INTERNATIONAL JOURNAL OF LEGAL STUDIES AND SOCIAL SCIENCES [IJLSSS]

ISSN: 2584-1513 (Online)

Volume 4 | Issue 1 [2026] | Page 443 – 459

DIGITAL DETENTION TO REAL FEAR: A CRITICAL ANALYSIS OF DIGITAL ARREST SCAMS WITH FOCUS ON THE STATE OF ODISHA

-Subham Satapathy [1] Priyankita Sahoo[2]

ABSTRACT

Digital arrest, the latest cybercrime exploiting through cognitive duress and virtual impersonation, is becoming a considerable threat to India in this techno age. The perpetrators act as legal enforcement officials, to concoct allegations so as to put on hold the victims through video calls. They do so as to extort a lumpsum amount by creating an extremely stressful environment for the victim. Odisha has seen several notable cases pointing towards the evolution of the methods used by the scammers and the need for inter-agency measures to counter such criminal activity. This research paper follows a doctrinal approach starting with the definition of the term digital arrest and its functionality. It also draws through constructive analysis of five such cases from the state of Odisha, studying the modus operandi, the situation, the profile of the victims and the legal provisions that at present is used for punishing the perpetrators and it can be done so by recognising the pattern of the cases through media reports. It also takes a dive into the statutes, for example, provisions of the Information Technology Act and Indian Penal Code or the Bharatiya Nyaya Sanhita and what do they speak in the enforcement part. This paper also puts into some recommendations and reformatory measures which include wide spread awareness, crafting grass root level policies with future faced approach, creating a mix of new cutting-edge technology and a robust legal framework into preventive plan of action. This paper aspires to act as a tool for the lawmakers, cyber experts, police and other interested parties in countering this emerging threat of Digital Arrest.

Keywords: Digital arrest, Digital forensic, Odisha, Cyber fraudsters, syndicate, digital literacy, cyber surveillance, modus operandi.

[1] Author is a LLM student at KIIT School Of Law, India
[2] Co-Author is a LLM student at KIIT School Of Law, India

INTRODUCTION[3]

In the recent decade, India has seen a surge in the use of internet services, adding a spike to cyber-crimes also. As the saying goes pros and cons roll parallel and with development comes new faced challenges. One such challenge is the rise in cases of Digital Arrest. Here the defrauders impersonate a law enforcement official and restrict the victim using mental coercion so as to extract money from the victim. With advent of modern technology, the levels of crime has also been on a rise. Recently our Prime Minister Narendra Modi in his appearance on Mann ki Baat podcast, raised this burning issue and has warned people to be aware of such fraudsters. Governent is implementing several measures and awareness practices as counter measures to this act. Contrast to traditional arrest, digital arrest creates such a mental toll on the victim that his/her physical movement is restricted by means of video calls using social media tools. Most of the time, the criminals claim that either the victim is directly involved in a crime or one of the family members is involved in the crime and to get respite from any legal action or sanction, the victim is coerced to pay a lumpsum amount. They constrain the victim by forcing them to stay live through the video call until the transaction is completed. The underline modus operandi of the fraud is to create a panic like situation involving high level sanctions and extorting money out of the victims on the pretext of getting them relief from the crime. In recent times, the state of Odisha has also seen a surge in such cases where under false pretext, victims have been pulled into the trap and have lost lakhs of rupees. The concerned departments involving Cyber Cell of state Police, Enforcement Directorate, Reserve Bank of India and then we have the Indian Cyber Crime Coordination Centre under Home Ministry have done some exemplary work in creating awareness, educating people and forming an inter-state cooperation in handling such cases. Reserve Bank in particular has been running multiple advertisements in National Television under the tagline "mein murkh nahi hoon" (I am not a fool). Such methods have been contributing to success but the struggle against the act of Digital Arrest is continuing and it requires a mix of self-awareness, high vigilance and strong legal framework for the victims.

[3]Bhawana Shukla, Don't Get Trapped: Understanding Cyber frauds, Digital Arrests and How to protect yourself, 2025, SCC Online https://www.scconline.com/blog/post/2025/11/05/understanding-cyber-frauds-digital-arrests-protection-tips-law-made-easy-scc-times/

RESEARCH METHODOLOGY

This paper follows a trail of doctrinal research. It gives a complete understanding of the legal provisions involved in this. This method in particular has been used in this paper to make a complete analysis of the primary sources like statutes, administrative guidelines, case law etc as well as the secondary sources like media reports, legal dictionaries etc. This understanding creates a representation of what is happening, what has been done and what needs to be done in the context of Digital Arrest cases. This method will also help in extensive acknowledgement of the cases and suggest policies on mitigating the issue. Through this method, the aim is to formulate a statement of thought on countering the issue through case studies in the state of Odisha.

