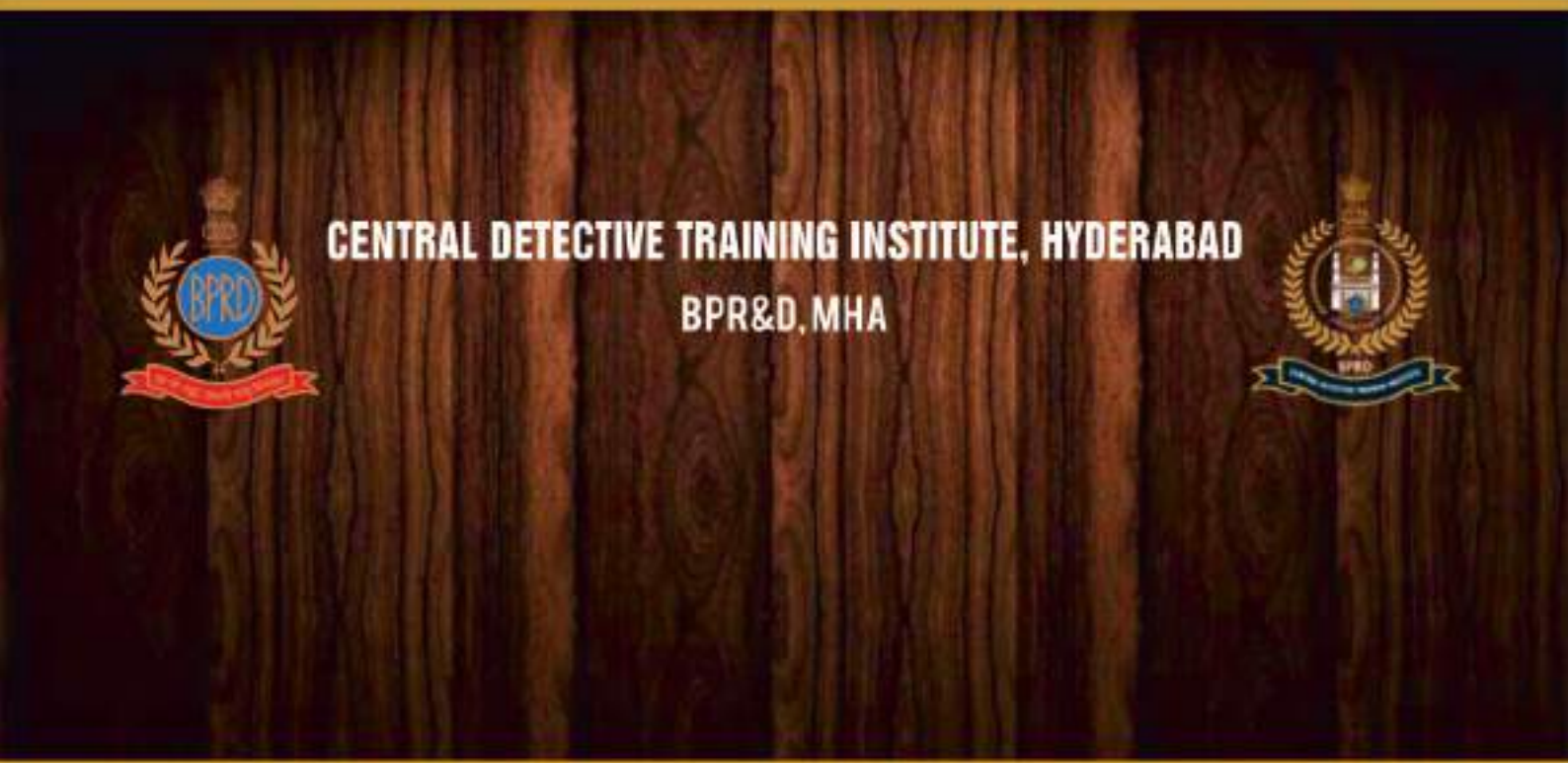
Apr-June 2025

CDTI, HYDERABAD

Bulletin

HORIZON

Our Motto "ज्ञानं सम्यग् वेक्षणम्" which means
"WISDOM LIES IN PROPER PERSPECTIVE"



A Quarterly Bulletin of Central Detective Training Institute, Hyderabad

MESSAGE OF THE DIRECTOR

Shri. Salmantaj Patil, IPS
Director

It gives me immense pleasure that the Central Detective Training Institute, Hyderabad is launching its quarterly year news magazine **"HORIZON"** for the period April to June, 2025.

CDTI, Hyderabad is designated to be the Centre of Excellence for **"Police Technology, IT and Cybercrime"** and coupled with the establishment of **"National Cyber Research, Innovation and Capacity Building Centre (NCRI&CB)"** under the Indian Cyber Crime Coordination Centre (I4C), MHA, enabled CDTI-Hyderabad to hone the investigative skills of police officers in the field of cybercrimes.

CONTENTS

COURSES CONDUCTED FROM APRIL TO JUNE, 2025

From 01st Apr to 30th Jun, 2025 a total of 33 Courses (including Workshops,Webinars, Conferences) were conducted in which 1342 Officers were trained.

S. No.	Name of the Course	Date		No. of Participants
		From	To	
1.	Workshop on Cloud Forensics	01.04.2025	01.04.2025	20
2.	Workshop on Cyber Forensics	02.04.2025	02.04.2025	28
3.	Webinar on protecting children in Meta Verse: Discuss potential risks and safety measures for children	04.04.2025	04.04.2025	39
4.	Conference on Cyber Crime Investigation SOPs	08.04.2025	08.04.2025	50
5.	Workshop on Social media crime investigation techniques	15.04.2025	15.04.2025	65
6.	Webinar on How to report cybercrime, virus, ransomware & Malware	17.04.2025	17.04.2025	66
7.	Metaverse: Emerging challenges like virtual crimes, cybersecurity issues, and identity theft within virtual environments	21.04.2025	25.04.2025	28
8.	Social Media Investigation & Cyber Threat Analysis	21.04.2025	25.04.2025	36
9.	Basic Cyber Crime Investigation and CDR IPDR Analysis (at DPO, Rajanna Sircilla)	29.04.2025	30.04.2025	104
10.	CDR IPDR Analysis & MLAT	05.05.2025	09.05.2025	38
11.	Basic Cyber Crime Investigation and CDR IPDR Analysis (at DPO, Adilabad)	07.05.2025	08.05.2025	56
12.	Webinar on Humanitarian and empathetic approach towards drug users	09.05.2025	09.05.2025	89
13.	Webinar on New Criminal Laws - 2023`	13.05.2025	13.05.2025	58
14.	Webinar on Understanding trends in Urban Policing	13.05.2025	13.05.2025	42
15.	Webinar on Leveraging databases for effective policing	14.05.2025	14.05.2025	41
16.	Conference on AI in policing and Smart Policing; AI based crime analysis; Integration of technology & community engagement	14.05.2025	14.05.2025	55
17.	ToT Course on Strategies for Efficient Investigation & Trial	15.05.2025	16.05.2025	20
18.	Cyber Security & Forensics (Level -2) in collaboration with CDAC, Hyderabad	19.05.2025	22.05.2025	38
19.	ATM & Digital Payment frauds and AI based Crime Analysis	19.05.2025	23.05.2025	22
20.	Basic course on Cyber Crime Investigation and Digital Forensics	19.05.2025	23.05.2025	24
21.	Intermediate course on Cyber Crime Investigation and Digital Forensics	26.05.2025	30.05.2025	24

22.	Fraud detection and investigation: Hospital, passport, digital arrest, examination frauds, lottery scams, e-ticket scams and real estate frauds	26.05.2025	30.05.2025	22
23.	Webinar on counter illegal migration through international borders	26.05.2025	26.05.2025	62
24.	ToT NCL (Batch 1 Part 1) in collaboration with PMA team	09.06.2025	11.06.2025	25
25.	Ethical Hacking and Counter measures	09.06.2025	13.06.2025	20
26.	Digital Evidence in Cloud Computing, Securing Critical Infrastructure from Cyber Attacks, and Legal-Ethical Challenges in investigating cyber crimes in encrypted environments	16.06.2025	20.06.2025	20
27.	Investigation of Deep and Darknet crimes, tracking of Crypto Currency driven offences and misuse of Crypto-currency	16.06.2025	20.06.2025	24
28.	ToT NCL (Batch 2 Part 1) in collaboration with PMA team	23.06.2025	25.06.2025	24
29.	Cyber Security & Forensics (Level -3) in collaboration with CDAC, Hyderabad	23.06.2025	26.06.2025	21
30.	Money-Making Scams: Ponzi schemes, fake investment offers, and online financial frauds, et	23.06.2025	27.06.2025	27
31.	Cyber Crime Investigation and CDR IPDR Analysis (at DPO, Dharashiv, Maharashtra)	24.06.2025	25.06.2025	101
32.	AI, Crypto Currency & Block Chain Technology & Misuse of Crypto -Currency	30.06.2025	04.07.2025	29
33.	ITEC Course on Digital Evidence investigation (for Sri Lankan Police)	30.06.2025	11.07.2025	24
	TOTAL			**1342**

CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD

Course on "Social Media Investigation&Cyber Threat Analysis "

21-04-2025 to 25-04-2025

Sitting (L to R) S/Sri:-Uppada Venu,Inspr(Admn)CDTI, Sridher Nateti,Cyber Crime Expert,Hyd,Shailendra Sharma, 2IC, BSF, Dr.S.Karthikeyan, Vice Principal, CDTI, Rajashekara.N, IPS,Director, CDTI, Ajay Pal, 2IC, BSF, Arvind Chaudhry, ips, SP(Himachal Pradesh), K.K.V.Reddy, Dy.SP, CDTI, Sandeep Mudalkar, Cyber Expert,Hyd

Standing 1 (L to R) S/Sri :-Pralay Shill, Naik, Army/Military Police, Deepanshu, SI,BSF, Pravin Ananda Mahale, SI(Mah),Manas Ranjan Barik, DSP(Odisha), Karan Pamoria, A/Comdt,CISF, Mulnayanaben Danabhai Mir, SI(Guj), Mrs.Deepa, SI, RPF, Ms.Sahnaj Khatoon, ASI(WB), Manda Mallesham, ASI, RPF, Nelson CS, SI(Ker),Vikas Yadav, SI,CISF, Vinod Mehta, SI,CISF, Gopikrishna, SI(TG).

