

CYBER FRAUD SCENARIO



SAMPAT MEENA , IPS
Joint Director ,CBI



THE INDIAN LANDSCAPE

01

Population

- 1.39 billion in 2021
- 35% of population urban
- Median age 28



03

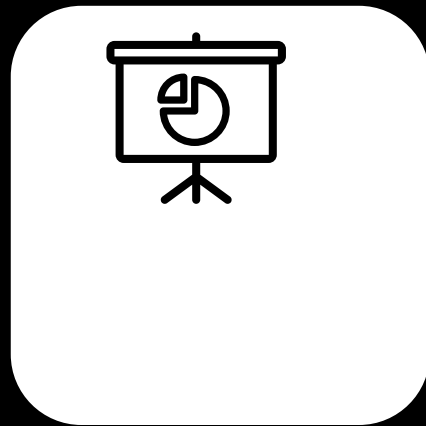
Mobile User

- 760 million smartphones users in 2021

02

Digital Population

- Digital adoption propelled by rural India, 45% growth in internet users
- No. of internet users grew by 8%



04

Social Media User

- Social Network users 448 Million. Expected to reach half a billion by 2023
- 87% defined as regular users, [accessed internet in last 30 days]





UNPRECEDENTED TRANSFORMATION OF INDIA

INTERNET REVOLUTION

The number of internet users in India is expected to increase to 900 million in 2025 from around 622 million in 2020

Each month, India adds approximately 10 million new active internet users - the highest rate in the world.

FINANCIAL INCLUSION

430 million+ new Bank Accounts opened in last 7 years under Centre's flagship financial inclusion scheme, Pradhan Mantri Jan Dhan Yojana (PMJDY)

1.2 BILLION + MOBILE USERS

There were nearly 1.20 billion mobile connections in India in January 2022

DIGITIZATION OF ESSENTIAL SERVICES

All essential public services and social infrastructure rely on digital platforms - Power grids, pipelines, Aarogya-Setu, AADHAR, welfare schemes, State Wide Area Networks etc

EXPLOSIVE GROWTH OF SOCIAL MEDIA

530 million+ WhatsApp users
410 million+ Facebook users
448 million+ YouTube users

E-COMMERCE & DIGITAL PAYMENTS

Highest Digital Payment Transactions in the world.

In the financial year 2021, around 44 billion digital payments were recorded across India.





CYBER THREAT OVERVIEW

Cyber Crime Incidents
in India in 2020

1.15 M

source: MHA

Reported financial loss due to
cybercrime reported in India
in 2019

Rs 1.25 Tr.

