

Innovation led cybercrime management

22 August 2019

FICCI

EY
Building a better working world

Foreword

The advent of initiatives such as Digital India and Smart City has brought about a paradigm shift in connectivity, services and threats in urban and rural areas. While greater connectivity promises wider deliverables, it also paves the way for the emergence of new vulnerabilities. Several leading companies in energy, telecommunications, finance, transportation and other sectors are targeted by new-age cyber criminals/adversaries.

The Institute for Defence Studies and Analyses (IDSA), in a report on cyber security, had warned of system failures across India due to cyberattacks against critical infrastructure. As per CERT-IN, one cybercrime was reported every 10 minutes in India during 2017. As alarming as it may sound today, but in the future, with 5G and IoT, on which AI will ride as part of economic nerves system of a country in war and peace (or we will be under permanent "peace-in-war"), these threats will be like walk in a garden. We can no longer be in a delusion that cyber security threats dwell exclusively in abstract cyberspaces or software. Hardware can be seriously compromised (for e.g., Super Micro motherboard hacking of Apple, a Bloomberg story).

China and PLA believe that AI will fundamentally change the character of warfare, resulting in a transformation from today's informatized warfare to future intelligentized warfare. A RAND study adds that China is preparing for systems destruction warfare, in which wars will be won by the belligerent that can disrupt, paralyze or destroy the operational capability of the operational system of the enemies, which includes sabotaging a country's cybersecurity infrastructure.

Now, work is required to be done in defining a Public Private Partnerships to develop a cyber security framework with participation of all national security players, owners/entities and regulators of critical infrastructure, Indian industry and innovation ecosystem to create intelligentized products. As internet is world wide web, with a wall at the gate of China, Team India needs to define and develop its cyber defence in partnership with global friends. In true "Make-in-India" spirit, given the Indian competitive advantages, it will be a win-win for all.

The Make in India initiative has identified 25 core sectors as part of its effort to give a special thrust. While cyber security is not one of the sectors, it could be embedded in certain sectors like – defence manufacturing, electronic systems, and IT and BPM. Make-in-India on cyber security and development of indigenous solutions to fight combat cyber-crime is the only way to create a viable "cyber defence" for India. In today's times, traditional methods of cybersecurity are inadequate to combat cybercrimes. Hence, there is a need to devise mechanisms which are proactive in nature and help in identifying and preventing cybercrimes/ cyber warfare.

This report delves into the strategies to confront new-age cyber-criminals with effective strategy for cybercrime management. I am confident that this report will be of considerable value to all the stakeholders in managing the threats in cyberspace which affect everyone.



Rahul Chaudhry
Chair- FICCI Committee on Homeland Security

Preface

Due to the extent and pervasiveness of cyber security threats, today's digital society is at risk. Nation states and cyber criminals are equipped with state-of-the-art capabilities and have the adequate funding to disrupt any type of ICT and OT infrastructure. The breadth and scope of cybercrimes is rising exponentially, damaging the digital aspirations of several industries and sectors such as healthcare, e-governance, retail, manufacturing, transport and financial services, including digital payments as well as smart cities in India and globally. While we often attribute cyber risks to the hackers' growing arsenal of tools, this can no longer be accepted as a reason for poor security practices and lack of visibility over weakness in nation's and organizations' digital infrastructure inventory.

Hi-tech crimes have been extant for numerous decades now. Criminals, over the years, have updated their methodologies and modus operandi with aid from emerging technologies to conduct crimes with ease. Criminals have evolved from the days of carrying pagers and leveraging cheap mobile phones and have built their own infrastructure to perpetrate crime in cyber space. Hence, criminals are early adopters of emerging technologies. Moreover, the returns from such crimes have also risen to billions of dollars from thousands and millions, without causing physical injuries and confrontations with victims. Fearmongering in cyber space is the new mantra.

The society and nations that are being built today with technological tools and the impact they are stirring on dual use of technology. Hence, to mitigate the aftermath of cyber threat tsunami sooner rather than later, cybercrime management ecosystem in India and globally warrants a concerted effort.

Such concerted and collaborative efforts are likely to provide assurance and trust to India's economy. It may also positively impact the conviction quotient in future era of ubiquitous computing. This joint thought leadership from FICCI and EY is a reference document for law enforcement and government agencies to enable them to understand the evolution in cyber space to prepare them for the future with the help of effective cybercrime management initiatives in the country while leveraging emerging technological innovations. This document provides a direction to tackle myriad cybercrime threats that we face as a society, today.



Rahul Rishi
Partner and Leader - Advisory Services,
Government and Public Services



Contents

06 Introduction

08 Changing face of cybercrime: trends, cyber threats, crime scenarios

14 Paradigm shift in digital technologies in India and cybercrimes

20 Challenges in cybercrime management

24 Innovations/Models in cybercrime management

30 Way forward



1 Introduction

> If we have to build public's trust in a digital world, then we will have to bear zero tolerance towards cybercrime
>
> Rajnath Singh
> Defence Minister of India
>
> Source: Press Information Bureau

The number of internet users in India had already reached half a billion in 2018[1]. Due to wide reach of mobile networks, cheap data prices, easy availability of feature and smartphones, etc., these users are distributed across urban and rural areas. Initiatives like Digital India and smart cities mission, which are part of technology-led transformational programs, have further empowered the Indian citizens at different levels. Continuous developments in the fields of analytics, technologies like Artificial Intelligence, Machine Learning, Cloud Computing and improvement of mobile applications open new possibilities for India's economic growth, nation building and citizens' empowerment. Simultaneously, these developments have shifted the crime pattern from physical to the digital world.