Stnding 2 (L to R) S/Sri :-A.Senguttuvan, SI(TN), Pushpraj M.Dhadhal, PSI(Guj),Vishnu Prakash Singh, ASI,BSF, Inderjeet Singh, SI, CISF, Aliur Rahaman Mandal, ASI (WB), Gopal Lamani, ASI, CRPF, Neeteesh Kumar, SI(Jharkhand),Borkar R.K.I, Inspr, CISF, Md.Nasar Khaled, DSP(WB), Shaik Junaid, SI(RI)(TG), Gobinda Roy,ASI(WB), Nizamudeen A, Inspr(Ker).

Stnding 3 (L to R) S/Sri:- Jeya Pandiyan G, SI(TN),Domala Vamsee Krishna, HC(TG), Joy Dutta,SI(Kolkata Police),Kankala Suresh, SI(TG),Sourav Roy, SI(Kolkata Police), Nagesh Gautam Salve, Inspr(Mah), Sanjay Tatya Lokhandemali, SI(Mah), Rajesh Sah, Nb(Sub), Army/Military Police.

CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD

Course on" ToT Course on Strategies for Efficient Investigation & Trial"

15-05-2025 to 16-05-2025

Sitting (L to R) S/Sri:-Uppada Venu, Inspr(Admn)CDTI,Mohd.Abdul Rahman(Faculty), A.Vamsi Krishna, Asst.Director(AP)FSL, B.V.S.Siva Prasad, Asst.Director(AP)FSL, Rajashekar N,IPS,Director, CDTI, Dr.S.Karthikeyan, Vice Principal, CDTI,K.K.V.Reddy, Dy.SP, CDTI, Gaurav Singhal, Associate.Director(PMA,E&Y), N Ravva,-Senior Consultant(PMA,E&Y).

Standing 1 (L to R) S/Sri:-Husuluri Siva Rama Krishna, Addl.P.P(AP),R.Rajesh, Addl.PP(AP),M.Sundaraiah Yadav, Addl.PP(AP),Raja Sekhar Batti, Spl.PP(AP), G.V.Teja, Addl.PP(AP), Kinjarapu Srinivasa Rao, Addl.PP(AP),Meppparapu Balakrishnama Naidu, Addl.PP(AP), K.V.Rameswara Reddy, Addl.PP(AP),B.Siva Prasada Rao, Addl.PP(AP), Borkasam Sreenivasulu, Addl.PP(AP).

Stading 2 (L to R) S/Sri-M.Nagi Reddy, SI(TG) ,M.Manohara Chary,CA, CDTI, Konda Ramesh,Inspr(TG),T.Sreenivasa Rao, Inspr(AP), Panneeru Vadagiri, SI(TG),G.Nagaraju,-Inspr(TG),Y.Venkateswarlu,Inspr(TG), P.Ramababu, Inspr(TG), Gosangi Ramakrishna Reddy, Inspr(Tech)(AP),B.Nagaraju, CA, CDTI.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Cyber Security & Forensics for Leas Judiciary,Level-2"
19-05-2025 to 22-05-2025

Sitting (L to R) S/Sri:-Sridhar Mateti,Cyber Crime Expert,Hyd, Tasneem,Sec in Command,ITBP,Mushtaque Hussain Shaikh,District Judge, Judiciary,Gohar Kumar Nimarna - - District Judge, High Court(WP),G.Sudheer Babu,IPS,Commissioner of Police,Rachakonda Police Commissionerate,Dr.S.Karthikeyan,Vice Principal, CDTI, P.Vimshikrishna,Police,Jr.Scientist -E,CDAC, Hyd.,G.Rajkumar,Dy.SP, Course co-Ordinator,CDTI, P.Sailaja, Scientist -D, CDAC,Hyd.

Standing 1 (L to R) S/Sri:-Abhishek Saxena,ASJ, High Court(WP),Pillari Krishna Reddy, Project Engineer,CDAC,Hyd.,Mrs.G.Nagamani, SI(AP),Mr.Sonal Gupta, Judge, Judiciary(MP), Mrs.Shaik Jubeda Begum,SI,TG),Mrs.Tejaswini Das, ASI,Odisha,Prosenjit Mukherjee, System Officer, High court(Kolkata),Tanvir Ikram Hazarika, SO,JMI(WP), - High court(Gauhati),Ashwin Subhash Alewar,CJSD&Addl.C.JM,Law& Judiciary(Meh.),Mimu Rabha,SI(Meghalaya),Devasmita Kalita,ACJM,High court(Gauhati)

Standing 2 (L to R) S/Sri:-Ravi Tank, PSI, Cyber Crime Police(Jamnagar), Robin T, Asst.Commnd,ITBP, Saleh Ahammad, Chief Judicial Magistrate(Assam), Mandeep Dhanda, - -Deputy Commndt./ITBP, Sharad Jaiswal, Civil Judge Sr.Division, High Court(WP), Vikas Kumar, Deputy Commndt./ITBP, Soumik Bhattacharya, System Office -High Court(Kolkata), Sourish Saha, Technical Asst.,Judicial Department, Amarendra Hazarika,Judicial Officer(Assam), Shubhendu Mondal, System Officer, Judicial -(Kolkata), Nagarjyoti Choudhury, Chief Judicial Magistrate(Assam), Abhijit Dey, System Asst., Judiciary(Kolkata), Raghavender Gaddam, SI(TG), Shakeel - Awadhutrao Sutrave, Civil Judge Jr.Division, Law and Judiciary(Meh.), Haresh Parala,SI(Tech.)(TG), Vinayak Shripatrao Patil, C.J.J.D and JMFC, - Law and Judiciary(T),Sanjay Kumar, Insp(TG),Tengsimgla K.Monk, SI(Meghalaya).

Standing 3 (L to R) S/Sri :-Goutam Singh, ASI,RPF(Gr.),S.Raghuveer, Dy.SP/CBI(AFL),Aloysius. A, SI(Ker.),Pradeep.P, SI(Ker.),Harsh Kumarjiya, ASI, SPO officer(Jamnagar), M.Harish Kumar,SI(TG), P.Hasan,T.I, Insp(Ker.)

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" ATM and Digital Payment Frauds & AI Based Crime Analysis"
19-05-2025 to 23-05-2025

Sitting (L to R) S/Sri:-Chakrapani,ACP,Rachakonda(TG),Sridhar Mateti,Cyber Crime Expert, CDTI, Abhilash Rao Kandari, Cyber Expert(TG), K.K.V.REDDY, Dy.SP, CDTI, G.Sudheer Babu,IPS,Commissioner of Police,Rachakonda Police Commissionerate, Dr.S.Karthikeyan,Vice Principal, CDTI,S.Alpurappa, Insp(Trg.), CDTI, Upendra Verma, Insp(Addmn),CDTI, Election Reddy, C.I, Rachakonda(TG).

Standing 1 (L to R) S/Sri :- Ranajith Nath, SI(WB), Ravi Ranjan Singh,ASI(Bihar), Md.Istiyak Ahamad, SI(Bihar), Nunu Das Roy,Insp.(Jharkhand), Mrs.Sumeeta Gupta, Insp(MP), Ms.Kalpana Rajpoot, Insp(WP), Mr.K.K.Asodariya,SI(Guj.), Farhan Nagalmeera Khan, SI(TG), Moreshwar Laxmanrao Pendam, Insp(Meh.), Vijay Rao,SI,(TG), Harsh Devmani,SI(Guj.).

Standing 2 (L to R) S/Sri:-B.Nagaraju,CA,CDTI, D.R.Bathrise,SI(Guj.),Sateyendra Kumar,ASI,Jharkhand, Suresh Constable(TG),D.Srinivas,SI(TG),Nabanita Saha,ASI,Tripura, Santu Ray - ASI(WB),Laxman Singh Pace,SI(MP), Pramod Goud,RSI(TG),Bappa Ghosh,ASI(WB),Sunil Sharma,SI(Exe.)(CISF),M.Allu Prasad, SI(Exe.)(RPF),D.V.Jaya Kumari,SI(T

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Basic & Intermediate Course on "Cyber Crime Investigation & Digital Forensic"

19-05-2025 to 30-05-2025

Sitting (L to R) S/Sri- Sridhar Maletl, Cyber Crime Expert, CDTI, Ramesh Kumar Nagle,Inspr(MP), Akhilesh Rao Kanduri, Cyber Expert(TG), K.K.V.REDDY, Dy.SP, CDTI, Sri Sudheer Babu, IPS,Commissioner of Police,Rachakonda Police Commissionerate, Dr.S.Karthikeyan, Vice Principal, CDTI, Rambabu, Inspr(TG), Srinivas Akula,Inspr (TG),Uppada Venu, Inspr(Admin)CDTI.