MEANING AND CONCEPT OF DIGITAL ARREST

Digital arrest is a fraud in which the main idea is to extort money out of innocent victims in the pretext of law enforcement officers and coercing the victims into believing that they have been actually involved in some kind of crime. They use several threats like drug package has been recovered in the victim's parcel, then freezing of bank account etc. They put the victim in immense mental duress so as to get them pay a lumpsum amount believing that they are paying some kind of fine to get respite from the act. The scammers mostly use voice calls at first to act innocent and with ongoing communication slowly they built the stress on the victim as if the victim is actually involved in a serious crime and the scamster is an angel in disguise who can bail out the victim out of this in exchange of some kind of fine or security fee. Then they switch to video call to assert higher degree of authority on the victim. The fraudster tries to single out the victim and creates a high intense situation where the victim is virtually arrested by means of live video calls until the amount is not transferred. The underline idea is to keep the communication constant and try to impersonate a legitimate situation and make believe that the victim has been trapped and has to pay the amount in order to get respite.

Important Characteristic associated with Digital Arrest[4]: From scamming through simple messages to now evolving to video calls, these cyber criminals are having a day out there. With evolving technology they are adapting and structuring new ways of cyber fraud. Key features of this new scam is:

[4] Major Sadhna Singh, Digital Arrest: The Modern-Day Cyber Scam, NITI Aayog, 2025 https://www.niti.gov.in/node/1642

1. Technology- The scamsters they use modern technologies such as video calls through social media apps and ask the victims to remain in constant touch throughout the transaction. The perpetrators use Artificial Intelligence to create deep fake videos so as to impersonate a law enforcement officer to create an atmosphere of legitimacy and build pressure on the victim.

2. Social manipulation- The scamster stalks through the social pattern of the victim first, which gives in some kind of personal detail which the scamster use to black mail the victim with and through this the victim is made believe that the scamster has such sensitive personal data of the victim which can create some kind of averring situation for the victim. This results in the setting of fear in the person's mind and creating a mental duress finally giving way to paying lumpsum amount to the perpetrator.

3. Lack of strong Cyber Security- The criminals try to make the most out of the weak data protection measures we have in India. The Cyber space is also not that well protected. Then we have issues of digital illiteracy where in people give away their passwords, OTPs too quickly.

4. Digital Transactions- With the advent of online payments by use of UPI, these cyber fraudsters have developed means and methods to exploit these apps. Mostly they target elderly people and try to coerce them by making fraud bank calls asking for OTP, passwords, pr clicking on crypted links to earn money in seconds.

5. Human Psychie- The most important aspect in every crime is the understanding of the mens rea of the perpetrator but in cases of Digital Arrest it is also important to understand that under what circumstances can the victim, in most cases an educated person be compelled to pay a lumpsum amount to a complete stranger within matter of minutes. These criminals have created such tactics in their belt that common people fall in their trap easily.

6. Restricting movement- The fraudsters game changing act is restricting the physical movement through virtual mode, when we think outside of it, we think it is impossible as how someone over a call can restrict our free will, but that is the core lay out of this Digital Arrest scam. The

success of the scam depends on for how much time the victim is restricted and within it the entire transaction must be completed.

Modus Operandi of this Fraud: The contours of this scam unveils a flickering need to understand the entire modus operandi of the scamsters. Understanding it can only lead to a successful evacuation strategy. Some of them are-

1. First call- The first call is very important as this is when the scammers have to put in their best efforts so that the victim is persuaded completely. If the first call fails and the person on the other side catches a wink that it's a fraud, the scam gets haywire. So for the success of the act the perpetrator uses all kinds of mental engineering to coerce the victim into falling in the trap.

2. Panic- The main weapon of the fraudsters is the stepping on the panic button for which they pull up their socks in creating a serious atmosphere and making the other side believe that he has actually committed a crime and there is no respite from this and he will face legal sanctions for his act. It is to be noted that the scamsters have such tricks up their sleeve that even highly educated individuals fall to the scam and become prey. It is important for the fraudster to continue with the panic situation till the end.

