
16	Other IPC	81194
Total Cognizable Crimes		1,69,477



V. A) Cyber Crimes chart year-wise- 2020- till Nov. 2024.

S.No	Year (Jan-Nov)	No. of Cases
1	2020	4,517
2	2021	8,826
3	2022	13,895
4	2023	16,339
5	2024	24,643



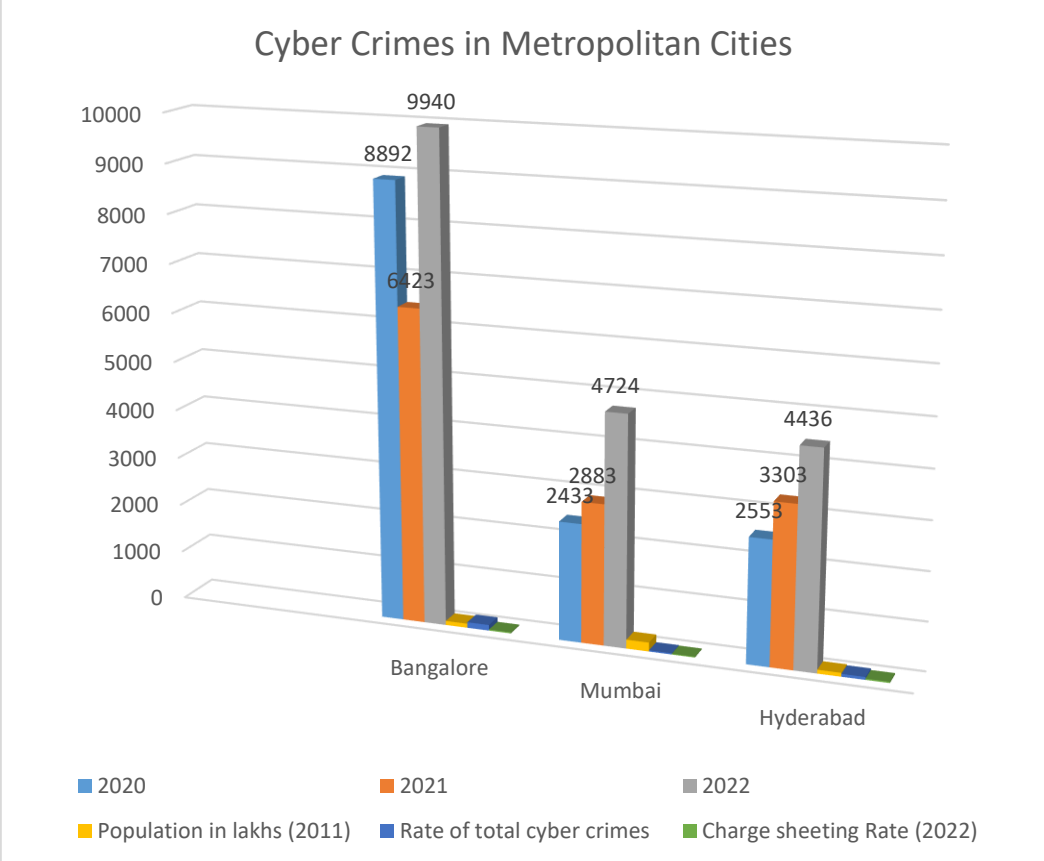
The overall percentage of cyber crimes in the state has increased by 43.38 percent in 2024. Out of a total of 33,618 cybercrime cases, Rs . 247 crores have been frozen, and Rs . 180 crores have been returned to the cyber victims. The highest percentage of recovery in crimes has increased in 2024, 1825 websites and URL websites involved in cyber frauds, and 15 thousand SIMs related to 9,800 cyber criminals have been blocked.

B) 15.03% attacks identified:
Telangana has shown its ability in detecting cyber-attacks going on across the country. It stood first in the country with 15.03% percent of the malware sent by the criminals being identified. The reasons for this are the presence of the fastest-growing IT industry in Hyderabad and the establishment of strong cybersecurity frameworks. Tamil Nadu, Delhi, Gujarat, and Rajasthan are in the next positions.