Standing 1 (L to R) S/Sri : Ahmad Ali Ansari,ASI(Jharkhand), Ram Kishore,ASI(Jharkhand),J.S. Zapadiya,SI(Gujarat),Sonu Kumar Singh,ASI(Bihar), Ms. Priti kumari,SI(Bihar), Mrs. Dropati Sahu,ASI(MP), Goutam Sarkar,Inspr(WB), Snehasish Das,Inspr(WB), Salimbhai B. Makrani,ASI(Gujarat), Ranjeet Kumar Singh,ASI(Jharkhand), Hav(MP), Shridhar Kalaodagi,Army.

Standing 2 (L to R) S/Sri- Ms. Pratima kumari,SI(Bihar), Ms.Aastha Rana,DSP(Gujarat), N.Manohara Chary, C.A,CDTI, Rupesh Kumar Nayak,ASI(Odisha),Hav (MP),Shashi Karan,Army, Hav (MP),Gourav Kumar, Army, NK (MP),Raju Yadav,Army,Chandan Kumar,SI(Bihar), Balaji Macchindra Mulke,SI(Mah), Mrs. Meena Arma,Inspr(MP), Hav(MP),Lingeswaran N,Army.

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Investogation of Deep & Darknet Crimes,tracking of Crypto Currency driven offences and misuse of Crypto-currency"

16-06-2025 to 20-06-2025

Sitting (L to R) S/Sri- K.Rajesh Babu, Inspr(AP),Shaileshkumar S.Mirgodal, Inspr(Exe)(Mah),Santosh Kumar Poddar, Dy.SP(Bihar), K.K.V.Reddy,Dy.SP,CDTI,Sri.Mantaj Jafaraj Patil, - IPS, DIG,Director, CDTI, Dr.S.Karthikeyan, Vice Principal, CDTI,E.Prashanth, Cyber Expert, Vijay W.Koladara,Inspr(Guj), Uppada Venu, Inspr(Admin)CDTI.

Standing 1 (L to R) S/Sri- Sajesh C.Jose,SI(Ker),Gaurav Sharma,SI(RO), BSF,Vijay Kumar Yadav,Inspr(Bihar),Mrs.Vidhyalakshmi S,SI(TN),Ms. Bharti ardbho gojiya,ASI(Guj), Mrs.Y.Priyanka, -SI(TG), Ms.Sneha A.Varsha,SI(TG), Rabindra Kumar, Inspr(Bihar), Sampat Ranganath Chemate, API(Mah), Asaduzzaman, ASI(Kolkata), Firoj Mondal,Sergent - (Kolkata), Elbarun Karmakar, ASI(Kolkata).

Stading 2 (L to R) S/Sri- Ankit, SI(TG), B.Srikanth Reddy, Inspr(TG), Pramod B,SI(Kar), R.C.Solanki,SI(Guj), Biju Uhang,SI(WB),Tapas Kumar Ray, SI(WB),Indrajit Pramanick, SI(WB), Mir Murshid Ali, SI(WB).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" Digital Evidence in Cloud Computing,Securing Critical Infrastructure from Cyber Attacks, And Legal-Ethical Challenges in Investigationg Cyber Crimes in Encrypted Environments

16-06-2025 to 20-06-2025

Sitting (L to R) S/Sri- Mohammed Azharuddin, Dy.SP(Bihar),Vinay Kumar Singh,Inspr(Bihar), Abhinandan Kumar Singh,Inspr(Bihar), Sandeep Mudalkar,Cyber Expert, Salmanraj Jafaraj Patil,IPS,DIG,Director,CDTI,Dr.S.Karthikeyan,Vice Principal,CDTI, Ms.V.B.Vash, Inspr(Guj), G.Rajkumar,Dy.SP,Course co Ordinator,CDTI, Uppala Venu, Inspr(Admin),CDTI.

Standing 1 (L to R) S/Sri :- Rajesh Kumar, SI(GD)(Haryana), Naresh,SI(Haryana), Arif Ahmed Patel, ASI(Guj), Ramsinghbhai Valji, ASI(Guj), Lyotiaranjan Behera, SI(Odisha), Nowshad E.-SI(Ker), Tausif Akbar, SI(WB), Vimal Chandran,SI(Ker), Manish Kumar, ASI(Haryana), Laxmi Pati, Inspr(Tech)BSF.

Stading 2 (L to R) S/Sri:-Aniket Sankpal,SI(Maha),Kunal K.Verlekar, SI(Goa), Sanjeet, SI(Haryana).

CENTRAL DETECTIVE TRAINING INSTITUTE,HYDERABAD

Course on" ToT on New Criminal Laws-2023" in Collaboration with Ernst & young LLP(PMA)

09-06-2025 to 11-06-2025

Sitting (L to R) S/Sri- Md.Abdul Rahaman,DSP Retd(TS), G.Sreenivasarao, Spl.PP(AP),Srinu Reddy Palaparthi, APP(AP), K.K.V.REDDY, Dy.SP,CDTI, Salmanraj Jafaraj Patil, IPS,DIG, - Director, CDTI, Dr.S.Karthikeyan, Vice Principal, CDTI, Kommineni Venu Gopal, Spl.PP(AP), P.Ramesh, Dy.SP/DSP(AP), Harshavardan Singh, Consultant, EY.

Standing 1 (L to R) S/Sri :- Tallapalli Vijay Kumar,Asst.PP(TG),V.Amar Srinivas,Spl.PP(AP), Y.Sreehari, Addl.PP(AP),K.Satyanarayana,APP(AP),Vaka Raja Kumar,Addl.PP(AP),Mrs.Duddukuri-Haritha,SI(TG), D.Nagababu, PP(AP),K.Suryaraju, Addl.PP(AP), Ravula Veerababu, Deputy Jailor(AP),V.Anjinaik, Deputy Jailor(AP),E.Subrahmanyeswararao, - Inspr(AP).

Stading 2 (L to R) S/Sri:-Aruta Jayaraju,SI(TG),K.Ravikumar, SI(TG), D.Gangadhar, Deputy Jailor(AP),Pallarao Bathini, SI(TG),Ramireddy, ASI(TG),Chandrasekhar, ASI(TG).

Stading 3 (L to R) S/Sri: Ch.Nagaraju, SI(TG),Vanam Saidulu, SI(TG), Rajasekhar Reddy ch, Dy.Jailor(AP), R.Ramulu, SI(TG).

CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD

Course on" ToT on New Criminal Laws-2023" in Collaboration with Ernst & young LLP(PMA)
(Project Management Authority)
23-06-2025 to 25-06-2025

Sitting (L to R) S/Sri-G.Ravi Babu, Jailor(AP),K.K.V.Reddy,Dy.SP, CDTI, M.Venkat Reddy, PP(AP), Md.Abdul Rahman, DSP(Rtd), Sahmantaj Jafartaj Patil, IPS,Dir(I),Director CDTI, Dr.S.Karthikeyan, Vice Principal, CDTI, A.V.Narayana, PP(AP), Krushan Irani, Uppada Venu,Insp(Admn)CDTI.

Standing 1 (L to R) S/Sri -Y.Sambasiva Rao, ASI(TGL, Srinivasa Rao, ASI(TGL, Prasad, SI(TGL, Maruthu Venkata Sambasiva Rao, Add.PP(AP), G.Bala Ranga Swamy, Add.PP(AP), N.Srinivas Chandra Sekhar, Add.PP(AP), Ratan Koteswarareddy, Add.PP(AP), Hideyathali, Head Constable(TGL, B.Narayanaswamy, ASI(AP), S.Vinay -Constable(TGL, K.Laxman Chowdhary, ASI(TGL

Standing 2 (L to R) S/Sri: V.Chiranjeevi, SI(TGL, K.Venkatesh, SI(TGL, Naresh Gadari, Constable(TGL, B.Harish, Deputy Jailor(AP), J.Ashok, Constable(TGL), M.Yogesh Kumar, - Deputy Jailor(AP), Y.Sarveshwara Reddy, Constable(AP), N.Srinivas Constable(TGL), G.Parameswara, SI(AP), L.Sadhakar, SI(TGL

CENTRAL DETECTIVE TRAINING INSTITUTE, HYDERABAD

Course on" Cyber Security & Forensics (Level-3) CDAC"
23-06-2025 to 26-06-2025

Sitting (L to R) S/Sri-Arvind Singh, Judge, Judiciary(MP), Kishore Kumar Nirwan, ADJ, High Court(MP),Mushtaque Hussain Shaikh, Dir.Judge(Vig), Sahmantaj Jafartaj Patil, - - IPS,Director CDTI, Dr.PR. Eashwari, Director, CDAC, Indraveni K, Scientist-"F" CDAC,Hyd, Dr.S.Karthikeyan,Vice Principal, CDTI, Shahid Sajiduzzaman MH, - - Judge/CJ(D)Mahi), G.Rajkumar, Dy.SP, Course co Ordinator, CDTI.

