CyGMa

Cyber Gyan Madhyam

January 2023 Vol. 1 Issue 1

A Monthly Newsletter of National Digital Crime Resource and Training Centre (NDCRTC), SVP National Police Academy (SVPNPA)

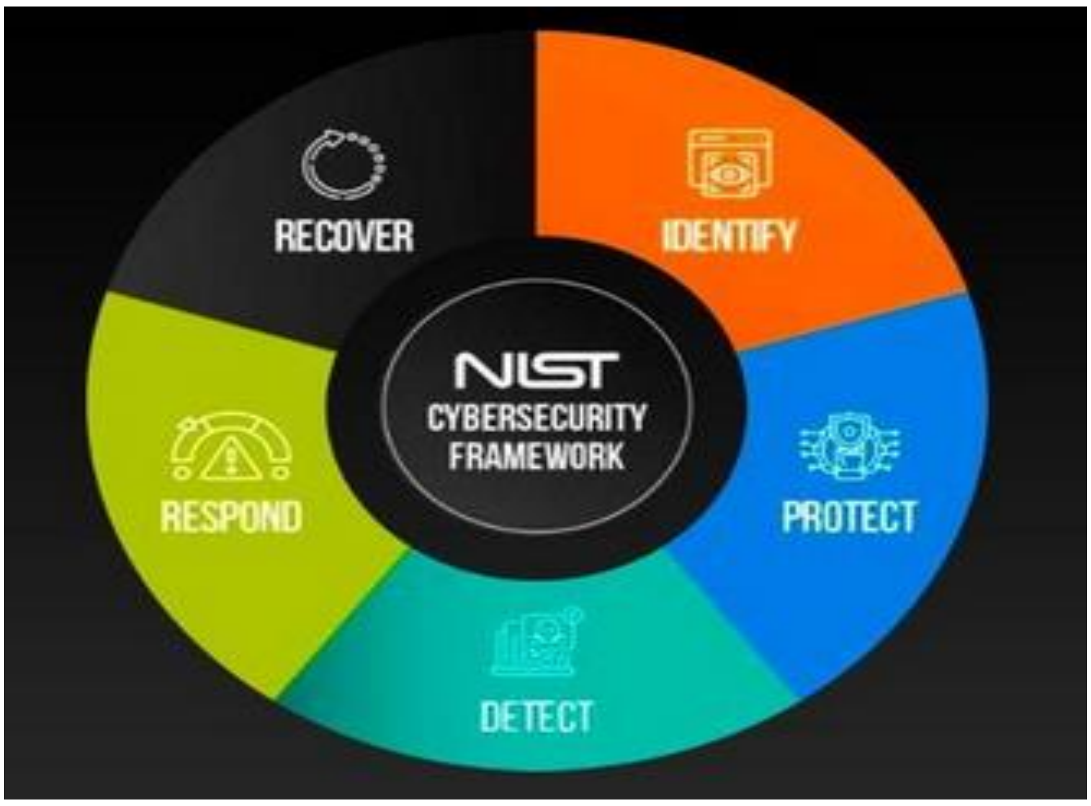
LATEST TECHNOLOGIES -Page 2

FRAUDS IN TREND-Page 3

JUDGEMENTS-Page 4

IS INDIA CYBER RESILIENT?

RANSOMWARE ATTACK ON AIIMS SERVERS



Cyber Security comprises of policies and technologies to be used to protect the systems from attacks. Though the organizations follow cyber security policies strictly, they are still being attacked. Then, what is the position of the organizations which are not serious about Cyber Security?

AIIMS Ransomware attack is one such example. The AIIMS hospital administration was informed that it is not up to the mark in terms of Cyber Security. Cyber Security experts said that the firewalls installed in AIIMS infrastructure are not configured properly and all intermediary devices such as network switches are unmanaged. They would have taken care of system security, firewalls, regular auditing of networks, and incident response teams which would have cyber experts. Organizations should be ready to invest in Cyber Security to stay secure, robust and resilient.

BEST PRACTICES -Page 5

EVENTS AND TRAININGS-Page 6

TECHNOLOGY WORKAROUNDS-Page 7

(Image Credits: lawministry.in, ptc.com, shutterstock.com, shrm.org, industrialdefender.com, economictimes.com, newindianexpress.com, ind-techconsultants.com)

January 2023 | CyGMa | Vol. 1 Issue 1
NEWSLETTER OF NDCRTC (SVPNPA)

LATEST TECHNOLOGIES IN IT INDUSTRY

CHATGPT FOR CYBER POLICING

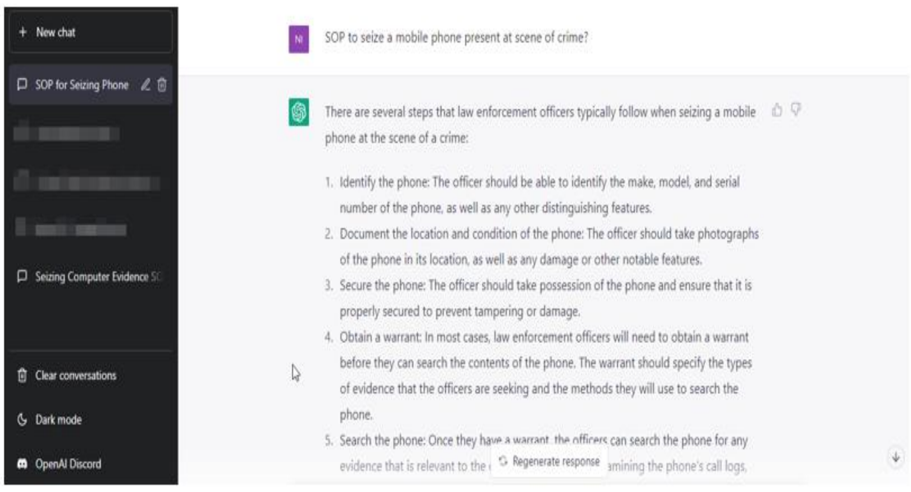
-Shri Nitin Sharma, Forensic Analyst, NDCRTC

Use of cyberspace is growing rapidly with the enhancement in technology. Technologies like Artificial Intelligence, Machine Learning, Virtual Reality etc., are extending the capabilities of cyber space in terms of its use cases and dependencies. A new invention by *Open AI* (Artificial Intelligence Research Laboratory) known as *ChatGPT* is in trend now a days and it is capable of answering the questions asked by the user in a conversational way. *ChatGPT* is an artificial intelligence based chatbot launched by *OpenAI* in November 2022. *ChatGPT* was trained using a machine learning technique called Reinforcement Learning from Human Feedback (RLHF). It is capable of answering questions from different fields like software development, penetration testing, content writing, user guides of any popular tools like latex etc.