C) Cyber-crimes in Metropolitan Cities: NCRB report:

S. No	City	2020	2021	2022	Population in lakhs (2011)	The rate of total cyber crimes	Chargesheeting Rate (2022)
1	Bangalore	8892	6423	9940	85.0	117.0	22.6
2	Mumbai	2433	2883	4724	184.1	25.7	16.6
3	Hyderabad	2553	3303	4436	77.5	57.2	25.4

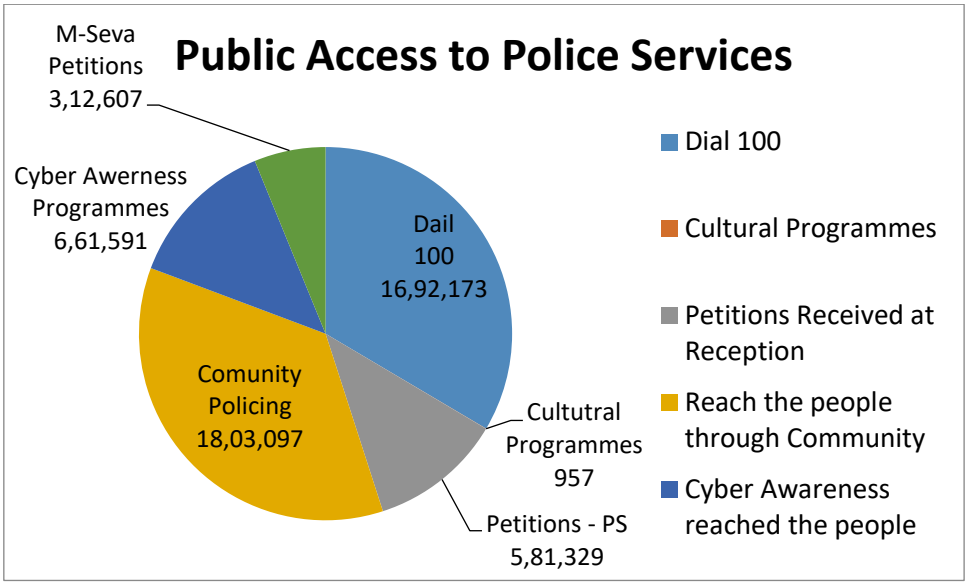
Source: NCRB Report 2020- 2022, Vol-II, P-833.



2020-2022 NCRB report on Cyber-crimes in Metropolitan Cities, out of 19 cities, was taken into consideration for the NCRB report. A total of 24,420 cases are registered in Bangalore (Karnataka), topped with 9,940, Mumbai (MH), 4724, and Hyderabad (Telangana), 3rd in place with 4,436 cases. [5]

D) Public Access to Police Services:
Telangana Police have extensively used Communication devices to reach the people and to address the people's problems as soon as possible. For that purpose, 100, E-mail, Twitter, Facebook, and other apps are used on electronic devices.

S.No	Subject	Number
1	Dial 100/112	16,92,173
2	Cultural Programmes	957
3	Petitions Received at Reception	5,81,329
4	Reach the people through the Community	18,03,097
5	Cyber Awareness reached the people	6,61,591
6	M-seva Petitions	3,12,607



VI. Telanagan Police Initiative & awards:

A) Sustainability Initiative award & International Digital Engineering Award:

The Tangana Police Department has received another prestigious 'Top Sustainability Initiative' award. The Computer Services and Standardization Department (CSSD) of the Telangana Police Department has been awarded the prestigious 15th National Digital Engineering Award at Assam under the category 'M-Governance Initiative of the Year 2024'.[6]

The award was presented by the Chief Secretary of Assam at Guwahati (Assam) on December 13, 2024. It was conferred for the outstanding results achieved by the Telangana Police Department in connection with the e-petty cases project, which has given good results in the mobile governance department.

E-Petty Mobile Application System will enhance public safety through digital evidence-based enforcement. With the Digital Application 'Tracking Immersion Process' by using GIS for Monitoring Ganesh Procession, TG COP won/ earned the prestigious International "Digital Engineering Award" in the "Digital Transformation of the Year" category at Dallas, USA in December 2024. This immersion process was monitored by “Global Society for Research & Development IAC (Information Services Group), organized in collaboration with CNBC-TV.