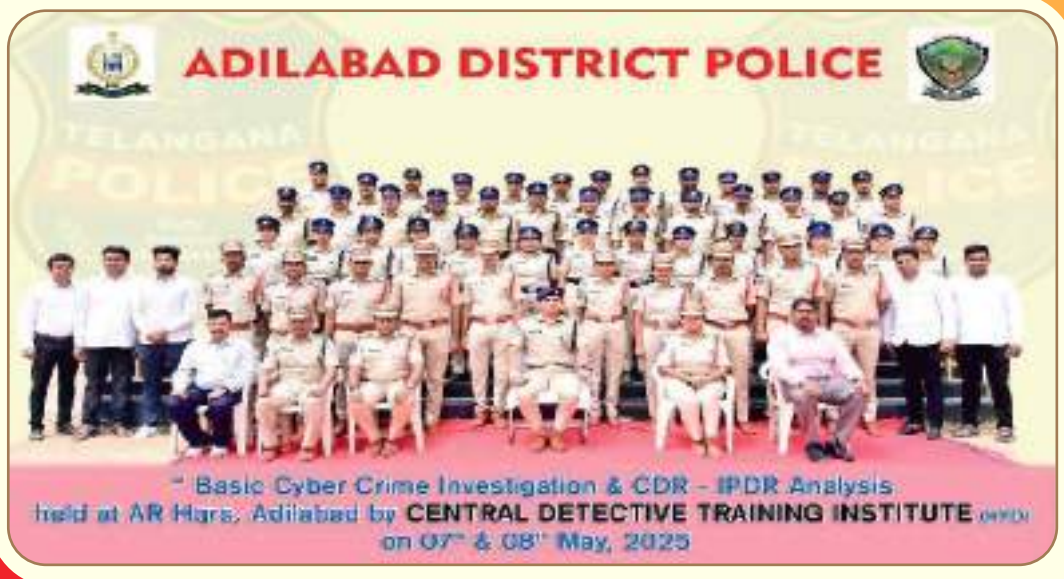
Standing 1 (L to R) S/Sri - T.Sanjay Kumar, Insp(TGL, Shamad Jaiswal, Judicial Magistrate(MP), Mrs.Gundre Bhavya Reddy,DSP(AP),PSailaja,Scientist-B, CDAC,Hyd, Ms.Sonali Gupta, - - Judge, Judiciary(MP),Mrs.Shaik Jubeda Begum,SI(TGL),Mrs.Tejaswini Das,ASI(Odisha),Vinaya Shripatrao Patil, Judge, CJ(D)Mah),Sharad Awadhutrao Surjuse -Civil Judge Junior Div(Mah), Ashwin Subhash Alwar, CJSD(Mah), Robin.T, AC, ITBP.

Standing 2 (L to R) S/Sri-Pradeep.P, Insp(Int), Bibin Raghuveer, DSP(AP), Vikas Kumar, DC, ITBP, M.Hitesh Kumar, SI(TGL, Dileep TG, Insp(Ker), Hareesh, SI(TGL), Mandeep Dhariwal - DC, ITBP, P.Hari Krishna Reddy, Project Engineer, CDAC, Hyd.

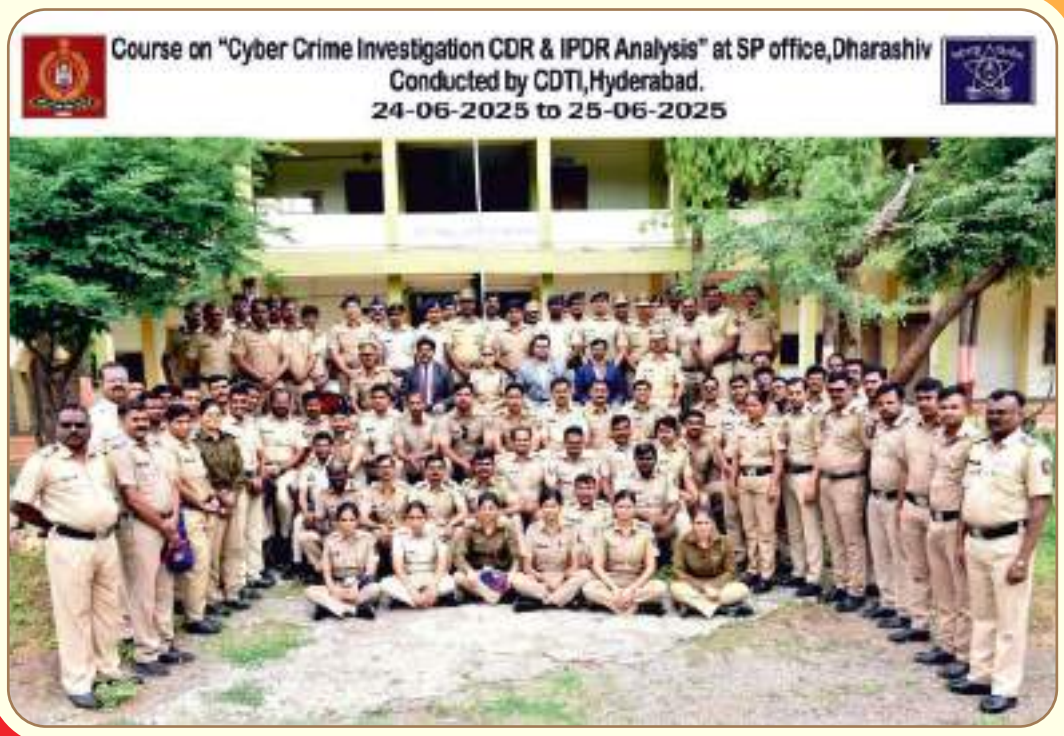
OUT REACH PROGRAMMES

1. Conducted two days course on **'Basic Cyber Crime Investigation & CDR-IPDR Analysis - issuing notices to various ISP and TSP'** for the Police Officers of the districts of Jagtial, Karimnagar, Siddipet and Rajanna Sircilla Districts of Telangana State on 29.04.25 & 30.04.25 at DPO Rajanna Sircilla, Telangana State. 104 Police Officers of the rank of Constable to Addl. SP have enthusiastically participated in the course.

2. Conducted 02 days course on **'Basic Cyber Crime Investigation & CDR-IPDR Analysis - issuing notices to various ISP, TSP'** on 07.05.2025 & 08.05.2025 at **AR Hqrs, Adilabad, Telangana**. 56 Police Officers of Adilabad District, Telangana state participated.



3. Conducted 02 days course **on "Cyber Crime Investigation and CDR-IPDR Analysis"** for the 101 Police Officers of Dharashiv District Maharashtra State, by resource persons of CDTI Hyderabad on 24 & 25.06.2025 at SP Office, Dharashiv District.



Presenting Memento to Ms. Ritu Khokhar, IPS, SP, Dharashiv District as token of appreciation on behalf of Shri. Salmantaj Patil, IPS, Director, CDTI, Hyderbad

AWARENESS PROGRAMMES

1. Conducted **Cyber Awareness Programme** for the students of **Kendriya Vidyalaya - II, Uppal, Hyderabad** on 11.04.2025. 36 students and 02 teachers participated in this Programme.

2. Conducted **Awareness Programme** on ‘Online Frauds’ for the students of **Megha City Junior college, Ramanthapur, Hyderabad** on 25.06.2025. 81 students and 03 teachers participated in this Programme.

3. Conducted **‘Cyber Awareness Programme and Safety of Women’** for the students of Shri Kendriya Vidyalaya No1 Uppal, Hyderabad on 26.06.2025. 50 students and 04 teachers participated in the Programme.

VISITS

- **CRPF DASOs** (Directly appointed Sub-Inspectors) who are presently undergoing Basic training at Central Training College, Coimbatore (Tamil Nadu) have visited CDTI Hyderabad in three batches on 7th, 8th and 15th of this month. Date-wise details of above trainees are as under: -

DASOs-97 Batch	Date	No of Trainees	No of Adm staff	Total	Came from
1st Batch	07/04/2025	59	06	65	GC CRPF, Hyderabad
2nd Batch	08/04/2025	60	07	67	GC CRPF, Rangareddy
3rd Batch	15/04/2025	62	04	66	GC CRPF, Rangareddy

The CRPF DASOs were also made aware about the functioning of the Institute and its training methods in standard investigation by using scientific evidence and methods. Shri Sridhar Mateti, Digital Forensic Expert explained the trainees on various types of Cyber & Social-media crimes and ways to prevent them, in a detailed manner. The trainees Sub-Inspectors also visited NCRI&CB Lab in Training Block.

- 09 Officers/ Staff of CDTI, Hyderabad visited **Indian School of Business (ISB), Hyderabad** and **International Institute of Information Technology (IIIT), Hyderabad** on 06.05.2025

- **RPF Officers** undergoing training at RPF Training Centre, Moula Ali, Hyderabad visited CDTI, Hyderabad on 23.05.2025 on an institutional visit.