Cybercrime, which was limited in scope and reach till a few years ago, has now become the biggest challenge for the nation states and the law enforcement agencies (LEAs). The web of cybercrime is becoming a new and by far, the most formidable frontier for the LEAs, where the perpetrators are faceless and are often located beyond the boundaries of a nation's jurisdiction and fail to get controlled through traditional policing methods. Cybercrimes, at large, impact governments, organizations and end citizens, impacting their robust functioning or daily life w.r.t availing services and conducting daily business.

In contemporary era, cybercrime has been dominated by novel, extremely sophisticated methods, making it difficult for law enforcement

1 https://www.statista.com/topics/2157/internet-usage-in-india/



agencies to manage the impact of attacks effectively. Over 90% of hackers are under the age of 35, out of which 58% are self-taught and 44% possess professional IT experience and certifications[2]. This means technical education does not play a relevant role in executing a cybercrime, but knowledge sharing perpetuates the issue. India lists among top five in the world for most high-profile cyberattacks caused by involving the usage of techniques like credential stuffing for account take over, exploiting gullibility of children and women at large and carrying out fraud on end citizens[3].

Some of the other high-profile cybercrimes in India include Petya ransomware attack on Jawaharlal Nehru Port in 2017[5] and a malware attack on Indian bank's ATMs that led to a loss of INR944 million (US$13.5m)[6]. In addition to the targeted attacks against businesses, individuals have also fallen prey to social engineering attacks, cyber coercion, etc. and have lost money. Use of mobile apps to inject malware into victim's mobile phone is yet another vector being used by cyber criminals. As per EY-Global Information Security Survey 2018-19, malware (20%), phishing (22%) and disruptive cyberattacks (13%) are the top three threats that organizations face[7]. Customer information, financial information and strategic plans of organizations are the top three most valuable pieces of information coveted by cyber criminals.

> “As per the information reported to and tracked by Indian Computer Emergency Response Team (CERT-In)[4], between January 2018 to November in 2018, 15,779 Indian websites were hacked.

2 https://www.hackerone.com/sites/default/files/2018-01/2018_Hacker_Report_0.pdf
3 https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-report-2019.pdf
4 https: https://www.cert-in.org.in/
5 http://164.100.47.194/Loksabha/Questions/QResult15.aspx?qref=56072&lsno=16
6 https://www.securonix.com/web/wp-content/uploads/2018/08/Securonix-Threat-Research-Cosmos-Bank-Report.pdf
7 https://www.ey.com/Publication/vwLUAssets/ey-global-information-security-survey-2018-19/$FILE/ey-global-information-security-survey-2018-19.pdf