To use *ChatGPT* one has to sign up on the website of *OpenAI* (https://chat.openai.com/auth/login) by providing the email id and mobile number along with the name of the user. Once the registration is completed, the user can ask any questions to the bot using the chat window available there. As per *OpenAI,* the chatbot is currently in its research phase and is available for free for everyone. Its developers are looking for the users' feedback to learn about its strengths and weakness.

ChatGPT is also capable of answering questions related to SOP to seize digital evidence like computers, mobile phones present at scene of crime.

ChatGPT is also capable of answering questions related to SOP to seize digital evidence like computers, mobile phones present at scene of crime.



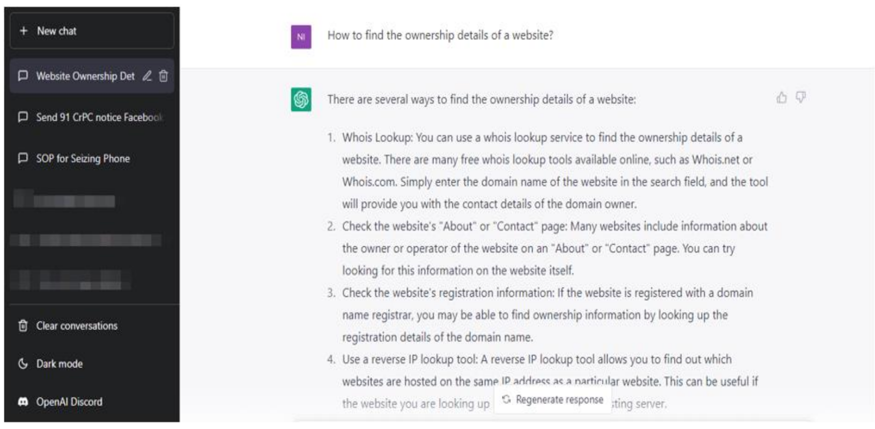
NI SOP to seize a mobile phone present at scene of crime?

There are several steps that law enforcement officers typically follow when seizing a mobile phone at the scene of a crime:

1. Identify the phone: The officer should be able to identify the make, model, and serial number of the phone, as well as any other distinguishing features.
2. Document the location and condition of the phone: The officer should take photographs of the phone in its location, as well as any damage or other notable features.
3. Secure the phone: The officer should take possession of the phone and ensure that it is properly secured to prevent tampering or damage.
4. Obtain a warrant: In most cases, law enforcement officers will need to obtain a warrant before they can search the contents of the phone. The warrant should specify the types of evidence that the officers are seeking and the methods they will use to search the phone.
5. Search the phone: Once they have a warrant, the officers can search the phone for any evidence that is relevant to the (amining the phone's call logs.

Figure 1: ChatGPT response for SOP of Seizing Mobile Device

It helps in identifying the address of various Intermediaries to send notices under 91 CrPC. It can help in finding information in investigations related to ownership details of a website.



NI How to find the ownership details of a website?

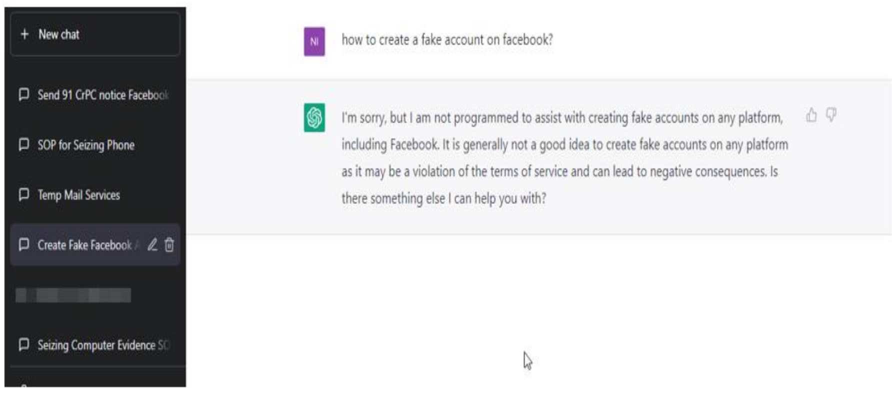
There are several ways to find the ownership details of a website:

1. Whois Lookup: You can use a whois lookup service to find the ownership details of a website. There are many free whois lookup tools available online, such as Whois.net or Whois.com. Simply enter the domain name of the website in the search field, and the tool will provide you with the contact details of the domain owner.
2. Check the website's "About" or "Contact" page: Many websites include information about the owner or operator of the website on an "About" or "Contact" page. You can try looking for this information on the website itself.
3. Check the website's registration information: If the website is registered with a domain name registrar, you may be able to find ownership information by looking up the registration details of the domain name.
4. Use a reverse IP lookup tool: A reverse IP lookup tool allows you to find out which websites are hosted on the same IP address as a particular website. This can be useful if the website you are looking up ting server.

Figure 2: ChatGPT response for finding website details.

There may be several questions related to cyber-crime investigation and other aspects of policing, which this chatbot can answer but all the answers provided by this chatbot must be cross verified from some authenticated source and legal aspects should also be considered. However, ChatGPT doesn't answer direct questions related to criminal intention but it is possible to get the answers in different manner.