Dr. S Karthikeyan, Vice Principal of CDTI, Hyderabad welcomed the participants

COLLABORATION WITH CDAC, HYDERABAD

- Four-day **Level -2 course on "Cyber Security & Forensics" for Law Enforcement Agencies (LEAs) and Judiciary** was organized by CDTI-Hyderabad in collaboration with the ISEA Project of MeitY and C-DAC, Hyderabad, **from 19th to 22nd May, 2025.** The course was designed specifically for Police Officers and Judicial Officers, 38 officers participated.
- The course was inaugurated by **Shri G Sudheer Babu, IPS, Commissioner of Police, Rachakonda Commissionerate.**
- Conducted a full day joint session on **"Judiciary limitations and challenges with respect to police functioning, Police officials limitations and challenges with respect to Judiciary functioning – enhancing the police and Judiciary Synergy"** on 21.05.2025 as per the **recommendation No. 97 of DGsP/ IGsP Conference, 2024.**

- Level -3 of the same course was conducted from 23rd to 26th Jun, 2025. 21 officers were participated

OTHER ACTIVITIES:

- Celebrated **World Environmental Day on 05.06.2025** at CDTI, Hyderabad with Officers/ Staff. ‘Beat Plastic Pollution’ oath was taken by the Officers/ Staff.

- Celebrated **International Yoga Day** on 21.06.2025 at the basket ball court of CDTI, Hyderabad with Officers/ Staff and trainees.

- A **career counselling session** about career progression after 10th and 12th to the wards of CDTI Hyderabad has been conducted today at 1630 hrs. to 1730 hrs. Director advised the students about the importance of choosing right career/path and directed to plan and study accordingly. Insp(Trg) S Alpurappa presented a PPT on the subject.

Workshop for Organizing 'National Police Hackathon'

- In compliance of instructions of the DGP/ IGP Conference, 2024; CDTI – Hyderabad proposed to conduct a National Police Hackathon (NPH). A meeting in this regard with the Heads of various Organizations/Institutes was organized under the Chairmanship of Shri Rajeev Kumar Sharma, IPS, DG, BPR&D, New Delhi on 23-06-2025 at the Conference Hall of CDTI, Hyderabad to discuss about organizing a "National Police Hackathon" in collaboration with reputed Institutions.

- Officers from SVP NPA, Centre for Good Governance, Telangana, Hyderabad; Telangana Cyber Security Bureau; Ms. P.R. Lakshmi Eswari, C-DAC, Hyderabad; ISB, Hyderabad; CFSL, Hyderabad; DSCI, Hyderabad; NIC, Telangana; IIT, Hyderabad and NFSU, Dharwad, Karnataka have participated in the meeting. DG, BPR&D has circulated the problem statements to the participants and requested them to select a topic on which a National Hackathon can be organized to find a solution to the problem statements.

- The DG, BPR&D thanked the officers for having accepted the invitation which resulted in very useful deliberations.
- On 26.06.25, Director, CDTI, Hyderabad had a meeting with Ms. Shikha Goel, IPS, DG Telangana Cyber Security Bureau and Shri Harshvardhan, IPS, SP CSB on organizing National Police Hackathon. It was decided that in near future BPR&D and CSB will jointly organize the NPH.

ITEC (Indian Technical and Economic Cooperation) course :

- Scheduled ITEC course on 'Digital Evidence Investigation' for the Sri Lankan Police Officers from 30.06.2025 to 11.07.2025. 24 Police Officers of the rank of ASP/ SP reached at the new hostel of CDTI, Hyderabad on 29.06.2025.

- Dr. G K Goswami, IPS, ADGP & Director, UPSIFS, Lucknow inaugurated the course on 30.06.2025. Mrs. J Snehaja, IFS, Head of MEA branch secretariat & Regional Passport Officer, Hyderabad was the guest of honour

Internship Programmes

The following students from NFSU, Dharwad and KLU, Guntur are undergoing unpaid internship programme at CDTI, Hyderabad for a period of One month:

S. No.	Name of Student	Education	University Name
1	Ms. Kelavath Saritha	B.Sc M.Sc Forensic Science	NFSU, Dharwad
2	Ms. Aditi Swarnkar	B.Sc M.Sc Forensic Science	NFSU, Dharwad
3	Mr. Poluru Jiji Dhanve	B. Tech M.Tech Computer Science and Engineering (Cyber Security)	NFSU, Dharwad
4	Mr. Vishal Prashant S	B. Tech M.Tech Computer Science and Engineering (Cyber Security)	NFSU, Dharwad
5	Mr. K Methushueal Chandra	MBA	KLU, Guntur
6	Ms. I Chitti	B.Sc M.Sc Forensic Science	NFSU, Dharwad

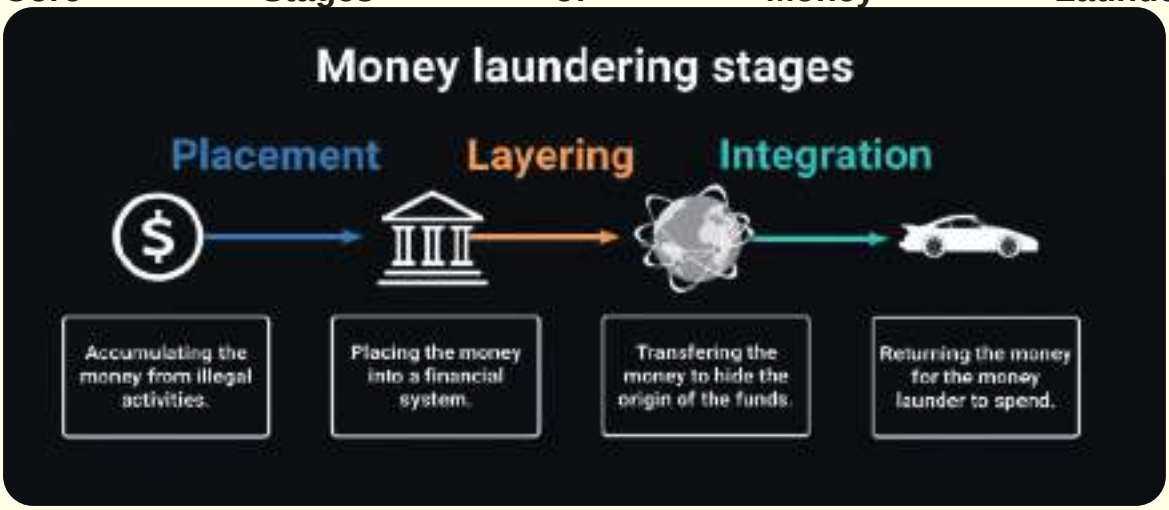
Money Laundering as a Service

The Emerging Criminal infrastructure

Ms. Divya
Cyber Expert, I4C

IntroductionMoney laundering has dramatically evolved from a traditional criminal activity into a sophisticated, industrialized service threatening global financial systems. Money laundering represents a systematic process of disguising illegally obtained funds as legitimate financial assets. Criminals develop intricate strategies to transform “dirty money” into seemingly clean financial resources, exploiting vulnerabilities within global financial infrastructures. The process involves strategic manipulation of financial systems to obscure the original source of criminal proceeds.

Core Stages of Money Laundering:



1. **Placement:** Criminals introduce illegal funds into legitimate financial systems through complex initial transactions.
2. **Layering:** Sophisticated techniques are employed to conceal money’s origin by creating multiple complex financial movements.
3. **Integration:** Laundered funds are strategically reintegrated into legitimate economic channels, appearing as normal financial transactions.

The Emergence of Money Laundering as a Service (MLaaS): Modern criminal networks have transformed money laundering into a professional, systematized service model. This industrialized approach allows various criminal actors to leverage advanced financial manipulation techniques, creating a structured infrastructure that operates with unprecedented efficiency and global reach.

Key Characteristics of MLaaS: MLaaS represents a paradigm shift in financial criminal

activities, characterized by:

- Professional, business-like operational structures
- Advanced technological exploitation
- Seamless global collaboration
- Specialized service providers offering targeted laundering capabilities

Technological Enablers of Modern Money Laundering: Digital technologies have revolutionized money laundering methods, providing criminals with sophisticated tools to transfer and conceal funds. Cryptocurrencies, online banking platforms, and advanced digital networks have created unprecedented opportunities for financial crime, enabling rapid, complex transactions that challenge traditional detection mechanisms.

Cryptocurrency and Digital Platforms: Emerging digital technologies offer criminals multiple advantages:

- Rapid cross-border transactions
- Enhanced money trail obfuscation
- Complex layering mechanisms
- Reduced traditional banking scrutiny

Geographical Hotspots of MLaaS: Certain geographical regions have emerged as critical hubs for industrialized money laundering activities. Southeast Asian countries like Cambodia, Myanmar, and Laos have developed complex ecosystems that facilitate large-scale financial crimes, often involving state-level complicity and systemic institutional vulnerabilities.

Criminal Network Structures: Modern money laundering operations mirror legitimate business organizational structures, featuring sophisticated hierarchies and specialized roles. These networks include strategic planners, field operators, technical experts, legal advisors, and financial intermediaries working in coordinated, complex systems.

Exploitation Mechanisms: Criminal networks strategically exploit:

- Shell companies
- Legitimate business structures
- Cryptocurrency exchanges
- Online platforms

Global Impact and Risks: The industrialization of money laundering presents multifaceted threats to global economic and social systems. These risks extend beyond immediate financial losses, potentially destabilizing institutional integrity, undermining regulatory frameworks, and facilitating broader criminal activities.