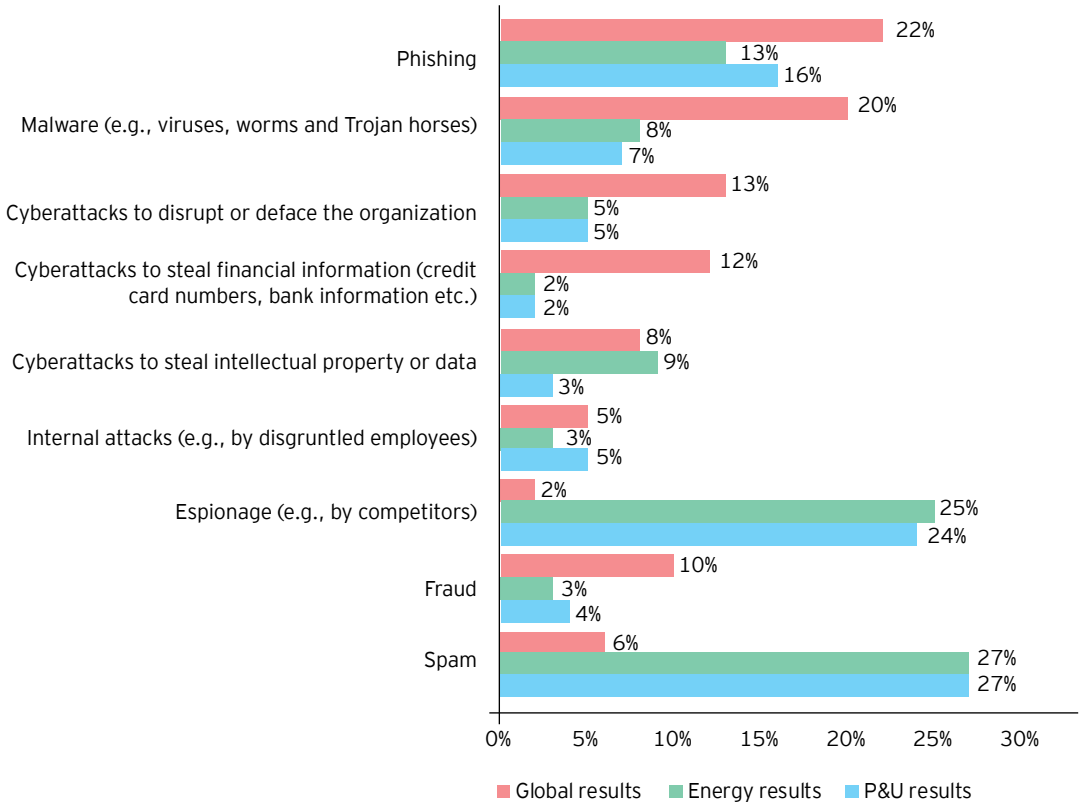


2

Changing face of cybercrime: trends, cyber threats, crime scenarios

Organizations and governments, have shaped innovative opportunities by digitally transforming their operations by adopting digital technologies like mobile, Internet of Things (IoT), cloud, blockchain and Artificial Intelligence. The transition towards edge computing may have a significant impact on IT and operational technology (OT) systems and is laying the foundation of new digital era. The use of advanced technologies has benefited states and governments but have increased the risk of cyberattacks and helped cybercriminals to increase their influence. There is still a noticeable gap in knowledge for the implementation of cybercrime legislation, cybersecurity strategies, computer emergency response teams (CERTs), awareness and capacity to spread out the strategies and capabilities in the field of cybercrime management.





Source: EY Global Information Security Survey 2018-19

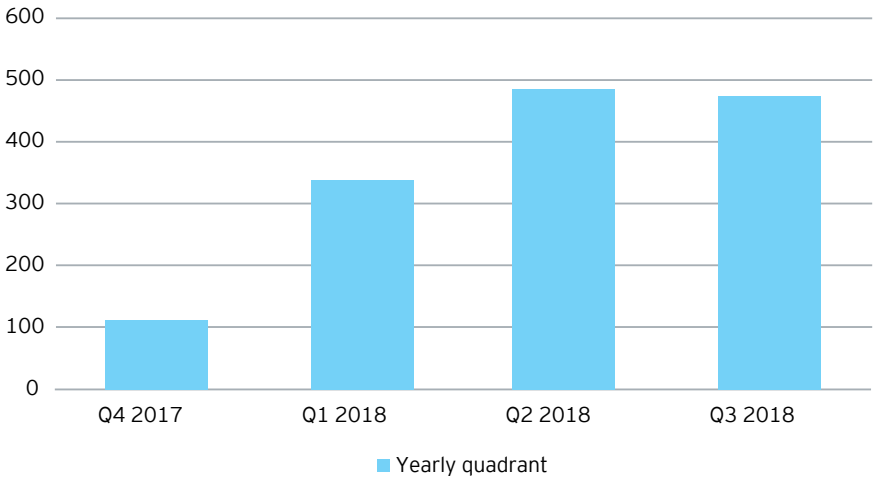
2.1. Trends in cyber space

Targeted phishing attacks[8]

Phishing is the most common way of stealing information in today's cyber world. Phishing attacks continue to be at the top of security threats, as gullible users continue to fall for it. The attacks are getting sophisticated day by day with well-crafted emails. A 2018 study showed that there is a 297% increase in retail phishing websites as compared to previous year.

Another study conducted by Forbes showed that 22% of online phishing attacks happened on global companies whereas 13% on companies catering to energy sector and 16% on power and utility sector. Critical infrastructures are becoming prime targets among the hackers, in which phishing is leveraged as a technique significantly.

Retail phishing websites

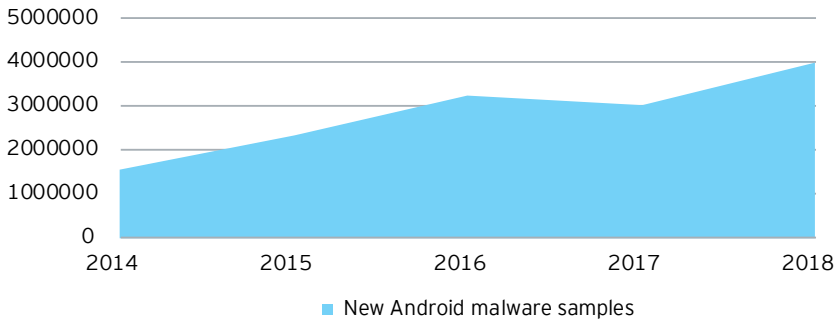


Source: Forbes Tech Council

Use of mobile devices by cybercriminals[3]

Mobiles are becoming the more preferred way of launching cyberattacks as they allow quick getaways and ubiquity. Cybercriminals are developing customized applications to increase their anonymity and to avoid detection of their identity which makes tracking them down even more difficult. There is an average of 82 rouge mobile applications identified each day. A mobile application called as "Battery Saver" has infected more than 60,000 users and was available on Android app store. Hackers were successful to plant a rogue code inside the application and successfully uploaded the .apk file on the Android Play Store to make it guise as a legitimate application and leveraged it to steal the user data on mobile devices. A survey done by GDATA shows the rise in Android malware samples and predicts that the same scenario will continue in the coming years due to the dynamic increase in the mobile technology and with the rise of cyber threats.

Survey for Android malware



Source: GDATA

8 https://www.forbes.com/sites/forbestechcouncil/2019/02/07/five-cybersecurity-trends-to-watch-for-in-2019/#3ae708d34c66

3 https://www.akamai.com/us/en/multimedia/documents/state-of-the-internet/soti-security-web-attacks-and-gaming-abuse-report-2019.pdf

Darknet: a threat to society[9]

Illegal trade on darknet markets is an arduous challenge to grapple with and is augmented by increasingly complex nature of transnational organized crime. Darknet markets, also known for crypto transactions, provide a large anonymous platform for trading in illegal goods and services like drugs, weapons, cyber-crime-as-a-service (CaaS) and even child pornography. Hackers also share their vulnerabilities and even malicious tools over it. CaaS is widely available on various types of dark-web platforms. Since these transactions use crypto-currencies, this makes it virtually impossible for law enforcement agencies to track and trace them.