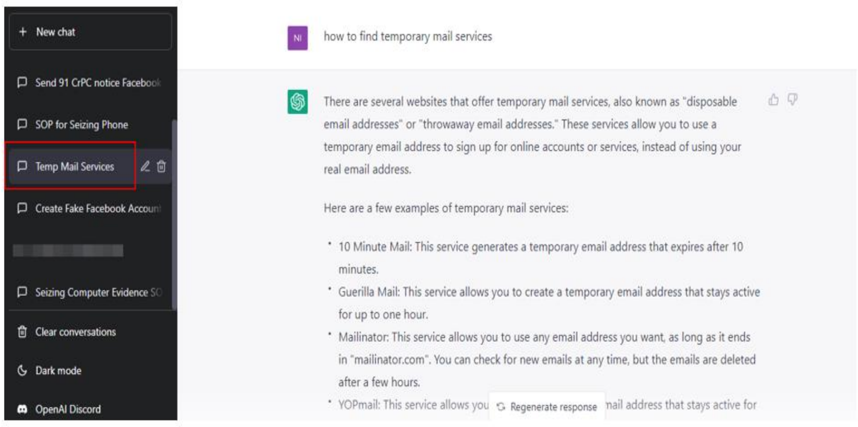
ChatGPT is getting huge popularity among people. Fraudsters have created fake applications in the name of ChatGPT for spreading malware.



NI how to create a fake account on facebook?

I'm sorry, but I am not programmed to assist with creating fake accounts on any platform, including Facebook. It is generally not a good idea to create fake accounts on any platform as it may be a violation of the terms of service and can lead to negative consequences. Is there something else I can help you with?

Figure 3, 4: ChatGPT responses related to fake 'Facebook' accounts and temporary mail services



NI how to find temporary mail services

There are several websites that offer temporary mail services, also known as "disposable email addresses" or "throwaway email addresses." These services allow you to use a temporary email address to sign up for online accounts or services, instead of using your real email address.

Here are a few examples of temporary mail services:

- 10 Minute Mail: This service generates a temporary email address that expires after 10 minutes.
- Guerilla Mail: This service allows you to create a temporary email address that stays active for up to one hour.
- Mailinator: This service allows you to use any email address you want, as long as it ends in "mailinator.com". You can check for new emails at any time, but the emails are deleted after a few hours.
- YOPmail: This service allows you nail address that stays active for

FRAUDS IN TREND

FRAUD SIMILAR TO MAN-IN-THE-MIDDLE ATTACK OF RS. 44 LAKHS FOILED [1]

Man-In-The-Middle (MITM) fraud is a type of fraud in which fraudster enters a conversation taking place on a virtual platform by exploiting technological loopholes. Subsequently, the fraudster pretends to be a participant of the conversation and eavesdrops on sensitive data like banking credentials, etc. A MITM fraud of Rs. 44.43 lakhs was prevented by the swift action of the cops as well as the complainant. The complainant is a director of a Mumbai-based textile company and he had transferred money to the fraudster as he pretended to be his partner. He realized the scam after noticing that the amount was sent to a different account number than that of his partner. Immediately, he dialed the 1930 helpline number and informed them about the matter and registered an online complaint on the National Cyber Crime Reporting Portal (*https://cybercrime.gov.in/*). The cyber crime unit of Mumbai Police contacted the bank from which the complainant had transferred the amount, and asked it to stop the process. As the complaint was made during the golden hour, the police said they could successfully stop the transaction and freeze the account which prevented further fraudulent transactions.

CBI, DELHI POLICE, FBI BUST 'TECH SUPPORT' SCAM THAT TARGETED U.S., CANADIAN CITIZENS [2]

The Central Bureau of Investigation (CBI) and the Delhi Police have assisted the Federal Bureau of Investigation (FBI) in busting a major scam, which duped thousands of the U.S., and Canadian citizens over the past decade on the pretext of providing remote tech-support. More than 20,000 victims belonging to US and Canada were targeted in this scam. A total of over $10 million were lost by the victims.The gang of accused (from Delhi, Haryana, New York, Ontario) created fake pop-up windows to display on the personal computers of the victims. These fake pop-ups were designed in such a way that victims computers get into "freeze" state that prevented them from using or accessing files on their computers. Also, false claims of virus infection of victims computers were made by these fake pop-ups that directs them to call technical support team whose call centers located in India. U.S. Attorney *Philip R. Sellinger* thanked CBI and Delhi Police for their assistance in making the arrests.

FRAUDSTER WHO CHEATED AROUND 50 PEOPLE AS IPS OFFICER GOT ARRESTED[3]

One *Vikas Gautam* (30), used to sell tea in front of the prominent Civil Services coaching institutes of Mukherjee Nagar. During the same period, he has started impersonating one IPS officer with name *Vikas Yadav* (2020 batch) on various social media platforms. When UPSC published results in 2020, accused Vikas Gautam created one Instagram profile 'Vikashyadav_ips'. He has posted the details of list of candidates selected in UPSC on his Instagram profile, also, declared his selection into UPSC.

The accused had contacted (as *IPS Vikas Yadav*) and influenced various people to get their work done in return for money. More than 50 people were cheated by him that accounts to a total of more than Rs.14 lakhs. He got arrested by Delhi Police.

IT YOUTH LOST RS.27 LAKHS FOR A LOAN OF RS.40 LAKHS [4]

In the process of getting a loan of Rs.40 lakhs from a finance company, an IT youth who resides in area of *Vishrambaug* Police Station has submitted documents and paid Rs 1.5 Lakh online who got convinced as amount paid is for loan being high amount.

A further two lakh rupees were demanded by fraudsters citing the reason that the money was kept on hold by RBI. In the continuous manner, victim was cheated a total of Rs.2745000 for a loan of Rs.40 lakh by the fraudsters.

U.S CITIZEN GOT ARRESTED BY FBI FOR HACKING POINT OF SALE (POS) SERVICE PROVIDER[5]

On December 8 2022, *Foster Cooley* was arrested by FBI (New York Office) for intruding and diverting money of $400,000 (approximate 3.3 Crore Indian rupees) through credit card payments of a New-York based hair salon company. It came to known that unauthorized access was obtained by *Cooley* for one of the POS accounts of four branches of the hair salon company through stealing usernames and passwords of employees with the help of browser-based spyware/ malware.

Cooley, after obtaining access changed the bank accounts (to his accounts) for receiving payments from hair salon credit card holders.