source: National Cyber Security Co-ordinator

↑ 12% from previous FY
Total cybercrime Cases
registered in India in 2020

50035

source: MHA

↑ Ransomware attacks in
India in 2021 over 2020

218%

Source: Palo Alto Networks

Loss due to Digital Banking
fraud in 2020-21

Rs 634 M

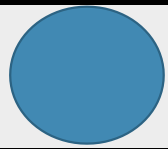
source: CERT-IN

Estimated average amount of
Ransomware payment made
by Indian Organization

\$1.2 M

Source: Palo Alto Networks





CYBER ATTACK TREND

*Big Game Hunting
or
Supply Chain Attack*

*Crypto mining
&
Ransomware*

Insider Threats

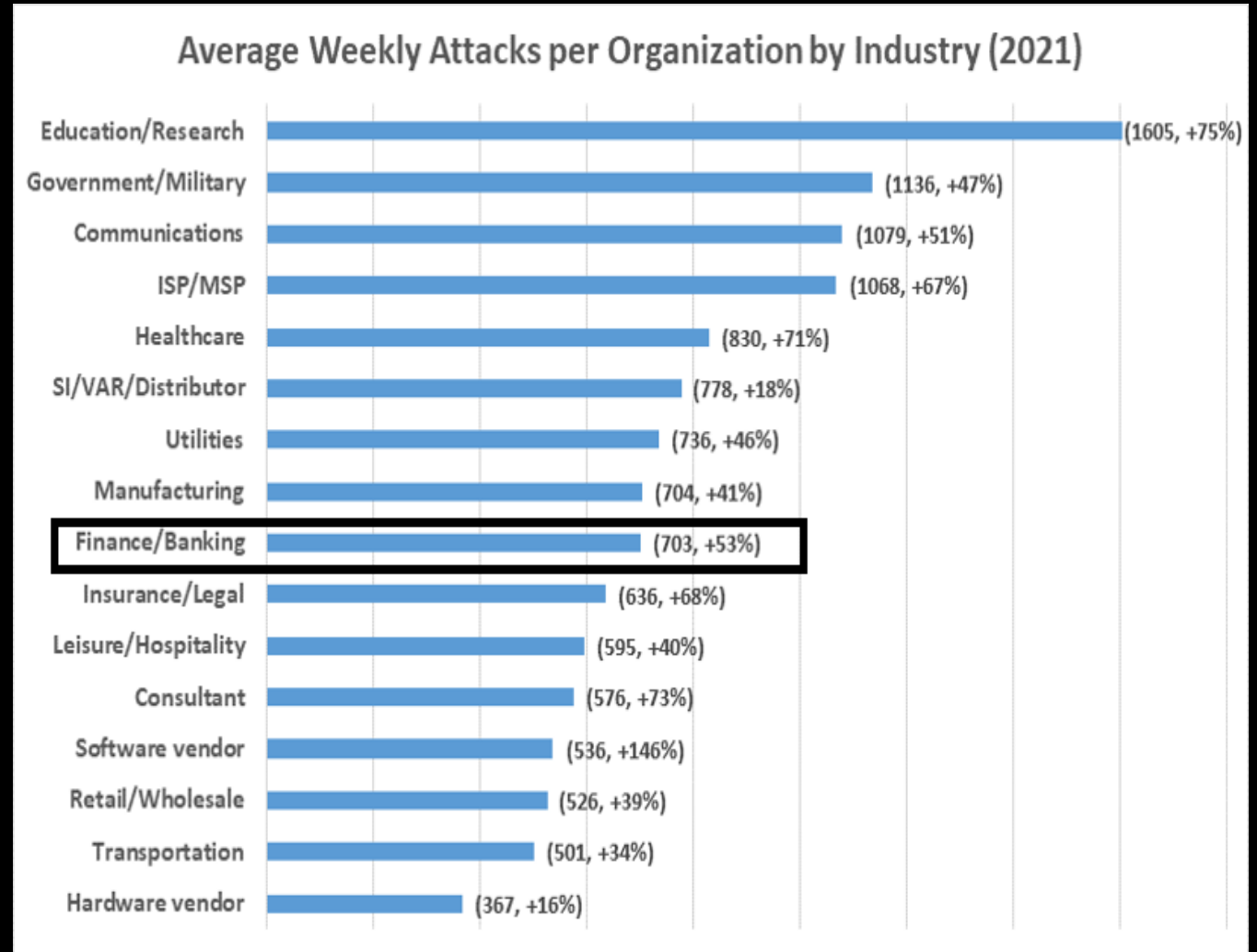
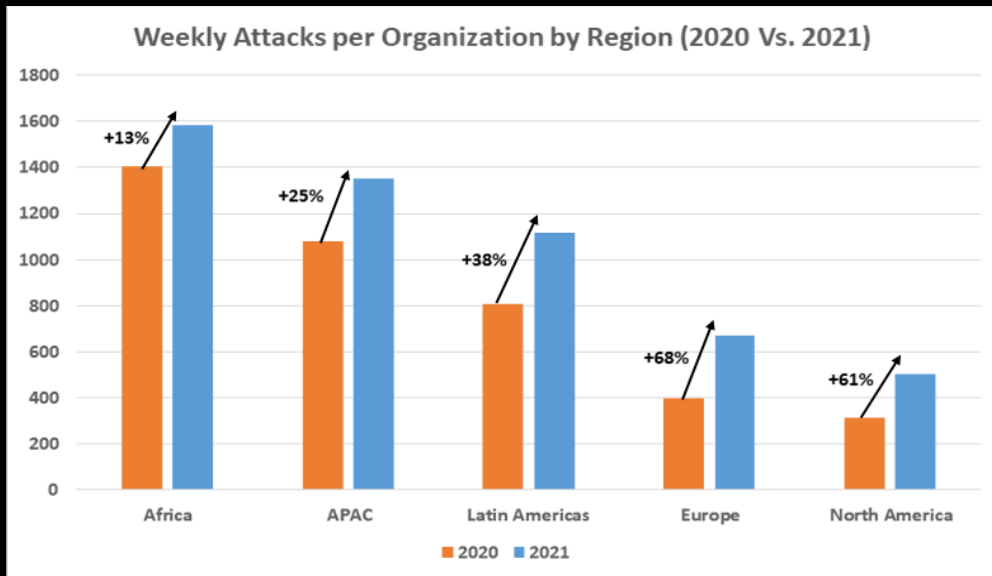
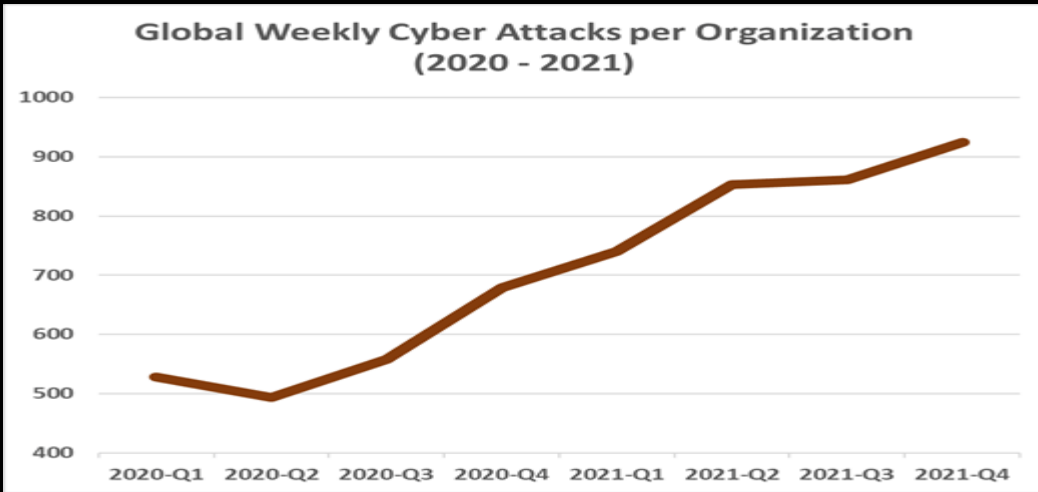


Cyber Warfare






UPWARD TREND OF CYBER ATTACKS DUE TO EVOLUTION OF DIGITAL ARENA






INDIA'S CRITICAL INFRASTRUCTURE UNDER ATTACK !!!