Legitimate platforms for illegal activity[10]

Cybercriminals often use popular social media platforms like Facebook, Instagram, WhatsApp, etc. to communicate and conduct frauds. Social media fraud attacks such as scamming (selling of fake products, identity theft, creation of fake account, etc.) have increased significantly over last few years and methods of duping are becoming innovative day by day. As per media reports, cybercriminals have recently used Telegram Bot to automate their illegal and fraud activities. The illegitimate platforms are elevating the demand of offerings such as fraud-as-a-service and include categories of search like debit cards, wallets, sale of private software, VPNs, selling bank accounts, coupons, pirated movies and TV seasons and hiring manpower for illegitimate activities.

Bulletproof hosting[11]

Bulletproof hosting is identical to regular web-hosting. The former is significantly lenient about what can be hosted on their servers and follows "don't ask, don't tell" policies. Bulletproof hosting services are often found in countries which have relaxed laws on the content type to be hosted on these servers. These countries are the ones with weak extradition laws, therefore it becomes easier to evade law enforcement. Due to the varied laws in different countries, the vague or weak laws create a grey area that allows the hosting service providers to claim immunity against what their customers host. Illegitimate hosting services are used to host exploit kits, store stolen data and even host illegal websites under the shadow of dark web.

Blockchain for cybercrimes

Blockchain is rearchitecting how trust is to be delivered in digital use cases. Blockchain is experiencing its own challenges with respect to its usage in cybercrimes. For e.g., blockchain offers utility benefits in the IoT field. With the number of connected devices predicted to increase by 26 billion during 2019, there is an increase in the use of a blockchain-based domain name system (DNS) to host sites that sell illegal services and other sensitive data. Unlike normal DNS, blockchain-based DNS have no oversight which makes it even harder for law enforcement to investigate.

The popularity and use of blockchain among cybercriminals are growing and are likely to improve cybersecurity of their infrastructure and secure their illegal operations. Cyber criminals, being extremely adaptive and imaginative, use a concoction of old and newer techniques to stay alive and avoid being caught.

Abuse of RPA and data ethics

Robotic Process Automation (RPA) is focused on automating monotonous activities in offices such as of cashier, teller and data entry, and can have a transformative impact on organizations. These monotonous activities include automating processing insurance claims, procurement, payroll, bank reconciliation, invoices, etc., reducing the processing time by 70%. However, RPA accompanies some security risks. The usage of robotic process information robot gives access to the confidential information that can be leaked. It also provides criminals the authority to hijack RPA to misuse the system or its data. The processes and tasks that are modifiable to automation are often organizational procedures that require automation platform to have access to confidential information (i.e., customer data). If a robot gets compromised by some cyberattack, all the confidential information which the robot had access to also gets compromised with it. With the growth of technology, cyber threats also grow.

9 https://www.europol.europa.eu/publications-documents/drugs-and-darknet-perspectives-for-enforcement-research-and-policy

10 https://community.rsa.com/servlet/JiveServlet/downloadBody/101537-102-1-257415/RSA-CurrentStateofCybercrime-2019.pdf

11 https://us.norton.com/internetsecurity-emerging-threats-what-is-bulletproof-hosting.html

2.2. Emerging cybercrime threats

ATM attacks (Jackpotting)[12]

Jackpotting is the most sophisticated form of exploiting automatic teller machines (ATMs) and is a new entrant to the cybercrime radar. This approach involves infecting an ATM with malicious software. Any early form of this type of attack involved the transfer of malware to the ATM on a USB through an interface portal. Hence, modes of infiltration are becoming more effective and necessitate less involvement of the hacker.

Crypto jacking

The year 2018 witnessed a rise in crypto jacking, a technique which leverages malware or other means to infect an end-user's computers with software that hijacks the systems' resources and sets them to mine cryptocurrencies. In 2019, this effort is likely to accelerate again, as hackers try to compromise cloud administrator accounts using new or known vulnerabilities, by phishing for administrator credentials. Hackers are likely to exploit these accounts by running mining software to mine cryptocurrency and may remain undetected for a considerable amount of time.

Form jacking[13]

The use of malicious JavaScript code to steal credit card details and other sensitive information from payment forms on the web pages of e-commerce sites or any other site with payment section is termed as form jacking. Form jacking is not a new technique, but recently, they have emerged as an interesting and sophisticated way of stealing information. Form jacking has increased dramatically since mid-August 2018. Almost 50,000 retailer websites are compromised last year by a hacker group called as Magecart which inserted malicious code into their websites to steal payment card information of thousands of customers.

AI for cyber criminals

AI's limited usage era in our day to day life has ended. Its presence is ubiquitous with emergence of never seen cyber risks. Hackers are capable to infect organizations' systems using smart AI-powered malware. This malware may remain undetected and propagate inside the network and may be able to gather the information about users' behaviors and organizations systems. Adapting to its surroundings, the malware can unleash a series of attacks targeted to take the advantage of the user. The sophistication of this attack is new and may prove to be extra effective. While a few examples of the attacks using AI have been seen in the form of bypassing CAPTCHA systems, improving the accuracy of phishing, developing highly evasive malware, etc.