ELDERLY CHEATED OF RS.44000 IN ELECTRICITY BILL SCAM[6]

Cyber criminals have cheated one elder man of age 66 years who stays in Ajmer, by sending a message with respect to disconnecting electricity supply for his house if in case electricity bill is not paid immediately. The victim responded to the message sent by the fraudster by making a phone call on the number identified in the message. The fraudster suggested him to pay the electricity bill online by downloading one mobile application mentioned by the fraudster. The victim had downloaded the application and forwarded OTP to the cheater. Immediately an amount of Rs.44000 was deducted from his account.

[1] *https://www.freepressjournal.in/mumbai/mumbai-man-in-the-middle-fraud-of-rs44l-foiled*
[2] *https://www.thehindu.com*
[3] *https://www.indiatoday.in*
[4] *https://timesofindia.com*
[5] *www.justice.gov*
[6] *www.latestly.com*

JUDGEMENTS

FACEBOOK WAS IMPOSED A FINE OF RS. 50,000 BY HC OF UTTARAKHAND [7]

Uttarakhand High Court was hearing a PIL alleging that fake IDs were being created on Facebook and friend requests sent through ID belonging to a petitioner. It is also mentioned in PIL as threats of edited obscene photos and videos were being made through these IDs in exchange for lakhs of rupees. The petitioner (victim) has complained about the same to Facebook and a reply received from Facebook as "Thank you for your email. Please note that this email is used only for the purpose of answering questions about the process to submit user grievances to Facebook. Facebook will not respond to grievances submitted to this email. If you have a grievance that you would like to submit to Facebook, you may do so here."

However, Facebook has not acted to the grievance submitted by the petitioner. By referring to the Information Technology Rules 2021 (Intermediary Guidelines and Digital Media Ethics Code) to exercise powers conferred by *sub-section (1), clauses (z), (so) of section 87 of the Information Technology Act, 2000*, High Court, imposed a fine on Facebook for not responding to petitioners' grievance. A total amount of Rs 50000 out of which, Rs.25000 to be paid to the petitioner and the remaining amount to be deposited with the Uttarakhand High Court Bar Association. The court has set a fresh deadline of February 16 to file its reply. The costs be deposited within three weeks.

CBI COURT SAYS "ACCUSED CANNOT BE FORCED TO DISCLOSE THE PASSWORD. BUT?" [8]

CBI Court in Delhi says in a case under prevention of corruption act, "Accused cannot be compelled to give passwords as he is protected by Article 20(3) of the Constitution as well as section 161(2) of CrPC. But, investigating officer has right to access the data of the computers and its software which were seized with the help of agencies or experts at the risk of accused of loss of data". The CBI court has relied upon various Supreme Court of India (SCI) judgements for this case. In *State of Bombay Vs Kathi Kalu Goad* case, SCI says, passwords are testimonial fact and used to find the evidence against accused. This comes under self-incrimination; hence the accused should not be forced to give the passwords. In this particular *Mahesh Kumar Sharma Vs CBI case*, CBI court says, if the passwords to be used only for identification and comparison with other evidence, this comes under second category which is not protected by Constitution and accused can be compelled to give the passwords.

DIGITAL LIBRARY OF SVPNPA

Sardar Vallabhbhai Patel National Police Academy (SVPNPA) has come up with e-Library which can be accessible by all the IPS officers from all over India. This e- Library has subscriptions of world-famous publishers such as *Taylor & Francis*, *Springer*, *LexisNexis*, *Live Law*, *Manupatra*, *SAGE*, *Emerald Insight*. The various journals and e-books can be accessed from all these sources.

There are around *64,810* e-books, *19,156* journals, *39* magazines that can be accessible through SVPNPA e-Library. Also, *Live Law* database, *Lexis Nexis* Database and *Manupatra* Databases are accessible. Around 3 lakhs videos are accessible related to several subjects. For more details visit: *https://www.elibrary.svpnpa.gov.in/*. For sign-up and other details please write an email to: *vamsikrishna@svpnpa.gov.in* .

[7] Citation*: Alok Kumar vs Union of India and Ors. Writ Petition (PIL) No. 151 of 2021*

[8] Citation*: CBI vs Mahesh Kumar Sharma CBI No 31/2021, orders released on 31/10/2022*.

CYBER FORENSICS AND INVESTIGATION

INNOVATIONS AND BEST PRACTICES

Deepfake Technology And The Ways To Regulate It [9]

A technology which can use machine learning algorithms, audio and artificial images to create fake avatar (deepfakes) that does not exist is called as deepfake technology. The deepfakes can spread misinformation. Deepfakes can replace the appearance of a real person, their voice or both with fake/artificial appearance or voice. With the evolution or advancement of the technology, it is challenging and harder to detect deepfakes.

Identity theft, financial frauds, attacks involving disinformation, manipulating elections, social engineering are some of the adverse applications of deepfakes. It has been identified that deepfakes were used to impersonate various personalities such as former U.S. Presidents Barack Obama and Donald Trump, India's Prime Minister Narendra Modi, Facebook chief Mark Zuckerberg and Hollywood celebrity Tom Cruise among others.

As per the policy, the companies and people who are responsible for creating deep fakes must ensure that the content created using deepfake technology need to explicitly labelled and can be traced back to its source.

China has setup a policy to restrict deepfakes. As per the policy, the companies and people who are responsible for creating deep fakes must ensure that the content created using deepfake technology needs to explicitly be labelled and can be traced back to its source. As per the China's new rules, all the people and companies that uses deepfake technology should receive consent from individuals prior editing their voice or image.

Also, for reposting news which was made using deepfake technology, companies or people have to use only government approved list of news outlets.

Political direction and public opinion should be maintained, and the deep fake tech companies should abide by local laws and respect ethics.