3. Successful impersonation- These scammers they thrive out potential victims by impersonating as senior law enforcement officers such as Customs officer, CBI officers, Senior Bank officials etc and try to intimidate the victim by alleging serious offences against the victims. They try to spoof their caller id to make it look more realistic.

4. Legitimate Persuasion and Digital confinement- The scamsters try to make themselves look like legitimate government officials and they try their very best, using different tricks to make the victim believe that he has actually committed a crime and they being legitimate government officials can provide respite. For the continuation of the panic scene, they force the victims to stay connected through video calls and not disconnect it. The victims feeling pressurized seeing such law enforcement officers tend to agree to this and stay connected till the transaction of money is not completed.

5. Payment technique- Most of these funds are collected through UPI apps and routed through digital wallets, next gen banking systems and crypto. Most of these are channels of Money Laundering and whitewashing.

6. Retreat/ Vanish- After the end of the transaction, these angel like government officers who the victims thought have helped them in getting respite from the crime (which they have not committed but were made to believe that they have vanish till the time the person realises that he has fallen to a trap of a scamster.

Psychological and Societal Consequences[5]- Victims when they realise that a scam has happened to them, generally get on a high emotional and mental toll thinking of the societal consequences which otherwise creates a nervous breakdown in them. Victims agonize themselves with-

1. Profound Anxiety- After the victims realise what has happened, most get into deep anxiety shock and complete nervous breakdown. They suffer from emotional and mental trauma. Some get symptoms of PTSD (Post Traumatic stress Disorder) with insomniac like situation.

2. Sense of loss of life- Sometimes combination of the above and tendency of having suicidal thoughts can lead to the victim believe a sense of loss of life and the will to live, generally when the quantum of fraud occurred i.e. the money involved is more.

3. Complete loss of faith in cyber systems- Due to increase in frequency of such incidents and poor handling by enforcement teams, the victims and their near ones lose trust in the system and are afraid to adapt to new technology. These attacks also attract negative publicity for Government schemes like Digital India.

[5] Dr. Rajnish Bishnoi, Dr. Pooja, Varnika Siyag, Rajvir Kaur, The Psychological Impact of Digital Arrest on Individuals: A New Threat to The Society, Vol. 44 No. 4 (2024): LIB PRO. 44(4), JUL-DEC 2024 (Published: 30-10-2024) [5] https://doi.org/10.48165/bapas.2024.44.2.1

4. Social Isolation- The victims of cyber-crimes in particular tend to fall into social isolation as they feel shame, humiliating and they tend to blame self for the act and try to withdraw from all social connections. They have this fear of negative judgement from the society.

CRIMINAL ACTS COUPLED WITH DIGITAL ARREST SCAM[6]

1. Stalking- The perpetrators keep looking out for potential victims by surfing through social media accounts and gather as much personal information as they can and sometimes harass the individuals making them believe that these fraudsters have something important to them for the purpose of blackmailing.

2. Phishing- It is the act of coercing victims into giving away their sensitive personal information like the OTPs, passwords, bank details by posing as reliable officers. This is mostly seen with aged victims.

3. Hacking- It is the act of accessing somebody's digital space without authorization and thereby find a medium to steal data or impersonate the account. in cases of cyber frauds what is mostly seen is hacking into an account and asking for monetary help from those accounts.

4. Fake news spread through their account by hacking- A new form has emerged wherein the cyber criminals hack into the system and try to spread misinformation from the particular account and then impersonate as law enforcement officers and try to terrorize the victim on why such hate speech has been posted and legal sanctions can be taken and he/she has to pay a certain money to get it removed from cyber space.

5. Money Laundering- Often these cyber criminals use these kinds of frauds to shadow the activity of money laundering, which is actually the backbone of most of these frauds. Recently

[6] Jyoti Chauhan, Digital Arrest: An Emerging Cybercrime in India (ijlmh journal, Vol-7, Issue-6, 2024) Pg no. 1632-1646
[6] https://ijlmh.com/wp-content/uploads/Digital-Arrest-An-Emerging-Cybercrime-in-India.pdf

government of India has banned all these betting apps in sports as they were presumed to be part of this fraud syndicate and used this route for money laundering.