> "According to a report, cryptocurrency thefts, scams and fraud could tally more than US$1.2 billion in first quarter of 2019.

Ransom hack

A new type of cyberattack called a ransom hack has been observed in recent times. In case of a traditional ransomware attack, customer data is held hostage until the ransom is paid, however, in case of ransom hack, data is not released even if the ransom is paid.

Targeting end citizens

Majority of the attacks globally are developed with a motive to dupe gullible end citizens, exploiting their lack of awareness and weak security preparedness while using ICT systems. The impact has evolved from data breaches in availing services to jeopardizing end citizens' life in the context of smart cities.

12 Cyber Risk Radar for BCM - Q1 2019 EY discover

13 https://www.symantec.com/blogs/threat-intelligence/formjacking-attacks-retailers

2.3. Cybercrime scenarios

Global campaign targeting critical sectors[14]

An antivirus giant in India discovered a new global campaign which was targeting nuclear, energy, defence and financial companies. The campaign took advantage of an in-memory implant to download and retrieve a second-stage implant called "Rising Sun" for further exploitation. The Rising Sun implant uses source code from Lazarus Group's 2015 backdoor Trojan in a new framework to infiltrate these key industries. The campaign, while masquerading as legitimate industry's job recruitment activity, gathers information to monitor for potential exploitation.

SS7 exploit intercepts the SMS sent for two-factor authentication

Recently a bank in United Kingdom became the victim of Signaling System 7 (SS7) protocol exploit. Cyber-criminals misused this convention, which is typically being utilized by telecom organizations to arrange steering of writings and calls. This method helps track telephones over the world and allows them to block telephone calls and messages without compromising the phone. As per the UK's National Cyber Security Center, this was used to capture codes (OTPs) utilized for banking transactions.

Public blockchain: Ethereum Classic was attacked

According to Coinbase, a popular cryptocurrency exchange platform, the blockchain of Ethereum Classic (ETC) cryptocurrency was attacked. Attackers were successfully able to perform "51% attack" and gained access to more than half of the network's computing power to rewrite the transaction history. This gave the attackers over 50% control of the network's hash rate on the blockchain that uses a proof-of-work algorithm.

70 million records stolen from poorly configured S3 bucket[15]

Simple Storage Service (S3) bucket is a cloud storage resource available in Amazon Web Services' (AWS). A single misconfigured cloud storage instance could cost an organization a loss of millions. In 2018, more than 70 million records were stolen from a poorly configured AWS S3 buckets. There are tools which can identify misconfigured cloud resources and can make hackers work easier.

Drug dealing using dark net

The Dutch national police's Dark Web Team was responsible for shutting down the dark web market, Hansa in 2017. Approximately 4,000 drug dealers were actively selling illegal drugs and other illegal substances on Hansa. Europol created a dedicated dark web team, after the U.S. Justice Department created its own joint criminal opioid darknet enforcement team which is known as J-Code, to combat online illegal sales. The investigation into a dark web child pornography site called Playpen, the FBI performed "network investigative techniques," or NIT—code allowed them to remotely install malware on nearly 9,000 computers in 120 different countries to locate and track the administrators of the site.

14 https://nciipc.gov.in/documents/NCIIPC_Newsletter_Apr19.pdf

15 https://www.symantec.com/en/sg/security-center/threat-report



3 Paradigm shift in digital technologies in India and cybercrimes

The digitization drive and adoption of emerging technologies is improving livability index of the people across the globe[16]. Humankind is set to undergo another wave of technological revolution fueled by emergence of every object becoming a part of cyber interconnected mesh. To enable this community of connected devices, developers and research organizations are taking everyday things and making them significantly better by adding computing power and software and connecting them to the Internet. Parallelly, cybercrimes are on the rise globally and India is no different.

Indian LEAs are also realizing the importance of having an in-depth understanding of cybercrimes along with paradigm shift of use cases and technology evolution to counter the emerging cyber threats that are rendering the traditional investigative mechanisms ineffective and its management.

In India, LEAs are collecting data related to crimes at an exponential rate. This data either pertains to cybercrimes or crimes enabled by the technology. Majority of the data is unstructured and is stored in fragmented repositories across the nation leading to its underutilization.

16 https://www.mckinsey.com/~/media/McKinsey/Business%20Functions/McKinsey%20Digital/Our%20Insights/Digital%20India%20Technology%20to%20transform%20a%20connected%20nation/Digital-India-technology-to-transform-a-connected-nation-Full-report.ashx



Handling cybercrime at national level warrants a concerted, integrated and collaborative framework at national and state level. It may consist of components such as leveraging analytics on data to derive the meaning from data trails, sharing of intelligence information, in-depth understanding of emerging technologies and law of the land, etc.