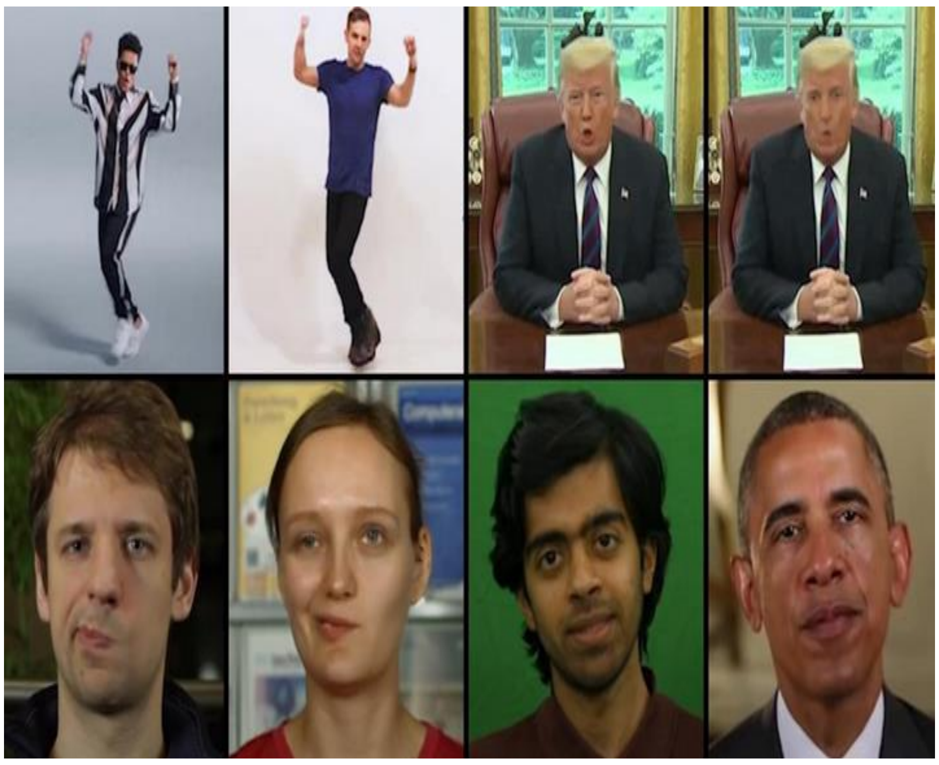


Figure 1: Real and fake(synthetic) images

Figure 2: Collection of deepfake images

[9] *Article and Images References: https://www.thehindu.com/sci-tech/technology/deepfake-technology-how-and-why-china-is-planning-to-regulate-it/article66277740.ece;https://towardsdatascience.com/deepfakes-an-unknown-and-uncharted-legal-landscape-faec3b092eaf?gi=5c8218bc5a07; https://www.technologyreview.com/2020/06/12/1003475/facebooks-deepfake-detection-challenge-neural-network-ai/*

EVENTS AND TRAININGS

A Five-Day Training Program on "***Advanced Digital Forensics***" sponsored by *I4C*, Ministry of Home Affairs was conducted from 28-11-2022 to 02-12-2022 in *SVPNPA*. The delegates from various states in the ranks of from ASP to ADG, Assistant Directors of various organizations of India, and foreign delegates from ***Maldives, Sudan, Tanzania*** and ***Ghana*** have attended the training.

Sardar Vallabhbhai Patel National Police Academy, Hyderabad-500052
5 days Course on "Advanced Digital Forensic for Law Enforcement Agencies"
(28th November to 02nd December, 2022)

Sitting left to Right S/Shri : Deepak Singh, C. Vamsi Krishna, AD (IT), Dr. Rohini Katoch, Sepat, DD(IS -I), Seju P. Kuruvilla, DD(OD), N. M. Reddy, JD(BC) A.S. Rajan, Director (SVPNPA), Dr. K.P.A. Ilyas, AD(Est-I) & Course Director, Dr. Ram Niwas Sepat, DD(Works), AYV Krishna, Dheeravath Kishan Singh, V. Karthick.
Standing Left to Right (1st Row) : K. Narasimha Swamy, Angela Mseke, Shaabani Puya, Greta Banda, Siman Saeed, Walaa Gaafer Mohamed Talha, Richmond Donkor, Aishwarya Sharma K. Sreedevi, Ibrahim Nazeeh Nazeeh, Raufuddheen Saeed.
Standing Left to Right (2nd Row) : Shaji Suganan, Garikapati Bindu Madhav, K. Ganga Reddy, Paladhi Krishna Murthy, Jeshtadi Anyonya, Shekhar H T, Motasim Elobaid, Ishtyaq Ahmed Kacho, Sayak Das.
Standing Left to Right (3rd Row) : Jitendra Singh Dangas, Rasheed Ahmad, Pawan Kumar, Akash Markam, Pritam Kumar, Krishna Kant Saini, Manoj Swargiary, Jassir Ashraf Mir

A Five-Day Training Program on "***Cyber Security Investigation Course***" sponsored by I4C, Ministry of Home Affairs was conducted from 05-12- 2022 to 09-12-2022 in *SVPNPA* for the judicial officers.

A Two Days Course on "***Crime Against Women and Children***" from 28-12 2022 to 29-12-2022 for Odisha Police was delivered at *Biju Patanaik State Police Academy*, Odisha by the Team of *SVPNPA*. The participants are from Odisha Police of various ranks from Sub-Inspector to Deputy Superintendent of Police. The number of participants trained is 22.

Courses on ***Malware and Network Forensics, Darkweb & Cryptocurrency Investigation, Advanced Digital Forensics*** for *Maharashtra Police at Maharashtra Police Academy*, Nashik from 12-12-2022 to 23-12-2022 were delivered by *SVPNPA* Team.

TECHNOLOGY WORKAROUNDS

ANDROID MOBILE: PATTERN BYPASS

-Shri Arif Ali Khan, Chief Forensic Analyst, NDCRTC

Problem Statement:
You have received an android-based mobile device for investigation which is in *ON* and locked condition, protected by a pattern lock.