6. Caller ID impersonation- This is done through SIM card spoofing. It's done so that when the victim receives the call, the caller Id will show some law enforcement agency's name, for ex: CBI, ED, Cyber Cell etc. This type of technique is also called Vishing.

PRESENT LEGAL FRAMEWORK

Current Indian laws do not cater directly to this new emergence. No Indian statute has addressed the crime of Digital Arrest directly but we have other co-related statutory provisions under which it is being dealt currently. Those are:

1. Information Technology Act, 2000- Section 66C[7], It deals with identity theft. It says that if anyone misuses any e-sign, or unique identity, password of any other person will be punished with terms up to 3 years imprisonment or fine up to one lakh rupees or both.
   Section 66D, it deals with cheating by impersonating through means of computer device and it attracts imprisonment up to three years or fine up to one lakh rupees or both.

2. Indian Penal Code/ Bharatiya Nyaya Sanhita 2023[8]- For the impersonation part BNS Section 204 talks about Impersonating a Public Servant and this attracts imprisonment of six months to three years maximum and fine.
   For the Cheating part BNS Section 318 deals with cheating in general and Section 319 deals with Cheating by impersonating another person. Both have imprisonment up to five years or fine or both.
   For the forged document part BNS has Section 336 and Section 340, both deal with concocted electronic records or possessing any forged document.
   For the extortion part BNS has Section 308 and it attracts imprisonment of up to 10 years or fine or both.

[7] Govt of India, MeitY, https://www.meity.gov.in/content/information-technology-act-2000
[8] Govt Of India, Ministry of Home Affairs, https://www.mha.gov.in/sites/default/files/250883_english_01042024.pdf

For criminal intimidation part BNS has Section 351 and it attracts imprisonment up to 7 years or fine or both.

3. BNSS/ CrPC[9]- Seizing of account as digital evidence is dealt under Section 106 of BNSS and Section 102 of CrPC.

4. Indian Cyber Crime Coordination Centre (I4C)[10]- It is formed under ministry of home affairs and recently it has passed an advisory to the public with relation to the rising cases of Digital arrest in India.

It is important for the public to understand that there is nothing such as a legal Digital Arrest, as there is no such thing in Indian Laws.

CASE STUDY IN STATE OF ODISHA

Here is a case study of four well reported Digital Arrest scams in Odisha. Each of the case study will cover a detailed factual analysis and scrutiny of modus operandi and victim profiling.

CASE STUDY NO. 1

THE SCAM INVOLVING ELDERLY COUPLE IN JHARSUGUDA

Summary of events: This case in particular occurred in May 2024 to an elderly couple from Jharsuguda, Odisha. The scamsters targeted selective elderly victims and who have a significant bank balance. Here in this case, the scamsters used skype and impersonated as police officers and made false accusation against the elderly couple that he was involved in a money laundering circle. They offered settlement amount and transactions were done in two instalments totalling the amount defrauded to 34 lakhs rupees. The fraudsters intimated the couple by threatening them to freeze their bank account and seize all their properties if they did not cooperate.

Aftermath[11]: The couple after realising that it is a fraud immediately reported the matter to Jharsuguda Sadar PS. Odisha Police with help from cyber cell started tracking the culprits and finally nabbing

[9] Govt of India, Home Ministry,https://www.mha.gov.in/sites/default/files/2024-04/250884_2_english_01042024.pdf
[10] I4C Coordination Centre, MHA, https://i4c.mha.gov.in/advisories.aspx
[11] Indian Express Article, 2024,https://www.newindianexpress.com/states/odisha/2024/Nov/22/four-from-gujarat-held-for-keeping-man-under-digital-arrest-looting-rs-34-lakh

them within 5 months of the scam, from Gujarat. The criminals acted as a gang and they had prepared excel sheet of hundreds of such victims and had profiled them as their next target. In this case 4 were nabbed, they belonged to Maharashtra and Gujarat region. From those caught, 20 cell phones, laptops and cash of 2 lakh rupees was seized. Around 14 lakh rupees could be recovered and returned to the couple.

Analysis: This case is face of one of many cyber frauds in recent times in Odisha. Effective policing and wide spread awareness are required for the public. In this case elderly couple was victim, so administration and banking system should be more vigil while handling transactions from such account and verify such large transactions.