3.1. National use cases and cybercrimes in India

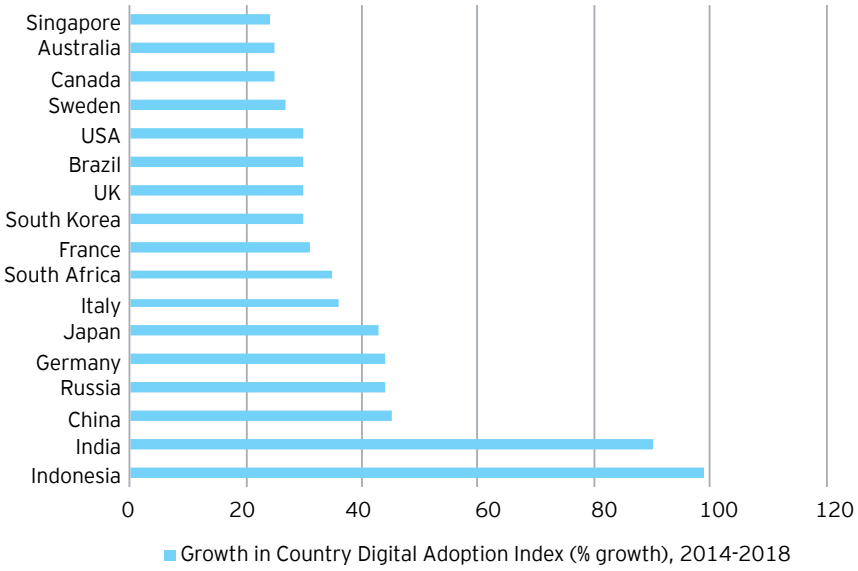
The Indian central government introduced Digital India in July 2015, under which, different projects were launched which resulted in refining e-governance and service delivery to citizens in each of the following areas:[17]

a) **eKranti – electronic delivery of services:** delivers government services digitally to improve efficiency, transparency and reliability. The progress has been made on 33 of e-Kranti's 44 mission mode projectss.[18]

b) **E-governance**: this project re-engineered the government to improve service and efficiency, examples include Aadhaar, e-visa and e-procurement. The central government published 926,070 electronic tenders in 2017–18, up from 476,983 in 2014–15.[19]

c) **Electronics manufacturing**: through this program, government promotes electronics manufacturing in India, with the target of net zero imports by 2020.[20]

Percentage growth in country digital adoption index (2014-2018)



Source: McKinsey

17 Digital India, May 1, 2018.
18 6 National e-Governance Division, Digital India, May 3, 2018
19 Central Public Procurement Portal, January 2019
20 "Mobile phones to get cheaper as government eases import duty", Hindu BusinessLine, May 6, 2016; MeitY, March 31, 2018.

d) Broadband highway: provides broadband connectivity in rural areas via optical-fiber cable to 2,50,000-gram panchayats, or self-governing village councils, to make it easier for millions of people to connect online.[21]

About 1.2 billion Indians have enrolled in Aadhaar, the world's largest unique digital identity program[22]. According to Global Cybersecurity Index, 2018, India ranks 47th globally with a score of 0.719[23]. The survey conducted by International Telecommunication Union assesses how countries are preparing themselves as per the changing face of cybercrime by following risk assessment-based approach and how India improved in the overall scoring from 2017's index results. The operational technology (OT) industry sectors such as manufacturing, energy, retail, etc. are also at par in adopting OT and IT connectivity and integrating its current infrastructure with internet to improve the country's progress.

This creates a new playground for cybercriminals to play in and posing a challenge for LEAs to catchup with industry use cases in India and usage of technology, leading to delays in cybercrime investigation, thwarting the menace and conviction of cyber criminals.

3.1.1 Crime scenarios in India

Case categories	Investigation objectives
I. Cases of cheating or fraud and embezzlement relating to public joint stock companies, large-scale banks, securities, insurance frauds, excise and customs, company related matters, corporate governance frauds	▶ Capturing and analyzing money trail in frauds ▶ Tracing the convict in India or globally ▶ Establishing credibility of evidence
II. Cybercrime cases like malware, virus attack, zero-day attack, denial-of-service (DoS); distributed-denial-of-service (DDoS) and computer-related frauds like carding, identity theft, phishing attack and internet scams	▶ Examination of mobile, computer and network devices, mails, emails, call data records, bank statements, financial records, etc. ▶ Cross border cybercrime investigation
III. Diversions of funds to associates, joint ventures or subsidiaries	▶ Capturing and analyzing anomalies in financial transactions
IV. Breaches of import and export control orders, serious breaches of Foreign Exchange Regulation Act, passport frauds	▶ Identification of convicts breaching the system and law of the land
V. Frauds or kickbacks (bribe), for e.g., non-listed firm's shares purchased at a higher price	▶ Enabling identification of insider frauds
VI. Violent Crimes enabled by technology	▶ Make data ingested for case(s) available for future case(s) as well for analysis and analytical purposes

21 For details of the government's action plan for digital, see India's Trillion Dollar Digital Opportunity, Ministry of Electronics and Information Technology, Government of India, February 2019.

22 UIDAI, April 2018;

23 https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf

3.2. Industrial use cases and cybercrimes in India

Digitization in the power and utility sector

Current state

- Utilities in India are investing heavily to modernize the infrastructure related to upgraded systems such as state-of-the-art email systems, IT infra, programmable logical controllers (PLCs), digital computer devices (DCCs), or supervisory control, data acquisition (SCADA) software, etc.