Prevention and Mitigation Strategies: Combating advanced money laundering requires comprehensive, multi-dimensional approaches involving technological innovation, regulatory frameworks, and international cooperation. Money laundering prevention demands a sophisticated, multi-dimensional approach that integrates technological innovation, regulatory compliance, and organizational resilience. Financial institutions and regulatory bodies must develop comprehensive strategies that address the complex, evolving landscape of financial crimes.

Know Your Customer (KYC) Processes: By implementing rigorous documentation

checks, conducting thorough background screenings, and continuously monitoring transactional activities, organizations can create a first line of defense against potential financial crimes. KYC processes enable institutions to develop detailed risk profiles, identify suspicious patterns, and proactively mitigate potential money laundering threats.

Comprehensive Anti – Money Laundering (AML) Compliance Policies: Effective AML policies should provide clear guidelines for detecting, reporting, and preventing suspicious activities, ensuring that every organizational level understands its role in maintaining financial integrity. By establishing transparent protocols and creating a compliance-oriented organizational culture, institutions can significantly reduce their vulnerability to money laundering risks.

Advanced Technology and Data Analytics: Modern financial institutions leverage sophisticated AI-driven analytics, machine learning algorithms, and real-time monitoring systems to identify complex transactional patterns that might indicate potential financial crimes. These advanced technologies can analyze millions of transactions instantaneously, detecting subtle anomalies that human analysts might overlook. By implementing cutting-edge data analytics, organizations can develop predictive models that not only detect existing suspicious activities but also anticipate potential future money laundering attempts.

Collaboration and Communication: Successful prevention requires robust collaboration between financial institutions, law enforcement agencies, regulatory bodies, and international organizations. By establishing strong communication channels, sharing intelligence about emerging threats, and participating in cross-sector information exchanges, stakeholders can develop a more comprehensive and adaptive approach to detecting and preventing financial crimes.

Legal and Regulatory Compliance: Adherence to established legal frameworks remains a cornerstone of money laundering prevention. Institutions must rigorously comply with international standards such as the Bank Secrecy Act (BSA) and local Prevention of Money Laundering Acts. This involves maintaining detailed transaction records, implementing mandatory suspicious activity reporting, and staying updated with the latest regulatory requirements. Legal compliance is not just about avoiding penalties but about maintaining the integrity of the global financial system.

Emerging prevention technologies include:dvanced transaction monitoring systems

- AI-driven fraud detection algorithms
- Blockchain tracing technologies
- Cross-platform information sharing mechanisms

Conclusion:

Preventing money laundering requires a holistic, adaptive strategy that combines technological innovation, human expertise, regulatory compliance, and collaborative intelligence. As financial criminals become increasingly sophisticated, prevention mechanisms must continuously evolve, integrating advanced technologies, comprehensive policies, and a proactive, risk-aware organizational culture.

Developing AI Models for Efficient Key Management in Cryptographic Protocols

Shri. Amit Dubey, *Makers Lab,*
Tech Mahindra, Noida

Introduction

In the digital era, data security is paramount, and cryptographic protocols play a pivotal role in ensuring secure communication, authentication, and data integrity. At the heart of these protocols lies the concept of key management, encompassing the creation, distribution, storage, rotation, and revocation of cryptographic keys. Efficient key management is critical to maintaining the confidentiality, integrity, and availability of sensitive data. The emergence of Artificial Intelligence (AI) offers innovative approaches to overcoming the challenges associated with traditional key management systems. This article explores the potential of AI models in enhancing the efficiency, scalability, and robustness of key management in cryptographic protocols.

Challenges in Traditional Key Management

Key management systems (KMS) are integral to cryptographic protocols, but they face several challenges, including:

1. **Scalability:** Traditional systems struggle to handle the exponential growth in the number of devices and keys in modern distributed environments, such as IoT networks.
2. **Security Risks:** Static key storage mechanisms are prone to vulnerabilities like insider threats, unauthorized access, and advanced persistent threats (APTs).
3. **Human Error:** Manual processes in key distribution and rotation are error-prone and can lead to security breaches.
4. Performance Overhead: Frequent key rotation and complex cryptographic computations can impact system performance.
5. **Dynamic Environments:** Traditional systems often lack adaptability in highly dynamic environments where nodes join and leave frequently.

AI-driven solutions have the potential to address these challenges by leveraging advanced machine learning (ML) algorithms, predictive analytics, and automation capabilities.

AI in Key Management: An Overview

AI can enhance key management in cryptographic protocols through its ability to analyze patterns, predict potential vulnerabilities, and automate processes. Key areas where AI can contribute include:

1. **Key Generation:** AI models can improve the randomness and security of key generation mechanisms by leveraging generative adversarial networks (GANs) or other stochastic models.
2. **Key Distribution:** AI-powered systems can optimize key distribution by predicting

network conditions, user behavior, and potential risks.

3. **Key Rotation and Revocation:** AI can automate key rotation schedules based on usage patterns and threat intelligence, ensuring timely updates without disrupting operations.
4. **Anomaly Detection:** Machine learning algorithms can monitor key usage and detect anomalies indicative of misuse or compromise.
5. **Policy Management:** AI can dynamically enforce and adapt key management policies based on contextual data and security requirements.

Key Techniques and Approaches

1. Reinforcement Learning for Key Distribution

Reinforcement learning (RL), a type of ML, enables systems to learn optimal strategies through trial and error. RL can be employed to develop adaptive key distribution algorithms that minimize latency and enhance security. For instance, RL agents can learn to predict the best routes and methods for distributing keys in a distributed network while avoiding compromised nodes.

2. Federated Learning for Secure Key Management

Federated learning (FL) allows multiple entities to train a shared ML model without sharing their local data, enhancing privacy and security. In the context of key management, FL can enable distributed systems to collaboratively develop AI models that predict optimal key management strategies without exposing sensitive information.

3. Generative Adversarial Networks (GANs) for Key Generation

GANs can be used to generate cryptographic keys with high entropy and randomness, ensuring robustness against brute-force attacks. By training a generative model to create keys indistinguishable from truly random sequences, GANs can address the shortcomings of traditional pseudo-random number generators (PRNGs).

4. Natural Language Processing (NLP) for Policy Enforcement

AI models leveraging NLP can interpret and enforce cryptographic policies by analyzing logs, configuration files, and other documentation. This approach ensures that key management practices align with organizational policies and regulatory requirements.

5. Anomaly Detection Using Machine Learning

Supervised and unsupervised learning algorithms can identify deviations in key usage patterns, signaling potential security incidents. For example, clustering techniques can group normal behaviors, and any outliers can be flagged as suspicious activities requiring further investigation.

Applications of AI-Enhanced Key Management

1. **Internet of Things (IoT):** IoT ecosystems require efficient and scalable key management due to their large-scale, distributed nature. AI can enable lightweight and adaptive KMS solutions that dynamically manage keys based on device context and network conditions.
2. **Cloud Security:** In cloud environments, AI models can optimize the encryption key lifecycle, ensuring secure storage, access control, and automated key rotation. AI can also monitor cloud access patterns to detect unauthorized usage.
3. **Blockchain Technology:** AI can enhance blockchain's cryptographic integrity by managing private keys for wallet security, automating multisignature schemes, and ensuring consensus algorithms' robustness against adversarial attacks.
4. **Financial Systems:** Financial institutions can use AI-driven KMS to secure transactions, manage customer credentials, and ensure regulatory compliance. Anomaly detection algorithms can prevent fraud and identity theft by monitoring cryptographic key usage.

5. **Quantum Cryptography:** As quantum computing poses threats to traditional cryptographic protocols, AI can play a crucial role in developing post-quantum cryptographic solutions. AI models can optimize key distribution mechanisms in quantum key distribution (QKD) systems.

Benefits of AI-Driven Key Management

1. **Enhanced Security:** AI's ability to detect anomalies and predict threats improves the overall security of cryptographic protocols.
2. **Scalability:** AI algorithms can efficiently handle the complexities of large-scale distributed systems.
3. **Automation:** Automating routine key management tasks reduces human intervention and associated errors.
4. **Adaptability:** AI models can adapt to dynamic environments and evolving threats, ensuring continuous security.
5. **Cost Efficiency:** By reducing manual intervention and optimizing resources, AI-driven systems lower operational costs.

Challenges and Considerations

While AI offers significant advantages, its integration into key management systems also poses challenges:

1. **Complexity:** Developing and deploying AI models for key management requires significant expertise and resources.
2. **Data Privacy:** Training AI models necessitates access to large datasets, raising privacy concerns.
3. **Adversarial Attacks:** AI models themselves can be targets of adversarial attacks, undermining their reliability.
4. **Regulatory Compliance:** Ensuring AI-driven systems adhere to legal and regulatory frameworks is critical.
5. **Explainability:** The black-box nature of some AI models can make it challenging to explain and justify decisions in sensitive security contexts.

Future Directions

1. **Integration with Quantum Computing:** As quantum computing evolves, AI-driven key management systems must integrate with quantum-resistant algorithms and protocols.
2. **Standardization:** Developing industry standards for AI-enhanced key management will ensure interoperability and consistency.
3. **AI Security:** Research on securing AI models against adversarial threats is essential to maintaining trust in these systems.
4. **Ethical AI Practices:** Ensuring transparency, fairness, and accountability in AI-driven KMS will foster widespread adoption.
5. **Real-Time Systems:** Enhancing the real-time capabilities of AI models for key management will be crucial for applications requiring instant responses.