CASE STUDY NO. 2

BERHAMPUR UNIVERSITY VICE CHANCELLOR CASE[12]

Summary of events: This case in particular covers how a highly educated vice chancellor of a university can also be trapped by the scamsters. In this case the Vice Chancellor Ms. Geetanjali Dash received a call on February 12, 2025 from the scammers impersonating as Enforcement Directorate officer and alleged that she was involved in ED cases and her name has found in their data base. To get respite from that she was Virtually arrested and was made to belief if she pays a fine of 14 lakhs rupees her name would be removed. In that panic situation she transferred the amount.

Aftermath: Ms. Dash upon realising, that she has been duped immediately informed the police officials. The Odisha cyber police worked hard and tracked down and two were arrested from Bhavnagar, Gujarat and brought to Berhampur on a five-day transit remand. Several cell phones, Aadhar cards, laptops were seized from them. Police returned Rs. 80,000/- and assured her that rest would also be returned after verification.

Analysis: Such high profile cases demonstrate the cyber criminals give in effort in profiling the victims. In this particular case the victim is a highly educated professor, even she fell in their trap. This suggest that even high ranked people can also be scammed which brings into fore the advanced level of mental coercing and urgency like situation created by these scamsters who are hardly intermediate pass. They employ this technique of detailed profiling and tracking through social media and target with accurate tactics. One of the aspects in this case should be pointed out that even being at such high authoritative

[12] TOI Article, 2025, https://timesofindia.indiatimes.com/city/bhubaneswar/2-cyber-frauds-held-from-guj-part-of-gang-that-duped-berhampur-univ-vc/articleshow/120238927.cms

position why did the VC gave in to their demands, it indicates she might be involved in any such transaction which is shady and in that fear in mind she gave in easily. It is appropriate to think that she should have reported this at the first instance only rather than giving in to the fraud. Police should verify her account and trace her transaction history.

CASE STUDY NO. 3[13]

PARADIP MAN DEFRAUDED OF 74 LAKHS

Summary of events: A person from Paradip area was defrauded of around 74 lakhs in a digital arrest scam in May 2025. In this case the scammers posed themselves as CBI and Delhi Police officer and tricked the victim in believing that a parcel addressed to him has been caught and seized by the Delhi Narcotics cell and Airport Customs. They claimed that the package had illegal narcotics, laptops, laundered bundles of notes, credit cards and that it was being sent to China. It created a panic situation and instilled fear in the victim's mind. He was under constant virtual detention and he finally gave in to the fraudsters demand believing that he will get relief from this criminal act and paid around 74 lakhs in instalments.

Aftermath: Upon realising that it was a scam and he had fell face on it, he immediately filed a police complaint with the Cyber PS of the Crime Branch. Within weeks Odisha Crime Branch arrested a 26 year old shopkeeper from West Bengal named as Rohit Kumar Jaiswal. He was a resident of Howrah. Several incriminating articles were recovered such as spoofed SIM cards, laptop etc. His bank account was also freezed.

Analysis: It is pertinent to understand why and under what condition a person who is completely unrelated to a crime is made belief that he has committed a crime for which he has to pay such huge amount of 74 lakhs of rupees. It is commendable on the part of Odisha Cyber Cell that within few days they tracked down the criminal and caught him. it is also important to look into how such a shopkeeper and aged only 26 years of age could have such criminal mindset and how he tracked down the victim. High level cyber security must be there in banking system and when large transactions are done it must be properly verified.

[13] TOI Report, 2025, https://timesofindia.indiatimes.com/city/bhubaneswar/bengal-shopkeeper-held-for-role-in-duping-paradip-man-of-rs-73-lakh/articleshow/121345912.cms

CASE STUDY NO. 4[14]

BHUBANESWAR CORPORATE EMPLOYEE SCAMMED

Summary of events: A techie working in Bhubaneswar has been duped in a case of Digital Arrest scam in August. The scamster posed as a police officer and used Skype as the source to contact the victim and levelled allegations that a suspicious parcel has been seized by police and it was addressed to him. He has to pay fine of Rs. 7 lakhs or else his bank account and properties will be seized. The victim informed that he does not have that much money in his bank account to which the scamster virtually contained him in the video call and asked him to apply for an online loan immediately, to which the techie gave in and immediately 6.94 lakh rupees was siphoned off from his account.