State-sponsored groups & cybercriminal gangs targeting critical civilian infrastructures, including:

 Software supply chains

 Hospitals

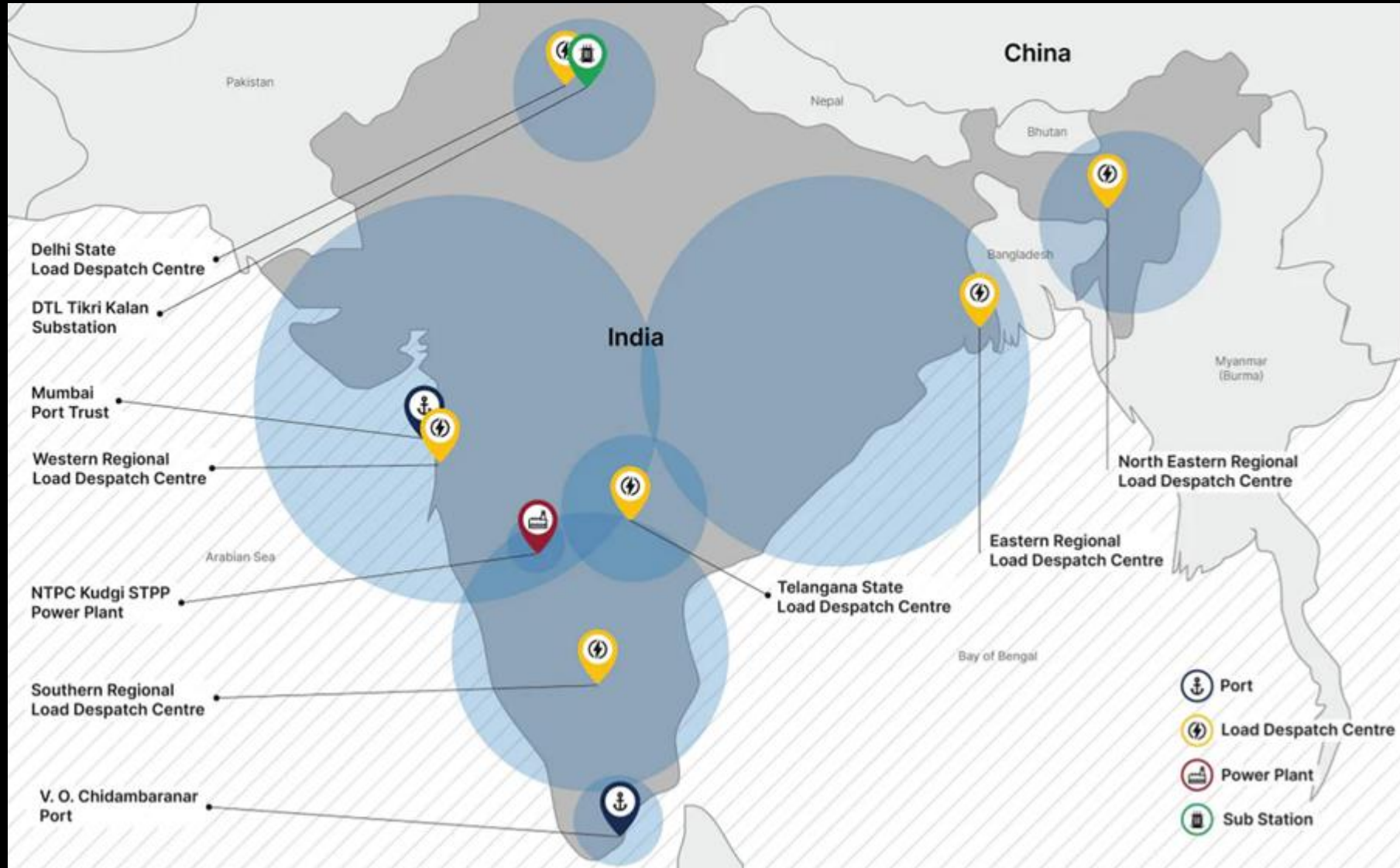
 Transportation networks

 Energy supplies





INDIA'S CRITICAL INFRASTRUCTURE UNDER ATTACK !!



Malware :

TRICKBOT

OCTOBER 2020
FINANCIAL FRAUD/
MALWARE+RANSOMWARE
DELIVERY BOTNET

Globally dispersed financial trojan and malware distribution botnet with a compromised IoT-based command and control infrastructure. Trickbot has also been used to deliver ransomware.

NECURS

MARCH 2020
MALWARE AND SPAM
SPREADING BOTNET

Globally dispersed spam and malware distribution botnet with a sophisticated and redundant command and control infrastructure. The Necurs botnet has been used to deliver ransomware, financial malware, spam, and stock scams.

THALLIUM

DECEMBER 2019
NATION-STATE

Nation-state actor. Targets government employees, think tanks, university staff, organizations focused on world peace and human rights, and individuals that work on nuclear proliferation issues. Most targets were based in the U.S., as well as Japan and South Korea.

PHOSPHORUS

MARCH 2019
NATION-STATE

Nation-state actor aka APT 35, Charming Kitten, and Ajax Security Team. Targets prominent individuals in business and government to steal credentials. Targets also include activists and journalists – especially those involved in advocacy and reporting on issues related to the Middle East.

GAMARUE

NOVEMBER 2017
MALWARE SPREADING
BOTNET

Sold as a Crime kit, first seen in 2012. Distributed at least 80 different malware families. Detected/blocked on an average of 1.1 million machines every month. Disruption started Dec 2015 involving Windows Defender team and DCU. Partnered with ESET and global LE agencies.

AVALANCHE

NOVEMBER 2017
CRIMINAL SYNDICATE

Int'l criminal syndicate involved in phishing attacks, online bank fraud, and ransomware. Also refers to the network of systems used to carry out the activity. Initial takedown global law enforcement occurred on 30 November 2016.

BARIUM

NOVEMBER 2017
NATION-STATE

Nation-state actor heavily targeting gaming and internet content industries. Highly targeted theft of sensitive information using a custom malware toolkit that has extensive capabilities (stealing credentials, exploitation and data exfiltration).