Conclusion

AI holds immense potential to revolutionize key management in cryptographic protocols, addressing the limitations of traditional systems and enhancing security, scalability, and efficiency. By leveraging techniques such as reinforcement learning, GANs, and federated learning, organizations can develop adaptive and robust KMS solutions tailored to modern cybersecurity challenges. While challenges remain, ongoing research and innovation promise to unlock the full potential of AI in securing digital ecosystems for the future.

Unmasking Cyber Terrorism: Challenges in Investigation and the Legal Battlefield

Dr. T V Rajesh,
DSP, NIA

While all the Police officers are quite familiar with the term 'terrorism' or 'terrorist acts' as well as the definitions thereof in accordance with the relevant laws of the land, the term 'Cyber terrorism' is comparatively a new one. As the technology advances, the unscrupulous elements in all fields of life, including criminals, have been taking undue advantage thereof, and in the digital era, Cyber terrorism has emerged as a significant threat for the nations as well as the societies. When the Police Officers are entrusted with the task of investigating the acts of Cyber terrorism and presenting it before the courts of law, they face multifaceted challenges ranging from technological barriers to legal hurdles.

Acknowledging the acts of Cyber terrorism across the globe and identifying the requirement of ensuring adequate deterrents, it was decided during the year 2008 to incorporate Section 66F in the Information Technology Act, 2000, which defines and provides for punishment for the acts of Cyber terrorism.

This definition was incorporated in the said Act along with other provisions related to different kinds of cybercrimes, during the amendment in 2008. Broadly, the definition of Cyber terrorism covers the acts terrorism using cyber space, such as hacking critical infrastructure and attacks on information systems, networks and data, spreading propaganda, coordinating real world attacks etc. basically, the cyber terrorists thrive on the borderless nature of cyberspace as well as the valour derived out of their anonymity. Cyberattacks on Estonian parliament, banks, ministries, newspapers and broadcasters etc. that happened in 2007, is an example of cyber terrorism. Such a cyber onslaught on Estonia was reckoned by the experts in the field as a sophisticated attack. One individual of Russian origin was punished by Estonia for the offence[1] . Further, during the year 2010, many Iranian facilities including Natanz nuclear facility, were attacked by the 'Stuxnet worm', which was identified to be a 500-kilobyte computer worm[2] . Coming to India, sensitive personal data of 81.5 crore Indians was leaked during the attack on the systems of the Indian Council of Medical Research (ICMR)[3] that happened in 2023. Prior to that the servers of the AIIMS in Delhi were hacked in 2022 in a ransomware attack, compromising the data pertaining to about 3-4 crore patients. It was reported that the hackers had demanded about Rs 200 crore in the form of cryptocurrency[4] . Though the investigations could identify the perpetrators, no legal action could be initiated due to jurisdictional issues.

Technological Sophistication

Perpetrators of cyber terrorism often take the assistance of malware, encryption

[1] news.bbc.co.uk/2/hi/technology/7208511.stm
[2] large.stanford.edu/courses/2015/ph241/holloway1/
[3] https://www.indiatoday.in/technology/news/story/personal-data-of-815-crore-indian-users-leaked-in-possibly-the-largest-data-breach-in-indian-history-2455818-2023-10-30
[4] Cyber warfare by Chinese hackers: The AIIMS story, International Journal of All Research Education and Scientific Methods (IJARESM), ISSN: 2455-6211 Volume 11, Issue 3, March-2023, Impact Factor: 7.429, Available online at: www.ijaresm.com

and anonymization tools like the TOR network. Such unscrupulous elements resort to dark web and Virtual Private Networks (VPNs) to remain anonymous. This kind of technological sophistication poses a great challenge to the Investigating Officers to identify the specific individuals or groups behind any cyber-attack. The fact that the law enforcement agencies lag behind the cyber-criminals in updating their technology, due to various reasons such as acute shortage of skilled manpower, limited training facilities, red-tapism to procure the forensic tools with latest technology, work pressure, lack of motivation at the field level etc., works to the advantage of the cyber-criminals. The cyber criminals are adept in acquiring and utilizing the latest technology available. Further, during the investigation of cyber-terrorism cases, the officers often come across evidence in the form of encrypted devices or files, which cannot be deciphered without the assistance of modern forensic tools or cooperation from the private players in the field, both of which becomes difficult to obtain during the crucial moments of recovery.

Chain of custody during Investigation

Ensuring the integrity of chain of custody of all the seized material is critically important in any investigation, in order to prove the case beyond reasonable doubt, as otherwise the criminals can go scot-free, taking advantage of benefit of doubt. It has to be established that the evidence in the case was not altered during collection, transportation, storage or even during analysis. However, the given the transient nature of the digital evidence, ensuring loss of evidence or securing it effectively during the course investigation could be at times difficult. For example, the server logs that the Investigator may come across during the cyber-investigation, could be erased, after a particular time. Further, the data stored in Random Access Memory (RAM) could be lost when the digital device is switched off for the purpose of seizing. If the evidence is found to be stored in cloud system, the investigator would be at the mercy of the technical person of the cloud-owner-company, to retrieve the evidence.

Challenges in Court

The complexity of cyber terrorism cases and the evidences related to such cases demand detailed and high level of technical explanations by the experts in the field. If the prosecutors as well as the judges are not able to grasp the nuances of the digital evidences submitted along with the chargesheet, it could give rise to misunderstandings and the situation may lead to the defence taking advantage of the same. In the cases of cyber-terrorism cases, the circumstantial evidence such as IP addresses or metadata are very crucial to establish the case. However, it would be easy for the defence lawyers to dispute the findings of investigation, claiming that the devices of the accused were hacked by someone else. This could raise a doubt in the minds of the court, the benefit of which can go to the accused. Further, methods adopted by the Investigators, such as statement of the accused, or the forensic tools, could be challenged by the defence, on the ground of constitutional provisions against self-incrimination, or rights to privacy, in spite of the fact that *"when any fact is deposed to as discovered in consequence of information received from a person accused of any offence, in the custody of a police officer, so much of such information, whether it amounts to a confession or not, as relates distinctly to the fact discovered, may be proved"* as provided under proviso to section 23 (2) of Bharatiya Sakshya Adhiniyam (BSA).

Legal Framework and International Scenaro

Cyber-terrorists cannot be stopped by boundaries or national borders. It is easy for tech-savvy cyber-terrorists to be in one country and use the servers situated in another country to unleash attacks on critical systems of a third country. The infamous WannaCry Ransomware Attack in May, 2017, which targeted computers across the globe, running the Microsoft Windows operating system by encrypting data and demanding ransom payments is a classic example for this. In this case, the ransomware exploited vulnerabilities in Microsoft Windows systems using tools allegedly stolen from the U.S. National Security

Agency (NSA), and affected more than 3,00,000 computers in 150 countries[5] . It was later found that the hackers based in North Korea[6] had used the servers located in different countries, to propagate the malware, thus making it difficult to identify the attacker's actual location. This ransomware cyber attack paralysed critical infrastructure worldwide, including hospital, airline etc., causing approximately $4 billion in damages[7] . This attack highlights how cyber-terrorists can circumvent jurisdictional constraints, and the need to have international collaboration in the fight against cyber-terrorism.

The deficiency of harmonized legal standards gives scope for significant barriers to international collaboration in this aspect. The different standards of treating a cyber activity as criminal or otherwise creates a lot of disparities, which will come in the way of evidence sharing and extradition requests. The Convention on Cybercrime of the Council of Europe of November, 2001, or better known as the Budapest Convention, is the first international instrument which has provided guidelines for investigating and prosecuting cybercrimes, including cyber terrorism. However, since many of the countries are not signatories to such instruments, a permanent solution for the issue is yet to be identified. The following few successful cases demonstrate the role of international cooperation in unmasking cyberterrorism.

(i) Arrest of Al-Qaeda's Cyberterrorist, Younis Tsouli (2005)[8]

Younes Tsouli, Moroccan-born British used several pseudonyms based on variations of Irhabi 007 and used online platforms to spread Al-Qaeda propaganda, to provide bomb-making instructions and to recruit members. Irhabi in Arabic means terrorist. His activities were mainly funded by Al-Daour, using fraudulent transactions of about 37000 credit cards. The collaborative investigation conducted by the agencies of UK, USA and Middle Eastern countries identified his IP addresses, tracked his online activities and Tsouli was arrested in London during October 2005. He was charged, prosecuted and later convicted under the UK's Terrorism Act, 2000, for inciting terrorism through internet.

(ii) Operation Ghost Click (2011)[9]

The scam, Operation Ghost Click, which began in 2007, infected a lot of computers in different countries. The modus operandi was to infect the computers with a malware called "DNSChanger", which could alter the DNS settings on a computer. Computers with Windows OS as well as iOS OS were affected. Thereafter, the requests made by the users to visit certain websites used to be redirected to other sites, belonging to the partners of the cyber-terrorists. It is assessed that the cyber-terrorists earned about $14 million. The collaborative investigation conducted by the FBI of US and the Estonian Police using the sophisticated cyber forensic tools resulted in the disabling of affected networks of computers six Estonians and one Russian were arrested. They were charged under various sections of law, attracting upto 30 years of imprisonment.