Breach

- A large PSU in India from oil and gas sector suffered a major cyberattack in 2015 involving identity thefts leading to losses of INR197 crore. Cyber adversaries replicated the firm's official e-mail address with trivial changes and used it to convince a client based in Middle East to transfer payments to their account.[24]

LEA's response

- Case filed under the IT Act and IPC
- Leveraging analytics tools, LEAs were able to trace the origin of the malware in the infrastructure of oil and gas firm which was used to establish a footprint in the PSU's IT environment
- By analyzing the email log, police concluded that someone was aware of the exchange of e-mails between the PSU and client regarding the transfer of a large sum of money who created an email ID like the one owned by the official of the PSU

Financial services and digital payments

Current state

- Financial technology or FinTech innovation is growing exponentially in India. Firms made early gains in digital payments as the number of transactions in India and payments made with digital wallets, mobile apps and net banking grew tenfold in last four years, from 202 million a month in 2013-14 to 2.03 billion a month in 2017-2018[25]. Exponential growth in digital payments and associated data have created plethora of novel opportunities in the way credit is assessed and delivered.

Breach

- A major e-wallet company in India suffered a major fraud in 2019 involving sellers and employees as accomplice in the crime. Fake transactions between merchants and employees were made to make undue gains from cashback offers, resulting in a loss of INR10 crore.[26]

LEA's response

- Case filed under the IT Act and IPC
- Police agencies seized system and hard drives of sellers and employees. By using the email investigation tool, the police analyzed the communication between the sellers and employees
- The e-wallet company's pertinent networks and database logs were investigated using analytics capabilities to establish the trail internally involving internal and external culprits

Healthcare

Current state

- India's healthcare system is vast and is fronting many difficult challenges, particularly in poor states and rural areas. The Indian Government recently introduced the National Health Protection Mission (Ayushman Bharat)[27]. To make the scheme work, the government acknowledged that it needs a digital platform as to support the technology. Besides enabling the quick enrolment of insurers and patients, the platform also could host electronic health records for each patient. With digital evolution, cyber risk has also increased.

Breach

- Indian hospitals crippled with the ransomware attacks as workers at Mahatma Gandhi Mission Hospital in Navi Mumbai discovered their computer systems locked in 2018, and an encrypted message demanded a Bitcoin ransom for decryption. The amount of the ransom and the strain of ransomware used has not been reported.[28]

24 https://www.expresscomputer.in/news/identity-theft-ongc-falls-prey-to-cyber-fraud-loses-rs-197-crore/14185/
25 Payment system indicators, Reserve Bank of India, Table 43, March 2015 and December 2018
26 https://www.livemint.com/companies/news/paytm-probe-reveals-at-least-10-crore-fraud-vijay-shekhar-sharma-1557838623841.html
27 "Ayushman Bharat for a new India 2022 announced", Ministry of Finance press release, February 1, 2018, pib.gov.in.
28 https://mumbaimirror.indiatimes.com/mumbai/crime/cyber-criminals-target-mgm-hospital-demand-ransom-in-bitcoins/articleshow/65031695.cms

LEA's response

- Case filed under the IT Act and IPC
- Police investigated infected systems with tools which enables analyzing the infected systems' processes and hard drives
- Cryptocurrency forensics tools were leveraged to trace the culprits

Retail and e-commerce

Current state

- Retailers running e-commerce platforms in India are running business on legacy IT infra with minimal protection. E-commerce industry is the one of the primary targets because it stores valuable personal information of end citizens.

Breach

- A major food retailer in India suffered a data breach in late 2018, resulting in a theft of 17 million users' records from a food-tech company's database. It caused the company to suffer reputational damage and direct and indirect losses translating it to a high revenue impact.[29]

LEA response

- Investigations are underway to investigate the footprints of cyber criminals with help of database and server forensics

3.3. Technological shifts in India and dual use

With the evolution in technology, there are no physical and logical limits as to where and when security breaches may strike. Technology shifts and trends may disrupt the business models and industries that exist today in next four or five years just like India is experiencing it now[30]. Cybercriminals use the same technology to commit frauds and crimes, opening the pandora box of dual usage of technology.

I. Cloud computing

- Cloud computing gives greater flexibility and functionality options to individuals and organizations. It can offer the same elasticity to be leveraged by the digital adversaries, and the pay-as-you-play usage model means that they can also benefit from the utility billing. It is noted that cyber-criminals are leveraging this platform:
  - as a business platform
  - to mount attacks like denial of service (DoS)
  - as a cybercrime target

II. Automation and robotics

- With the emergence of AI and robotics, it also entails the augmented risk of novel cyber security risks resulting in never seen cybercrimes. Robotic Process Automation (RPA) has become one of the major disruptors in this digital age.
- Cyber criminals, who either find a vulnerability in the cloud and hack into the robots or sink the financial markets, are certainly the most concerning risk. For businesses facing this criminal threat in the future, the consequences of a cyberattack could be devastating.[31]

III. Evolution of mobile transaction

- Mobile transaction is one of the key enablers of financial inclusion and access to online goods and services in growth and emerging economies.
- The mobile malware is on the rise with the number of new mobile malware variants introduced increasing by a massive 54% in one year. This is not helped by the fact that most mobile devices are running on older operating systems (only 20% of Android devices are running the newest release).
- Mobile phones in India are leveraged by cyber criminals for crypto jacking and denial of services attack with hijacking of computing power of devices.

IV. Analytics/Big Data

- In the current business environment with a pressing need to digitize, big data analytics is a critical component of an enterprise's digital strategy. When enterprises need to detect and respond to cyberattacks, industry follows the PDR paradigm, i.e., prevent, detect, respond. Companies and key analyst firms recognize that these challenges can be overcome with Big Data analytics. The same technologies are being leveraged by cyber criminals in India at large to profile their victims, to identify crown-jewels victims out of Big-Data haystack and to gain a richer understanding on specific targets.