Aftermath: The techie immediately filed a complaint with the Bhubaneswar Cyber Cell and they traced the transaction and call details to Gujarat. Within weeks the accused was arrested. What surprises the most is that in this particular case, the accused named Ramesh is a daily wage labourer and he has studied till Class VII. On further interrogation, Odisha Police managed to get 2 lakh rupees from him and it was paid back to the victim. It was further found out that Ramesh was involved in more than twenty-five similar frauds in different states.

Analysis: In this particular case it is paramount to understand how a Class 7 failed daily labourer managed to fool and dupe a well digital literate techie. Police action should be praised for such swift action. It also brings into fore; it is not the amount of awareness only but being patient and mentally strong to reject any kind of fear and panic situation can only deter the victim in falling prey to such scams.

CASE STUDY NO. 5[15]

CYBER SCAMS MAKE ANOTHER KILL: TARGET ELDERLY CA COUPLE

Summary of events: A senior citizen couple from Bhubaneswar has been duped of 1.5 crore rupees. The victim, a 68 year old Chartered Accountant, was scammed by the fraudsters posing as

[14] OTV Report, 2025,https://odishatv.in/news/odisha/gujarat-labourer-mastermind-in-rs-7-lakh-bhubaneswar-digital-arrest-scam-arrested-271071

[15] TOI Report, November,2025, https://timesofindia.indiatimes.com/city/bhubaneswar/68-year-old-chartered-accountant-falls-victim-to-rs-1-5-crore-cyber-fraud/articleshow/125159995.cms

Enforcement Directorate officer, Customs Inspector. He was under virtual detention for 10 days that is he was constantly under psychological pressure to give in. The story unfolds like, on October 18 he received a call over Whatsapp wherein allegations such as, his aadhar card has been used in money laundering activities and his name has been added in a FIR were made and he was forced to stay connected over call until he accepts their demand. Under immense psychological duress and panic he transferred 1.5 crore rupees. The story came to front when one of his family members observed a change in his daily behaviour and asked him, then a complaint was raised before the Cyber Police Station.

Aftermath: As of now, the culprits are still at large and the Police has launched an extensive investigation, tracing down the transaction footprints. This comes at a time when on November 3, Hon'ble Supreme Court while referring to a confidential report submitted by Centre observed that more than 3000 crore rupees have been lost through these scams and now this is turning as a very big challenge.

Analysis: it is very important to understand how technologically advanced these criminals are, they have used AI tools to mimic court room and police station like back ground in the video calls. This case in particular speaks volume about how elderly people with money in their bank account are targeted constantly. The trust part is elderly people easily fall in the trap as they have full trust in the law enforcement and believe that they have actually committed some crime. Government agencies must focus on how these elderly people can have better awareness level, conduct seminars for them or run targeted programmes on national TV.

ANATOMY OF THE 5 CASES DISCUSSED ABOVE

All these above cases suggest that, with technological advancements comes new types of challenges such as Digital Arrest case. Neither the law nor the enforcement agency can cope up with the growing concern. It is finally up to the citizens to be aware of such frauds and relegate such situation with patient rather can panicking and fearing the consequences. For the elderly people in particular avoid such calls if possible or else at best immediately inform your family members immediately. These scams can happen to anybody as we did see even a highly qualified person can be duped of lakhs and a case where a daily labourer scammed a tech savvy young guy from Bhubaneswar. Only weapon that we have is to stay calm and do not be fearful of any wrongful allegation or intimidation.

Let's make a comparative table to dissect these 5 cases:

CASE STUDY NO.	TECHNIQUE / MODUS OPERANDI	VICTIM PROFILE	AMOUNT LOST	ACCUSED PROFILE
1 Jharsuguda case	Fraudsters posed as police officer and alleged that he was involved in money laundering and his account will be seized if fine is not paid.	Elderly couple living alone with significant financial asset	Rs. 34 lakhs lost, police could recover Rs. 33 lakhs.	A group of 4 aged between 24-27 arrested from Surat.
2 Berhampur VC case	Scammers posed as ED officials and SC investigation team and alleged that she was involved in money laundering.	A highly qualified Vice chancellor of a university.	Rs. 14 lakhs lost, police seized Rs. 80,000/- only.	2 people aged 20 and 21 years were arrested.
3 Paradip case	Criminal posed as CBI officer and Delhi Customs with allegation that a parcel carrying drugs has been intercepted.	A 62-year-old victim and a resident of Paradip port area.	Rs. 73.62 lakhs lost.	26 year old illiterate shopkeeper from Howrah was arrested.
4 Bhubaneswar techie	Scamster posed as Delhi Police and alleged that a drug related parcel has been seized. Here Skype was used.	A young techie of Bhubaneswar virtually arrested using Skype.	Rs. 6.94 lakh lost, 2 lakh rupees recovered.	A daily wage labourer was arrested from Gujarat.