STRONTIUM

AUGUST 2016
NATION-STATE

Nation-state actor aka APT28 Fancy Bear. Highly targeted theft of sensitive information. Uses zero-day exploits and spear phishing attacks to gain network/account access.

DORKBOT

DECEMBER 2015
IDENTITY THEFT, FINANCIAL
FRAUD

Disables security, steals credentials, personal info., distributes other malware. Spreads via USB, messaging, and social networks. Partnership with Homeland Security and international agencies.

RAMNIT

FEBRUARY 2015
IDENTITY THEFT,
FINANCIAL FRAUD

Module-based malware which concentrates on stealing credential information from banking websites. International public-private partnership, shut down C&C servers, redirected 300 domains.

SIMDA

APRIL 2015
IDENTITY THEFT, FINANCIAL
FRAUD

Uses remote access to steal personal and banking info., as well as install other malware. Partnered with Interpol and industry partners and activated CME platform, to disrupt global malware attack.

CAPHAW

JULY 2014
IDENTITY THEFT,
FINANCIAL FRAUD

Focused on online financial fraud responsible for more than \$250M in losses. Coordinated disruption with public-private sector partnerships.

GAMEOVER ZEUS

JUNE 2014
IDENTITY THEFT,
FINANCIAL FRAUD

Extremely sophisticated trojan which steals banking credentials. Spread via spam or phishing messages. Worked in partnership with LE providing Technical Remediation.

BLADABINDI & JENXCUS AKA B106

JUNE 2014
IDENTITY THEFT, FINANCIAL
FRAUD,
PRIVACY INVASION

Discovered July 2012. Pervasive family of malware spread through infected removable drives and downloaded by other malware.

ZEROACCESS AKA SIREFEF

DECEMBER 2013
ADVERTISING CLICK-FRAUD

Hijacks search results, takes victim to dangerous sites. Cost online advertisers upwards of \$2.7 million each month. Successful disruption in partnership with Europol EC3, FBI, A10 Networks.

CITADEL

JUNE 2013
IDENTITY THEFT,
FINANCIAL FRAUD

Committed online financial fraud responsible for more than \$500M in losses. Coordinated disruption with public-private sector partnerships to combat cybercrime.

BAMITAL

FEBRUARY 2013
ADVERTISING CLICK-FRAUD

Hijacked user's search results, took victims to dangerous sites. Takedown in collaboration with Symantec. Proactive notification and cleanup process.

NITOL

SEPTEMBER 2012
MALWARE SPREADING
BOTNET, DISTRIBUTED DOS
ATTACKS

Introduced in the supply chain relied on by Chinese consumers. Settled with operator of malicious domain.

ZEUS AKA ZBOT

MARCH 2012
IDENTIFY THEFT, FINANCIAL
FRAUD

Steals identity, financial information, controls PC, turns off firewall, installs other malware, ransomware. Cross-sector partnership with financial services. Focused

KELIHOS

SEPTEMBER 2011
SPAM, BITCOIN MINING,
DISTRIBUTED DOS ATTACKS

Trojan that distributes spam, steals logins, bitcoins, downloads and executes files. Partnership between Microsoft and security software vendors. First operation with

RUSTOCK

MARCH 2011
SPAM

Rootkit-enabled back door Trojans which distributed spam e-mail. Support by stakeholders across industry sectors. Involved US & Dutch law enforcement, and CN-CERT.

CONFICKER

FEBRUARY 2010
BOTNET WORM


Worm spread via USB and internet. Would infect other devices in common network. Global cyber-security elites joined forces. Microsoft-led model of industry-wide efforts.