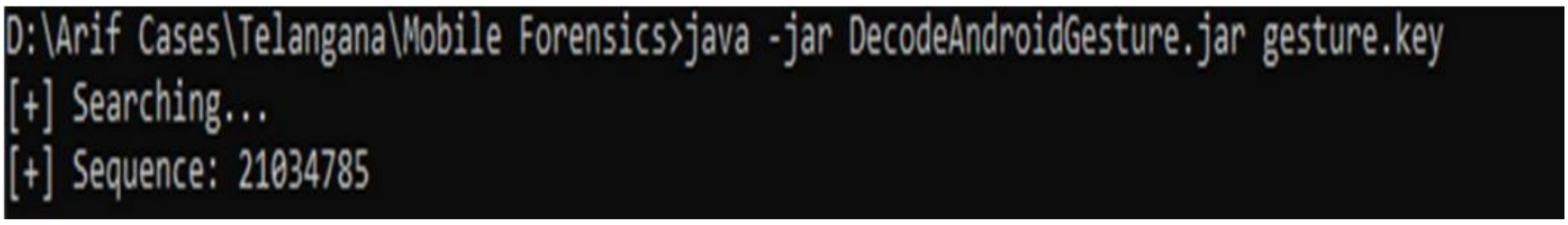
Possible Solutions:
1. Request the accused for password (Good luck!)
2. Use password-reset mechanisms (Beware! These may also result in complete wiping of data.)
3. Forensic Tools to the rescue!

We tried connecting the device to *Cellebrite UFED*, a mobile forensic tool that supports various types of data acquisitions.

At first, we tried physical mode of data acquisition so that if we aren't able to bypass password, at least we get the entire data that may be used as evidence. Unfortunately, this type of acquisition required root access of the device, and the device that we had was not rooted.

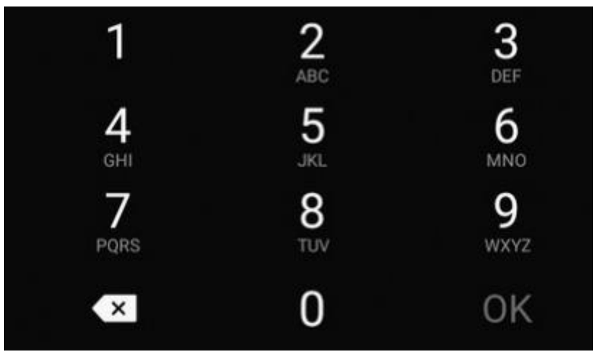
Next option, please!

We proceeded with the second most significant option of data acquisition, i.e., *File System* acquisition. This type of acquisition claims to acquire some important data from the device *even while the mobile is in locked condition*. We then followed the sequence of instructions as directed by the tool, and proceeded further. Incidentally, out of so many random files extracted by the tool which were seemingly of no use to us, we found a file **gesture.key** acquired from the device. We had information that android based mobiles store the pattern information in a file named *gesture.key*. We tried opening the *gesture.key* file using a generic text editor hoping to find some useful information. All we could see was some gibberish content. After some research, we found that the lock sequence/pattern information is encrypted with *SHA1* hashing function. Now, we tried figuring out the approach towards identifying the decrypted string and discovered a java program **DecodeAndroidGesture**, available on GitHub for the same. The tool was downloaded, and stored at the path where we had the *gesture.key* file, and was executed. Upon execution, an output containing a sequence was displayed as shown below.



```
D:\Arif Cases\Telangana\Mobile Forensics>java -jar DecodeAndroidGesture.jar gesture.key
[+] Searching...
[+] Sequence: 21034785
```

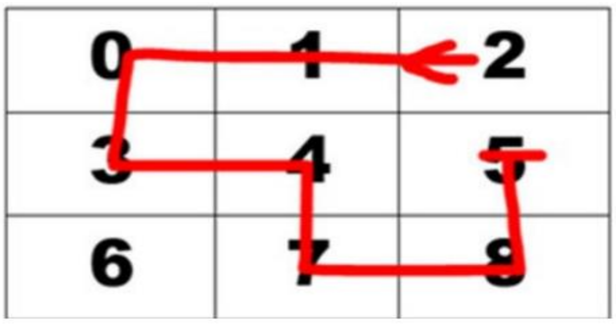
Next, we checked the dialpad of one of our phones to see the sequence of numbers. If you notice, the sequence/pattern identified by using the program was not possible using this layout, as 2-1-0 was not a feasible approach without having to traverse through either 4- >7, or 5->8.



1	2 ABC	3 DEF
4 GHI	5 JKL	6 MNO
7 PQRS	8 TUV	9 WXYZ
⌫	0	OK

Having realized that the above approach wasn't possible, we tried making possible approaches with a change in layout.

Finally, a layout beginning with 0 was designed to see if the same combination was feasible this way and it worked!!!



0	1	2
3	4	5
6	7	8

CYBOTS -CYBER BEAT CONSTABLES

- Shri Paras Rana, Shri Adarsh Kant Shukla
(IPS Probationers of 74 RR)

Introduction:

Crime prevention is one of the primary objectives of police machinery in modern nation-states. For this, even in ancient times, we had mechanisms like *Prahari* and *Digpala* who used to wander around the cities as patrolling agents. With the advent of democratic setup, this concept has been replaced by professional beat constables in Indian Police machinery. These beat constables are mandated to ensure regular monitoring of neighborhoods to prevent occurrence of crimes. In the 21st Century where we live in an era of parallel reality created by virtual spaces, the products of cyber world ranging from social media to dark web, occurrence of crime is no longer limited to physical space. Though we have beat constables in physical space, we do not have any sort of parallel mechanism in cyberspace, as the result of which, these unregulated cyberspaces have become hotbeds of criminal activities. It is in this context; the concept of a *Cyber Patroller Bot* is being proposed by us.

Crime And the On-Ground Situation:

Let us start with *Subreddits*, a *Reddit* discussion forum where the users would discuss and share their opinions about various topics. Few subreddit communities such as *r/jailbaits*, *r/rapingwomen* or *r/creepyshots* which were allegedly hosting and sharing content related to child pornography, private photographs of underage girls, taken without their consent, are identified. Also, it is identified that these *subreddits* were having discussions on why and how should one assault the women sexually with a checklist. The discovery of these controversial *subreddits* and the uproar among the activists led to shut down of these subreddits. How did these *subreddits* evade the regulation of *Reddit* moderators for so long?