5 Elderly CA duped	Cyber criminals posed as ED official and alleged that his aadhar card was linked to an account linked with money laundering. Whatsapp video call was used.	68 year old victim and a retired Chartered Accountant and a resident of Bhubaneswar.	Accused still at large and investigation is undergoing as of now.	Accused still at large. Investigation underway.

AWARENESS AND POLICY RECOMMENDATIONS

ODISHA'S STRATEGY

1. Odisha has one of the robust Cyber Cell and Economic Offence Wing working tirelessly to counter such cyber scams.
2. Odisha has been integrated under the I4C unit called as Indian Cybercrime Coordination Centre. This has helped in reporting of cyber crimes and investigating it using inert state machinery.
3. Odisha is part of the National Cyber Crime Reporting Portal which has a dedicated 24*7 helpline number 1930.[16]
4. Dedicated CAWACH[17] portal for cyber crime reporting has been established by the state.
5. State government has issued orders for establishing new cyber crime police stations all over state.[18]
6. Awareness programmes are being run through local newspapers for the masses to understand the rising danger and stay alert.

[16] Toll free no. https://cybercrime.gov.in/
[17] Govt of Odisha initiative, https://cawach.odisha.gov.in/
[18] Govt of Odisha, https://home.odisha.gov.in/news/creation-20-cyber-crime-economic-offences-cceo-police-stations-across-state

RECOMMENDATION

1. Extensive e-beat patrolling teams[19] (a digital police system which uses technology to monitor and check records on spot) mostly in urban police system should be launched to strengthen local surveillance. So that faster identification of local cyber-crimes could be reported.
2. Large scale campaigns in local language, local administrations must do door to door canvassing to spread leaflets spreading word of caution against such crimes.
3. Special recruitments must be arranged by the state governments to help cyber police track down cyber criminals more efficiently. They must be trained with handling digital forensics, evidence etc.
4. Inter-state coordination centres must be established so as to have a smooth and effective investigation.
5. Banks must strengthen their transaction verification methods and must regulate and verify personally with the account holder before allowing such transactions. Banks must also run targeted ads for elderly people to make them aware of such scams.
6. Law enforcement agency must try to recover 100% of the money lost in the scam, so as to gain trust of the public.

CONCLUSION

This paper concludes by reflecting that, the rising issue of Digital Arrest scams presents a new set of challenge for the country. The state of Odisha is just an example which has recently seen a jump in such scams and has since then facing consequences from it. In this new method, the perpetrators pose as law enforcement officer from CBI, ED, Police etc and level allegations against the victim against which they demand money as fine to bail them out from the situation. Their most important tool is creating a panic like and urgency situation and detaining the victim under virtual arrest till the transaction is complete. They threaten the victims using AI generated video back ground of court rooms, police stations etc to make the victims believe that they are legitimate law enforcement officers and it is a valid call. In all the five cases studied above, it is a well analysed fact that these scamsters target mostly educated people and elderly people with significant financial assets. It is pertinent to note that these people run a syndicate and do an extremely deep profiling of the victims before

[19] Mohammad Karim, 2025,OTV Report https://odishatv.in/news/odisha/rourkela-police-launches-smart-e-beat-patrolling-initiative-system-to-cover-600-sensitive-locations-267589

targeting. In one such case, when the accused was arrested an entire excel sheet was found with numbers, google pay accounts and other sensitive information of hundred such victims. It is important to understand that we don't have a specific law for digital arrest scams, mostly it is dealt under BNS, IT Act,2000 and administrative policies. But it is commendable on the part of police in particular from the above case studies, the Odisha Police Crime Branch has done an immense job and acted swiftly in catching the criminals within weeks. It must be understood that only administrative actions and strong law enforcement agencies cannot alone counter these scams, it is important that self-awareness, digital literacy and trust in police system must be at top notch level to successfully eradicate this disease from the society.