WALEDAC

FEBRUARY 2010
SPAM

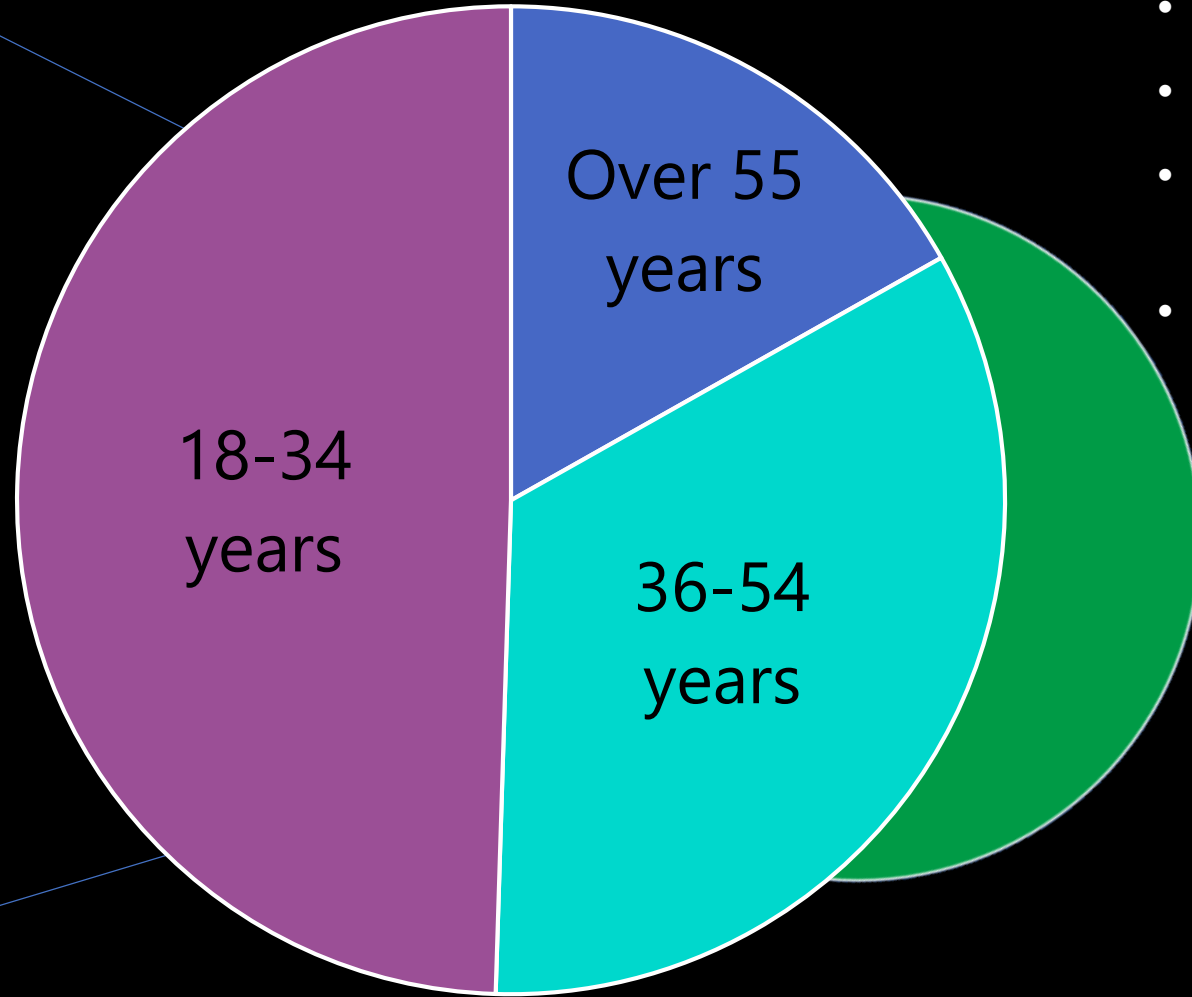
Trojan that collects email addresses, distributes spam, post data to webs, downloads executable files. Proving model of industry-led efforts. Severed 70-90,000 devices from the

Source:
Microsoft



Some unexpected data !!!

Breakdown by age
of victims



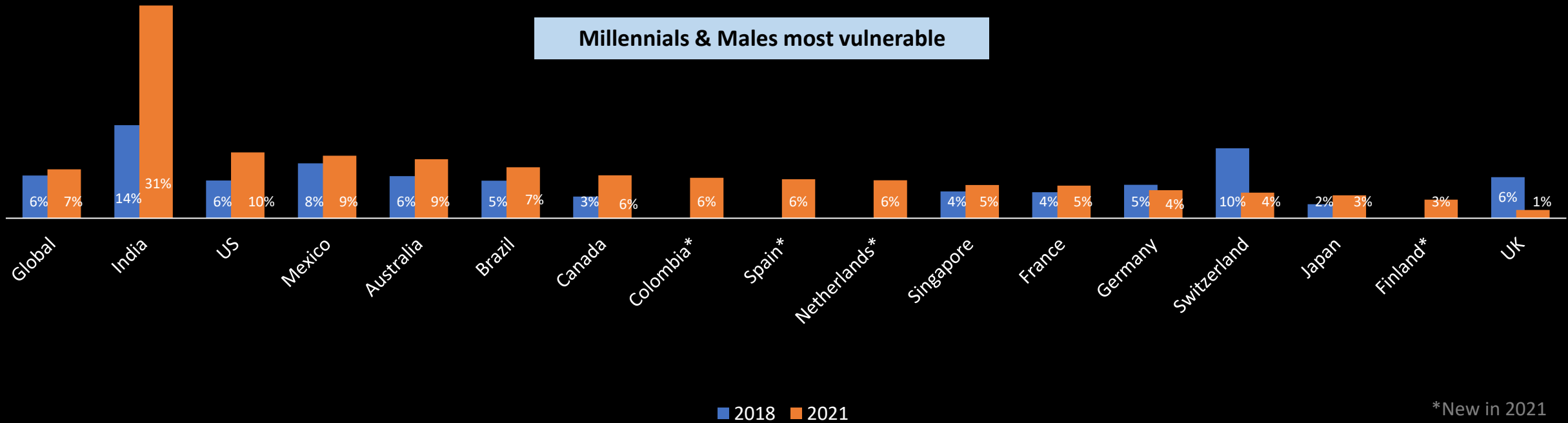
Of those, **14 people** continued with fraudulent interaction:

- Downloaded malware
- Visited a scam website
- Gave scammers remote access
- Provided payment