Telangana Cyber Security Bureau (TG CSB) for cybercrimes covering all states, The Telangana Police Department received a special commendation from the Hon'ble Union Home Minister for its contribution in building a 140, Ministry of Home Affairs centralized portal for Cyber Crimes connecting all the States by the TG CSB. Telangana Cyber Security Bureau (TG-CSB) has achieved better results than last year (Rs. 27.2 crores), giving relief to cyber victims. CSB has recovered Rs. 33.27 crores for a record 4,893 victims in the Mega Lok Adalat, which was held on December 14, 2024. TG CSB has excelled across the country in not only recovering but also taking legal action and returning them to the victims. Remarkably, Rs. 155.22 crores of 17,210 cyber victims have been returned.

B) QR-code for feedback collection:

On February 1st, 2025, Lanagana Police launched a QR code-based feedback collection system for police stations and offices across the state. Technology-driven initiative QR code strengthens the public-police relationship through feedback mechanisms. It enables citizens to easily share their experiences with various police services and also covers crucial touch points such as petition submissions, FIR registrations, traffic violation e-Challans, and passport verification services. Citizens can provide feedback by scanning QR codes displayed at police facilities or through calls from the citizen feedback call center, managed by the Centre of Excellence.[7]

C) Digital security with cyber hygiene

In the coming days, there is scope for crimes like AI-based malware, deep fake exploits, data theft, and ransomware. Cybercrimes will also increase with the expansion of the 5G network. Strong cybersecurity systems should be put in place for digital security. Organizations should provide necessary training to their employees.

Cyber hygiene, like data security, malware protection, secure configuration, data backup and recovery, privacy control, etc., should be given priority. In particular, AI-based defense systems should be strengthened to repel hacker attacks.

D) Bank staff in cyber-crimes:

Mule accounts are created for cybercriminals. That thief stole from those accounts and transferred them to different accounts. All this has come to light through the arrest of a large number of cyber criminals. In Telugu states, including Gujarat, Karnataka, New Delhi, UP, Maharashtra, West Bengal, and Bihar, city cybercrime police conducted a massive operation and arrested 52 cyber criminals. The police concluded that these cyber criminals committed 576 crimes, including 74 cybercrimes in Telangana, and looted Rs . 88.32 crores. It is noteworthy that 33 cybercrimes have been committed under the jurisdiction of the Hyderabad Commissionerate. Four employees of different banks who were cooperating with the cyber criminals transferred Rs. 23 crores to the accounts of major cyber criminals in Nepal and China. Their role has been found in 20 cases nationwide, 47.90 lakh cash with cyber criminals, and another Rs. 40 lakh worth of cryptocurrency, together with a total of Rs. 87.90 lakhs have been seized. It is said that Rs. 2.8 crores have been frozen in the accounts of criminals.

VII. Conclusion:

Eradication of computer crimes may not be completely achieved. It can, however, be reduced through public education, robust law enforcement, compliance, using effective secure e-ways, and the establishment of a secure framework for prosecuting these criminals. Banks need to provide a safe and secure banking environment.

REFERENCES:

1. Cybernetics" MerriamWebster.com Dictionary,
2. https://www.merriamwebster.com/dictionary/cybernetics Accessed 3rd July,2025.
3. Global Cybersecurity Index (GCI) 2024, 5th edition.
4. The National Crime Records Bureau (NCRB) Report 2020- 2022, Vol-II, P-833.
5. 'India Cyber Threat Report-2025- by Data Security Council of India (DSCI)
   Telangana Surakha Police Monthly journal, vol-10, editon-8, January, 2025, pp7-8.
6. Deccan Chronicle 18 December 2024, https://www.deccanchronicle.com/southern-states/telangana/telangana-police-wins-award-in-epetty-case-system-1847940
7. The Hindu, Telangana Police to display QR codes for citizens to give feedback on FIRs, petitions, and other services, January 09, 2025.