(iii) Arrest of the Carbanak Cybercriminal Group (2018)[10]

In the instant case, the criminals introduced malware into MS Windows based systems using phishing mails and using these malwares, stole a total of approximately $900 million from different banks as well as from private customers, by manipulating the access to the respective banking networks. The group targeted Russia, United States, Germany, China and Ukraine. The activities of the Carbanak group were discovered during 2014 by the cyber security company Kaspersky Lab. The complex investigation conducted by Spanish National Police, with the close assistance of Europol, FBI, the Romanian, Moldovan, Belarussian and Taiwanese authorities and private cyber security companies resulted in the arrest of the leader of the gang in Alicante, Spain in the year 2018, thereby disrupting a significant cybercriminal network.

[5] https://www.npr.org/sections/thetwo-way/2017/05/15/528451534/wannacry-ransomware-what-we-know-monday
[6] https://www.csoonline.com/article/563017/wannacry-explained-a-perfect-ransomware-storm.html
[7] https://www.kaspersky.com/resource-center/threats/ransomware-wannacry
[8] news.bbc.co.uk/2/hi/americas/7191248.stm
[9] https://www.theguardian.com/technology/2011/nov/10/ghost-click-botnet-infected-computers-millions
[10] https://www.europol.europa.eu/media-press/newsroom/news/mastermind-behind-eur-1-billion-cyber-bank-robbery-arrested-in-spain

(iv) Mumbai attack of 26/11/2008

The attack on Mumbai during 2008 had sent tremors of fear across the country. The investigation conducted subsequent to the incident revealed that the terrorists had used advanced technology, for planning and execution of the attack. The map, topography, population etc. were studied using "Google earth", and social media was used to track the movement of security forces. The investigation of the case was successful due to the cooperation in investigation extended by countries like US, UK, etc. however, lack of cooperation from Pakistan has come in the way of successful prosecution of all the accused.

While the above cases were successfully solved due to the international cooperation on the subject, there are unresolved important cases such as (i) Sony Pictures Entertainment Hack case of 2014, wherein sensitive data, including employee emails, unreleased films, and private information were exposed, (ii) the attacks on Ukrainian Power Grid which caused a blackout affecting 230,000 people in Ukraine in 2015 and the similar, but more sophisticated attack in 2016 targeting a transmission-level substation in Ukraine and (iii) Shadow Brokers and the NSA Cyber Tools Leak case in 2016, wherein cyber tools and exploits were stolen from the National Security Agency (NSA) of US. These unresolved cases underscore the importance of international cooperation and to have a common legal framework to counter cyber terrorism.

Conclusion

In the modern digital world, the cyber terror activities pose considerable challenges to the criminal justice system, including law enforcement agencies and the judiciary. If the challenges of collecting convincing evidences are overcome, the investigating officers face the risk of inadmissibility of some of the evidences in the court and being challenged by the defence lawyers, with a view to taking advantage of the benefit of doubt. In order to adequately address these issues, a multifaceted approach should be adopted, incorporating the capacity building measures, reforming the legal system and improving international cooperation.

Providing adequate training to the field level investigating officers with cutting edge technology with a view to enhancing their skills and equipping them with the latest cyber forensic tools with expert assistance is one important measure governments have to think of, while preparing to combat cyber-terrorism. Inviting other countries and providing training to them along with sharing of case studies could be beneficial for the officers of both the countries, due to the enhanced exposure such training provides. With the increasing research and development in the field of cyber security in the private sector, it would be a good idea for the governments to explore public-private-partnership in the area. Law Enforcing Agencies should be able to make use of artificial intelligence and machine learning techniques to identify the patterns, so as to enhance the detection of cyber-terrorism attacks and analysis thereof. Further, in view of the growing threats of cyber-terrorism and the ephemeral nature of the digital evidence, the governments should also think of reforming the related laws incorporating modified provisions on evidence-admissibility, and accordingly updating the procedures related to legal process and trial, in order to ensure justice to victims.

At the international level, all the countries should establish Mutual Legal Assistance Treaties (MLATs) and other mechanism, to ensure maximum cooperation with respect to investigation of cross-border cyber-terrorism cases. The maintenance of data related to cyber-crimes at country level, sharing the same with other countries whenever required, and maintenance of international database of cyber-terror cases as well as individuals involved in the cases could go a long way in streamlining the investigation of cyber-terrorism cases. Further, streamlining the definitions of offences and arriving at a consensus on deciding the maximum punishment could make the legal cooperation smoother among the countries.

Comparative study on IEA 1872 (Act No.1 of 1872) & BNS 2023 (Act No. 47 of 2023)

Shri. Rajkumar Bandopadhyay,
Chief Law Instructor,
Kolkata Police Training Academy

A comparative study on the Indian Evidence Act, 1872 (Act No. 1of 1872) & The Bharatiya Sakshya Adhiniyam, 2023 (Act 47 of 2023) regarding the credit of an accomplice as a witness:-

If we notice section 114 – Illustration (b) of the Indian Evidence Act – An accomplice is unworthy of credit, unless he is **corroborated** in material particulars.

On the other hand as per section 133 of the Indian Evidence Act – An accomplice shall be a competent witness against an accused person and a conviction is not illegal merely because it proceeds upon the **uncorroborated** testimony of an accomplice.

The essence of section 114 – Illustration (b) and that of section 133 Indian Evidence Act is totally different.

In one case – an accomplice is unworthy of credit, unless he is **corroborated** in material particulars and in the other case a conviction is not illegal merely because it proceeds upon the uncorroborated testimony of an accomplice.

In Bharatiya Sakshya Adhiniyam (BSA) 2023 (Act 47 of 2023),

Section 119 -Illustration (b) is same as section 114- Illustration (b) of the Indian Evidence Act, 1872 – an accomplice is unworthy of credit, unless he is **corroborated** in material particulars.

But significant change occurs in section 138 of the Bharatiya Sakshya Adhiniyam, 2023 (Act No. 47 of 2023) – An accomplice shall be a competent witness against an accused person and a conviction is not illegal if it proceeds upon the corroborated testimony of an accomplice.

Thus after one hundred and fifty two (152) years of inconsistency between section 114 – illustration (b) & 133 of Indian Evidence Act, 1872 (Act No. 1 of 1872) regarding the credit of an accomplice as a witness has finally come to an end.

More precisely we can say that the replacement of word 'Uncorroborated' by 'Corroborated' as noticed in section 138 of the BSA made the legislation more effective and meaningful.

Section 30 of the Indian Evidence Act 1872 (Act No. 1 of 1872) & section 24 of the Bharatiya Sakshya Adhiniyam 2023 (Act No. 47 of 2023) where it reveal that when persons are being tried jointly for the same offence and a confession made by one of them which affects that particular person and some other such persons and if it is proved in nature, the Court may taken into consideration that confession as against such other persons as well as against

the person who makes such confession e.g. if X and Y are jointly tried for the murder of Z and if it is proved that X said " Y and I murdered Z", the Court may consider the effect of this confession as against Y.

1. Legal Framework for Admissibility:-

Self-Incriminating Statements: A co-accused's confession implicating themselves and others may be admissible in court. However, it must comply with procedural safeguards, such as being made voluntarily and without coercion.

Statement Against Another: If a co-accused's statement incriminates another accused, it generally cannot be used as direct evidence against the other accused unless corroborated by independent evidence.

Section 24 of the Bharatiya Sakshya Adhiniyam 2023: A confession made by a co-accused can be considered by the court if both the maker of the confession and the implicated person are being tried jointly. However, it is treated as corroborative and not substantive evidence.

2. Evidentiary Value:-

Limited Weight: Courts often treat the statement of a co-accused with caution. Standing alone, it is insufficient to convict another accused without corroborating evidence.

The confession of a co-accused is not considered substantive evidence. Its role is limited to corroborating other independent evidence presented during the trial. Courts exercise caution when relying on such confessions, ensuring they are voluntary, reliable, and sufficiently corroborated by additional evidence.

Corroboration Requirement: The court looks for additional evidence to substantiate the allegations made in the co-accused's statement.

3. Use in Joint Trials:-

When multiple accused persons are tried together, the co-accused's statement can influence the case but only to the extent allowed by law. The statement may:

Reveal conspiracy or collective involvement in the offense.

Provide leads to evidence.

Shed light on the motive or planning of the crime.

4. Legal Challenges:-

Voluntariness: The statement must be made without threat or inducement.

Right to Silence: A co-accused's statement should not violate another accused's constitutional rights, such as the right to remain silent.

Cross-Examination: If the statement is used in court, the other accused should have the opportunity to cross-examine the co-accused (if the statement is made in testimony).

5. Judicial Precedents:-

Section 30 of the Indian Evidence Act, 1872 & Section 24 of the Bharatiya Sakshya Adhiniyam, address the admissibility of confessions made by one accused person that implicate co-accused individuals during a joint trial for the same offense. Specifically, it allows the court to consider such a confession against both the confessor and the co-accused. However, the evidentiary value of these confessions has been scrutinized in various judicial pronouncements.

CENTRAL DETECTIVE TRAINING INSTITUTE HYDERABAD

cdtshyderabad@nic.in
cdtihyd@gov.in
040-27038182, 29704150

@bprdcdtihyd
@bprdcdtihyd
@bprdcdtihyd

Address:
CDTI, Ramanthapur,
Hyderabad,Telangana,
Pin-500013

Editor in cheif : Shri Salmantaj Patil, IPS, Director
Editor : Shri V Bheemakrishna Naik, PA (TRG.)