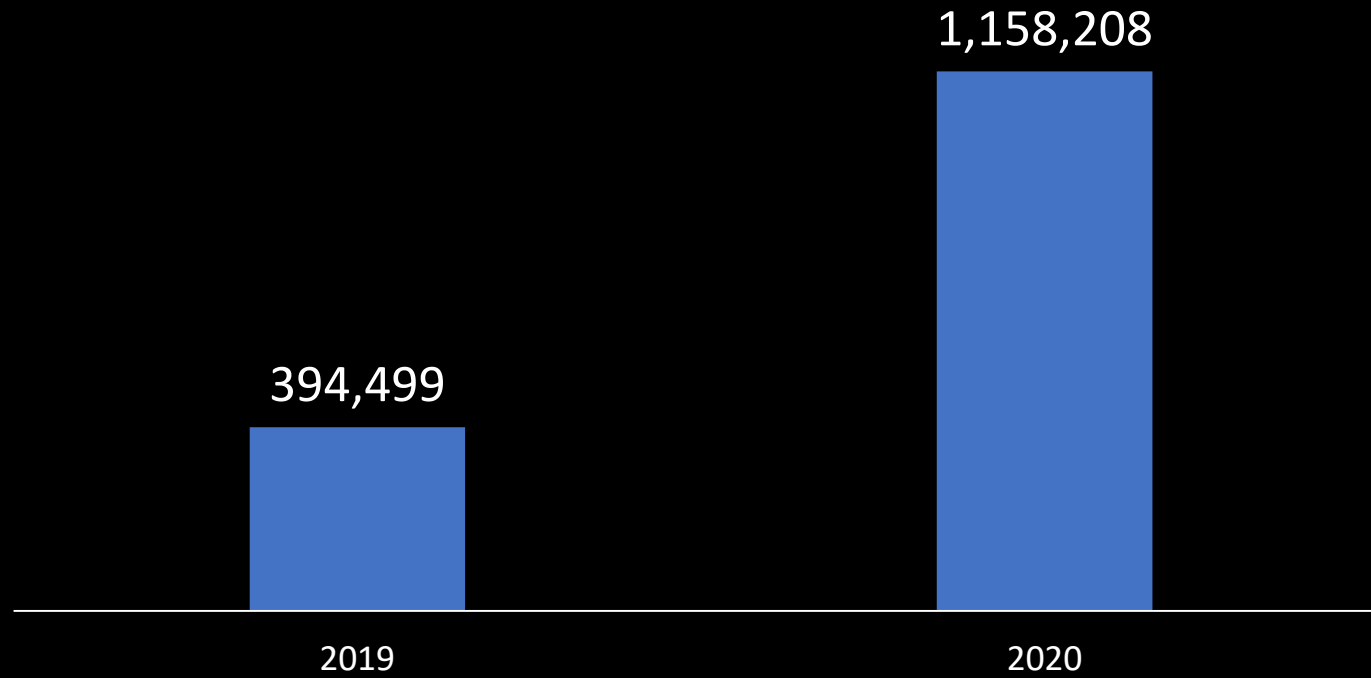
Number of People losing money in Tech Support Scam

India recorded the highest increase, with almost a third losing money through a tech support scam