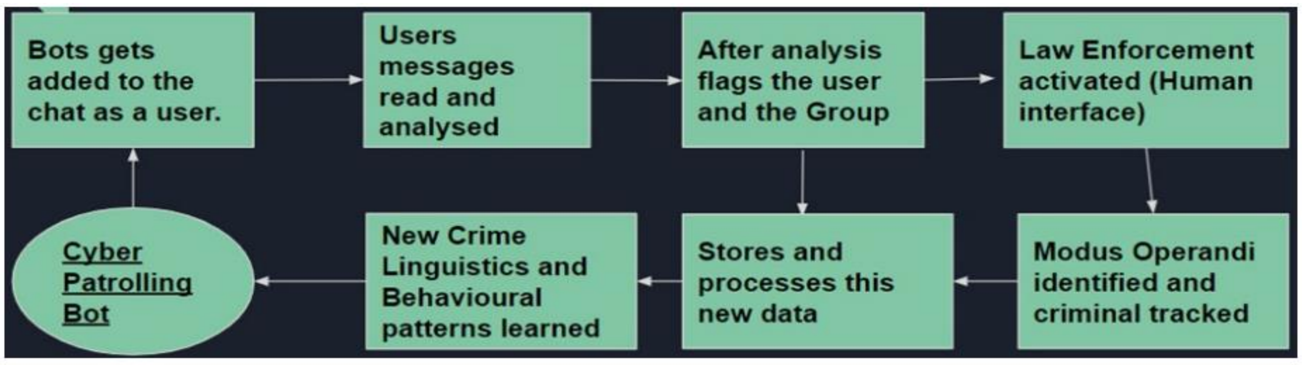
Let's talk about some of the *Telegram* channels. In the past, *'The Eagle of Khorasan'* was a *telegram* channel used for radicalizing the youth run by *Akhtar Hussain Lashkar*, having links with terrorist outfit *Al-Qaeda*, according to National Investigation Agency (NIA) reports. '*Poombatta*' was another *telegram* channel being run in Kerala for hosting and sharing child pornography. It was busted by *Cyberdome* team of Kerala.

Discord is a social media platform for engagement in the form of servers hosted by users. It was started as a forum for watching videos and playing games, but, later especially during COVID-19, it has attracted criminal minds across the globe owing to some of its advantages over other platforms. *Discord* started hosting servers meant for illegal drug trafficking, arms smuggling and revenge pornography, many of them busted by law enforcement agencies, while many continue being run privately.

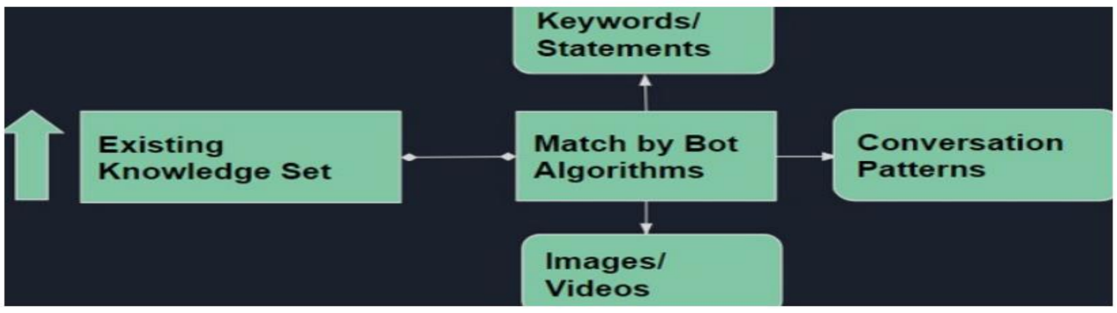
The Need for A Solution:

The commonality in the above mentioned three examples of crimes involving social media in luring the criminals towards these platforms is *Anonymity* and *end-to-end encryption* which makes it difficult to track the criminals. Additional features like 'Secret Chat' and 'Private Chat Rooms' where the messages get deleted automatically after a certain period, make it challenging for the investigators to trace the cyber offences committed by the criminals. The ineffective regulation due to delayed action or negligence on part of regulators and moderators on these platforms and the information asymmetry among law enforcement agencies followed by lack of specialized knowledge about the forums helps these communities being run in the underbelly of vast social media. Keeping in mind the challenges posed by these rising threats, we are proposing the idea of *Cyber Patroller Bot* or what we call it - a *'Bot Constable'* for cyberspace(internet), in line with Beat Constable for physical space. *Cyber Bots* (*CyBots*) can be a kind of virtual and autonomous software robots which would exist and roam around the cyber world i.e., internet or the other network (Dark web), and can interact with the systems or users who are part of these networks.

Working Architecture of Proposed Solution:


Bots gets added to the chat as a user.
Users messages read and analysed
After analysis flags the user and the Group
Law Enforcement activated (Human interface)
Cyber Patrolling Bot
New Crime Linguistics and Behavioural patterns learned
Stores and processes this new data
Modus Operandi identified and criminal tracked

Operational Architecture:

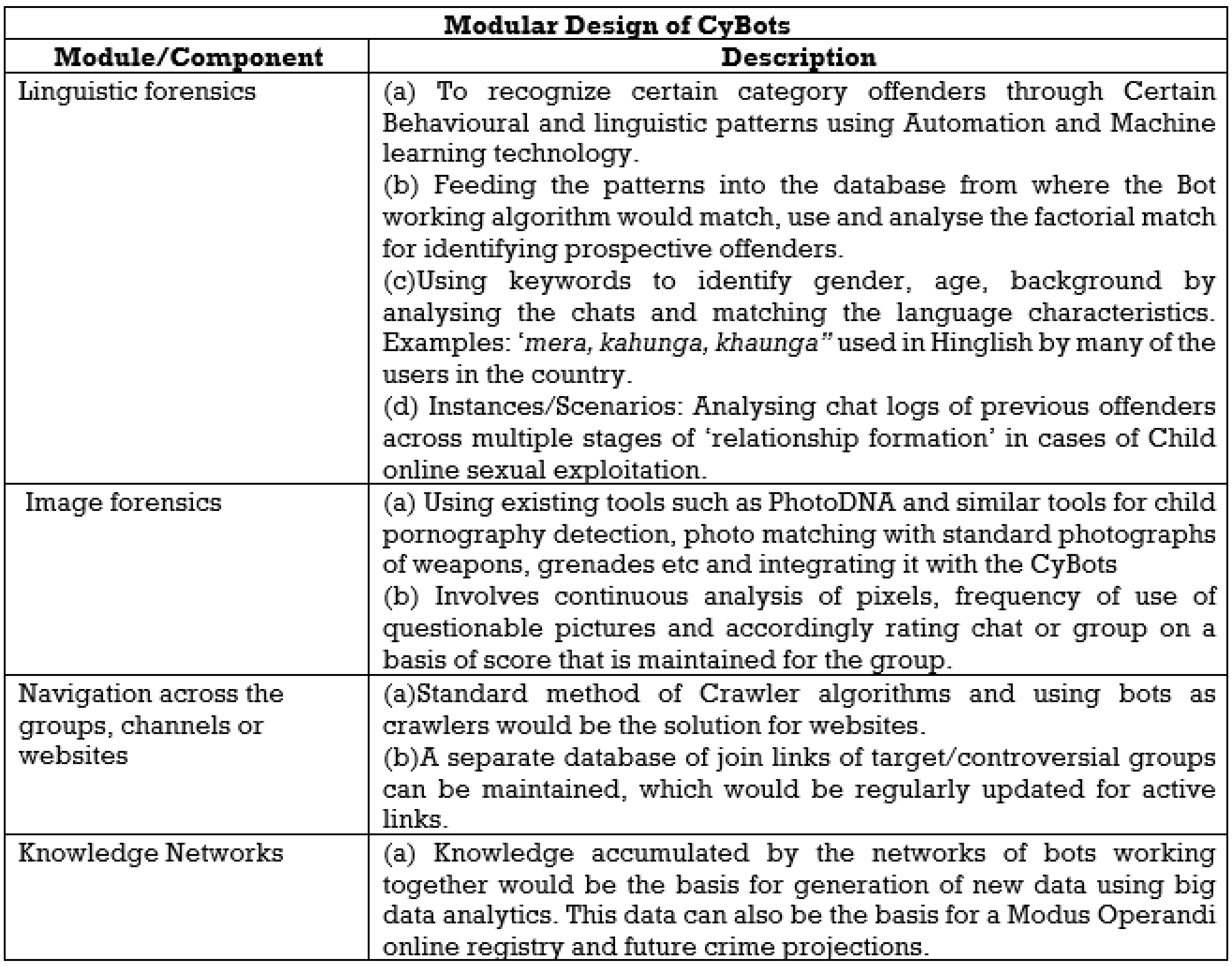


Detecting Cyber Crime- An analysis:

These *CyBots* would be programmed as Dynamic learners as they operate over connected networks, having an ever-increasing knowledge database. The solution involves a large, connected database which would assist the algorithm in identification, classification and flagging of users, social media groups or the websites to the law enforcement agencies for further information and action based on information available with the agencies. Multiple such projects of similar nature have been started by the police in

India, with the recent one for women safety launched by *Telangana Police* in November 2022. However physical internet users and human agents are used, forming specialized teams for such patrolling, and if we compare the costs involved along with Cost to Benefits ratio of such teams it is proportionately higher in the longer run and involves human limitations. It is analogous to a group of humans trying to race with a car on a straight metallic road, if you employ 1 person or 10 people, they won’t be able to chase the car in a normal scenario and only in the initial 5 to 10 meters they might match and catch it. So, this approach of tackling crime is much needed in these times. The task for the software proposed is to identify the target enclosures to classify them as problematic spaces.

Design Modules of CyBots:



Modular Design of CyBots

Module/Component	Description
Linguistic forensics	(a) To recognize certain category offenders through Certain Behavioural and linguistic patterns using Automation and Machine learning technology. (b) Feeding the patterns into the database from where the Bot working algorithm would match, use and analyse the factorial match for identifying prospective offenders. (c)Using keywords to identify gender, age, background by analysing the chats and matching the language characteristics. Examples: ‘*mera, kahunga, khaunga”* used in Hinglish by many of the users in the country. (d) Instances/Scenarios: Analysing chat logs of previous offenders across multiple stages of ‘relationship formation’ in cases of Child online sexual exploitation.
Image forensics	(a) Using existing tools such as PhotoDNA and similar tools for child pornography detection, photo matching with standard photographs of weapons, grenades etc and integrating it with the CyBots (b) Involves continuous analysis of pixels, frequency of use of questionable pictures and accordingly rating chat or group on a basis of score that is maintained for the group.
Navigation across the groups, channels or websites	(a)Standard method of Crawler algorithms and using bots as crawlers would be the solution for websites. (b)A separate database of join links of target/controversial groups can be maintained, which would be regularly updated for active links.
Knowledge Networks	(a) Knowledge accumulated by the networks of bots working together would be the basis for generation of new data using big data analytics. This data can also be the basis for a Modus Operandi online registry and future crime projections.

Initial Phase of Design and Implementation of CyBots:

At a basic level, we can design and implement *CyBots* to analyze the given text and assign a flag score based on its criticality. It can be ensured by

- Implementing the solution in lab environment
- Removing the biases from the results
- Adding the human interface
- Using a single language for preliminary checking of the effectiveness of CyBots

Limitations and Challenges:

- Datasets available from the archives of NCRB and other sources would not be in the required format. Also, the same might be limited in its scope for initial applicability, that would result in internally training the bots using the existing datasets.
- Initial Modelling might not work with desirable results, and the machine bias may creep in wherein certain attributes are automatically reflected in multiple results more than required.
- The whole system and data along with behavioral linguistic models may need remapping for complete program in case of using regional languages.
- Which theory to use for which model of behavioral analysis, and linguistic scanning is challenging for its implementation.

Conclusion:

Identification of relevant criminology models which are to be used along with identification of language specific forensics would be the first step to create database of target data. Then, structural analysis of the problems to define an elaborate system architecture would shape the implementation. Once a full-fledged solution of *CyBots* is developed, it can help and serve the Indian Police machinery in detecting, responding and preventing crimes in less amount of time and subsequently can reduce the crime rate that enables the nation development at a faster pace.

***