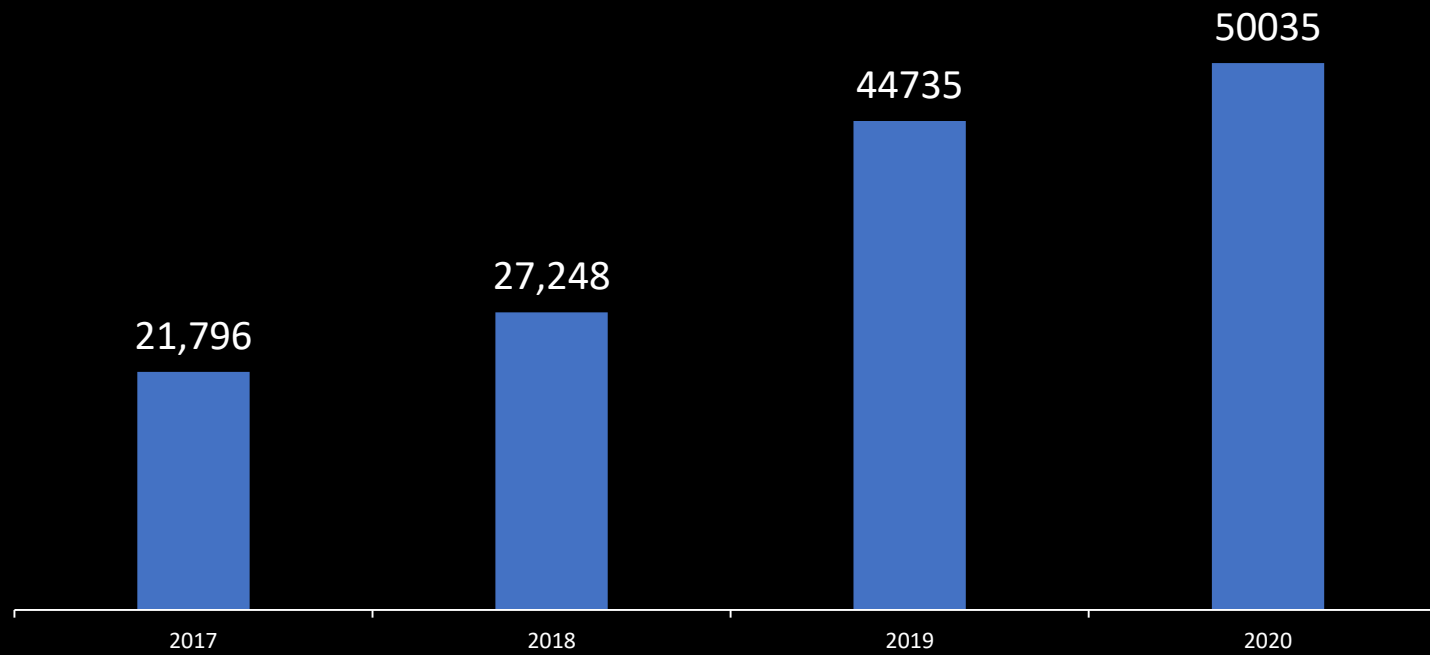
INCIDENTS REPORTED



Source: MHA



CASES REGISTERED

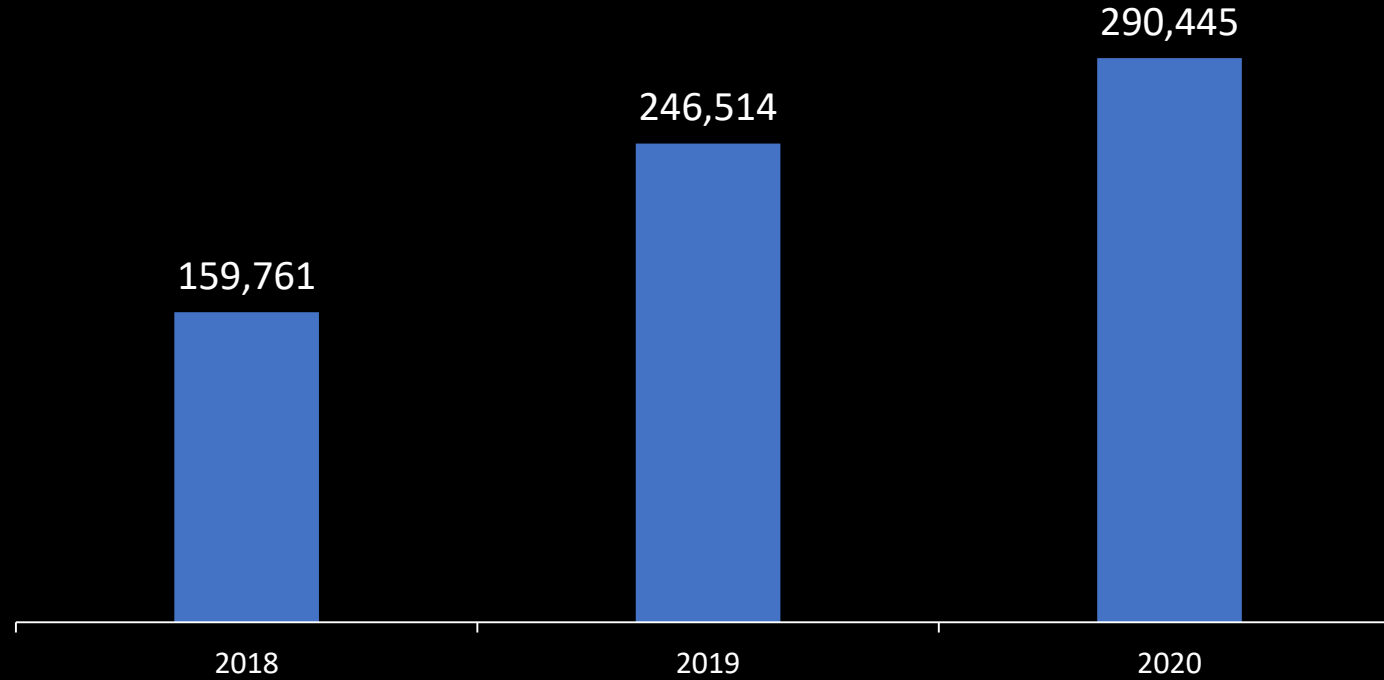


Source: MHA

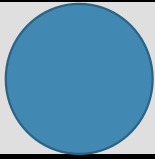




INCIDENTS RELATED TO DIGITAL BANKING



Source: CERT-IN



INDIA'S INTERGRATED RESPONSE

Cyber Security

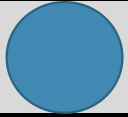
PREVENTION & SUPPORT



Cybercrime

PROSECUTION & DISRUPTION





CYBER CRIME IN INDIA : LEGAL PROVISIONS

- Information Technology Act , 2000 [IT Act Important Provisions](#)
- Procedure for investigation and trial - Criminal Procedure Code (CrPC), amended from time to time.
- Procedure for admissibility of evidence - IEA.
- Admissibility of electronic evidence incorporated post IT Act. [Section 65B introduced in IEA for admissibility of electronic evidence]
- Other Acts amended to recognize electronic record and digital evidence.
- Extra Territorial Extent (sec. 75 of IT Act) [75A of Information Technology Act](#)



Cheating by personation
using Computer Resource

66D

66E

Violation of Privacy

Cyber Terrorism

66F

67A

Transmitting of material
containing sexually explicit
act

Transmitting of material
depicting children in
sexually explicit act

67B

67C

Preservation and retention
of information by
intermediaries





CYBER CRIME INVESTIGATION DIVISION, CBI

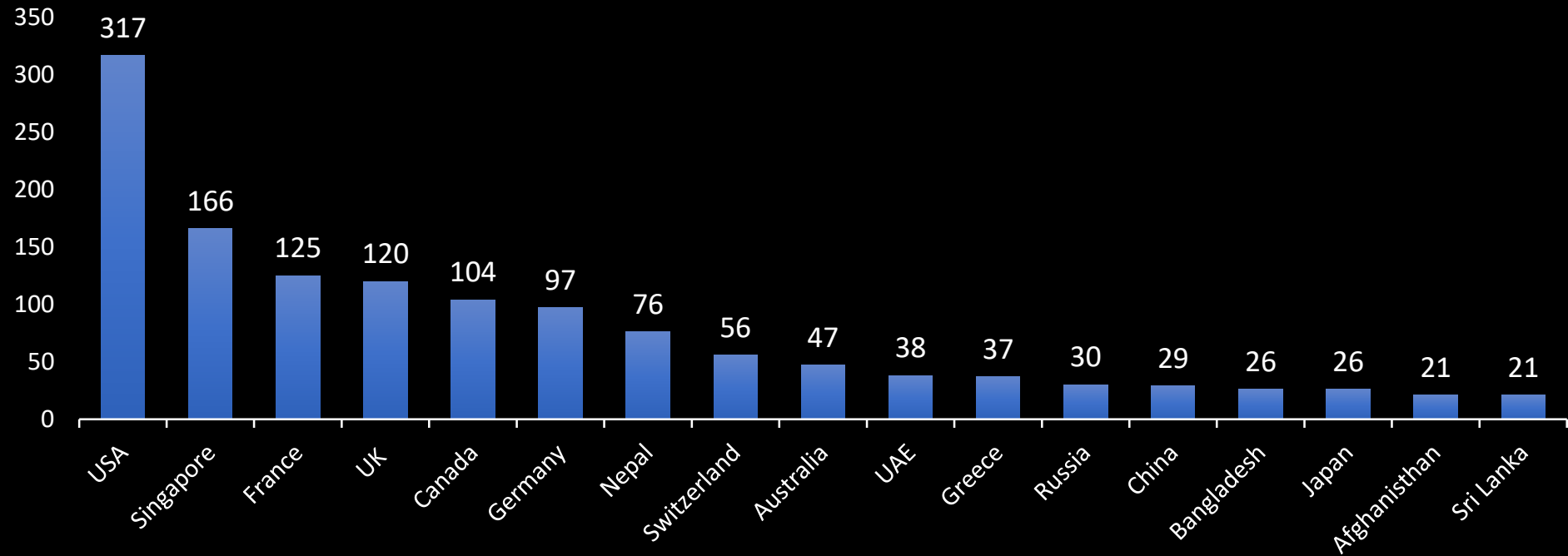
- Mandated agency of the Central Government to investigate Computer related crimes.
- Collaborates with the Indian Cybercrime Coordination Centre (I4C), CERT-IN and other LEAs in India and abroad, shares its experience and gives feedback to various agencies.
- Maintains close rapport with international agencies for exchange of ideas on latest trends and formulation of best practices in the field.
- Point of Contact for G-8 24/7 network, an international assistance / cooperation channel in addition to the INTERPOL.
- Conducts analysis of cybercrime trends, identifies areas requiring special attention for prevention and detection of cybercrimes





CCID & WORLD

CCID CBI receives references through NCB India from across the world



Source: NCB India





CHALLENGES

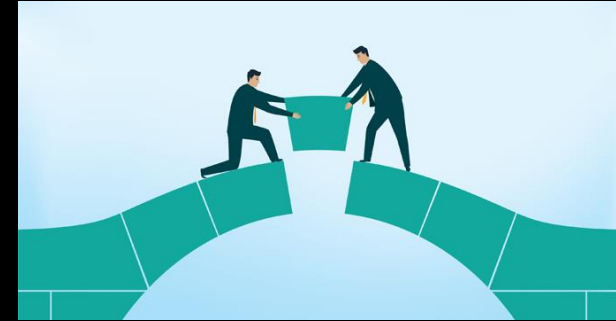
- Generalized Interpol Requests (Call Data, IP Records for extended & non specific period)
- Absence of follow up
- Missing Nodal Point
- Challenges of domestic laws
- Complainant Missing
- MLAT requests not coming
- Cumbersome and protracted procedure of LR-MLAT
- Lack of uniform formats across the agencies.





CHALLENGES

- Knowledge gap between victims (illiterate and semi literate) which makes them easy prey
- Creating public awareness for such large segment of population is a challenge.
- Challenges of awareness among Prosecutors and Presiding officers
- Multiple nation jurisdictions requiring LRs/MLATs for evidence
- Easy availability of spoofing call apps
- Availability of Scarce digital foot print due to use of VPNs, VOIP calls, use of anonymity networks to encrypt traffic and hide IP address and locations





WAY FORWARD

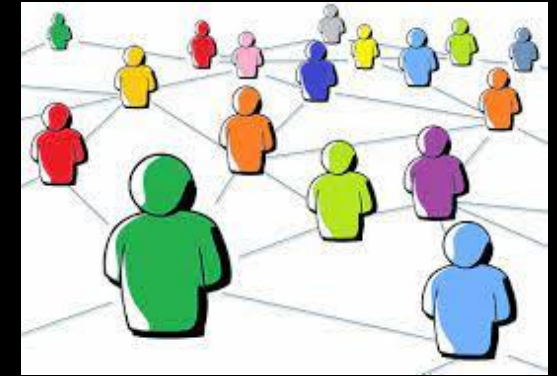
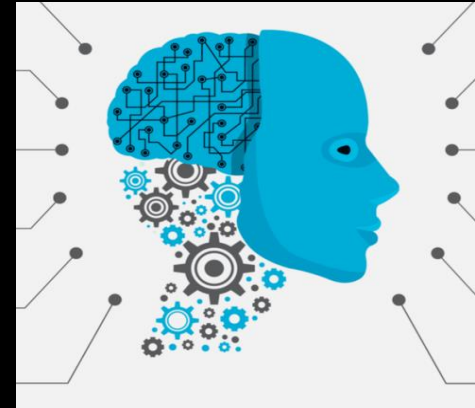
- Nodal points
- Continuous Follow Ups
- Cooperation in Investigation
- Formal/Informal Information Sharing
- Local Prosecution
- Cooperation in Data Preservation
- Mutual Capacity Building
- Sharing of best practices
- Sharing of Investigative tools





PREVENTIVE

- Close coordination between law enforcement, social media intermediaries, banks, financial institutions and tech service providers.
- Apply Big data analytics and A.I algorithms for trend analysis for patterns and connections.
- Mass public awareness campaigns involving various stake holders.
- Use of Public sector Banks (due to their geographical spread) to lead such public awareness campaign against financial crimes through use of technology.





PREVENTIVE

- Simple and easy to understand tools for awareness campaign.
- Vernacular campaign with simulated videos etc
- Use of social media and mobile service providers to alert public on new cyber crime methods and provide guidance
- Publish awareness material in local print and visual media including TV channel service providers in local language need to be done extensively



EFFECTIVE RESPONSE TO CHALLENGE REQUIRES CROSS-JURISDICTIONAL COLLABORATION



Thank You