29 https://retail.economictimes.indiatimes.com/news/industry/is-the-indian-retail-sector-doing-enough-to-be-cyber-secure/67850530
30 https://niti.gov.in/writereaddata/files/document_publication/CyberSecurityConclaveAtVigyanBhavanDelhi_1.pdf
31 https://www.weforum.org/agenda/archive/artificial-intelligence-and-robotics/

V. Artificial Intelligence

- Most of the principle industries are already leveraging Machine Learning (ML) and Artificial Intelligence (AI) to automate their processes and improve the overall performance. Cybersecurity and cybercrime are no exceptions. With new advances in AI-driven technology, utilizing AI in cyberattacks may become an even more popular[32].
- Cybercriminals are using various evasion methods to avoid detection and AI helps to optimize different elements of this process in India.
- While social engineering is one of the most popular hacking techniques, it takes a lot of time to implement it properly. AI may help in collecting information also by writing emails or calling potential victims.

VI. Virtual Reality and Augmented Reality

- Digital reality is likely to have manifold applications in consumer as well as enterprise space, in the longer term. Investments in the VR and AR segment are growing. Consumers are showing interest and industry leaders are recognizing these areas as a potential opportunity for growth. Misuse of AR and VR is being exploited for frauds and social engineering attacks in India.
- Data such as behavioral information, movement tracking and body measurements are highly sensitive. These along with other identifiers, such as name and financial transaction data, are being leveraged by sophisticated cyber criminals to create cyber avatars of India end citizens and commit crimes on their behalf without their knowledge.



32 https://www.weforum.org/agenda/2019/03/here-are-the-biggest-cybercrime-trends-of-2019/



4 Challenges in cybercrime management

The cybercrimes are generally increasing and are becoming a prevalent choice of most of the criminals due to the ease attackers derive in committing them. These crimes also offer less risk of getting caught as law-enforcement officials lack access to capabilities and resources which can be useful in effective cybercrime management. A few of these major challenges are briefly discussed below, which India needs to cater to and thwart the menace of cybercrime and threats robustly.

I. Inadequate training infrastructure

- A police officer's warrants capacity building in terms of technical skills in cyber forensics and security to investigate offenses under the IT (Amendment) Act, 2008 and other law of the land in making. Exhaustive and continuous training in cybercrime investigations and forensics to conduct quantity investigations is the need of the hour in states and central law enforcement departments.



II. Weak reporting culture

- The cybercrime reporting culture in India determines the emerging trends and can be used to build up data lakes to tackle future crimes. It is observed that lack of reporting in cybercrime in India due to end citizens' inadequate awareness and failure in treatment of cases pertaining to major crimes by central and state police institutions are responsible for increasing cybercrimes.

III. Absence of tools and capabilities

- Law enforcement agencies are equipped with inadequate digital forensic tools for performing initial forensic analysis under various domains such as disk forensics, mobile forensics, video and image enhancement, CDR, tower dump analysis, etc.

IV. Examination of case data suffers from undue delay

- Due to capacity constraints and increasing volume of data to be analyzed, there are plenty of cases pending with state and central forensics laboratories across India, resulting in creation of backlogs. This further leads to loss of critical time window to follow the leads due to delay in forensic examination in some cases. In such a scenario, investigating officers rely on the reports submitted by private cyber forensic companies which the analysis of articles.

V. Thwarting darknet markets

- Darknet refer to that class of networks that aim to guarantee anonymous and untraceable access to web content and anonymity for a site. There is now a sophisticated and self-sufficient digital underground economy in which criminals are providing cybercrime-as-a service using darknet such as selling of drug, hiring a contract killer, malware distribution, identity data, child pornography, etc. It is becoming increasingly challenging for the law enforcement agencies to actively target these underground markets and disrupt their services.

VI. Anonymity of cryptocurrencies

- The growing popularity and application of cryptocurrencies made some countries to legalize a few cryptocurrencies. However, it is extremely difficult to regulate cryptocurrencies and now numerous governments around the world are paying attention to them. LEAs too are facing challenges

in tracing the transactions and identifying the identity of the sources who are involved in the transactions.

VII. Legal framework limitations

- With emergence of new technologies, laws pertaining to cybercrime may become obsolete in many countries. For example, in the Indian scenario, currently, there is no law defining cryptocurrencies and fake news, and scenarios are still being debated with respect to cybercrime management.
- The data related to the offence or the offender may be residing outside India. In such cases, mutually legal assistance treaties letter rogatory process is invoked to get the information as evidence or accused from foreign countries. At the time of writing this paper, India have signed MLAT with 39 foreign countries. Double criminality or dual criminality is a requirement in the extradition law of many countries. It states that a suspect can be extradited from one country to stand trial for breaking a second country's laws only if a similar law exists in the extraditing country.

VIII. Lack of cooperation and collaboration

- Lack of cooperation between regional state LEAs and central agencies also pose challenges in cybercrime investigations. There is also a lack of platform where different state police units can collaborate or assist investigation officers in cybercrime cases.

IX. Emerging technologies

Lack of knowledge pertaining to emerging technologies and limited or no access to data located outside India poses bigger challenges for digital forensic examiners during investigations. There are also challenges under anti forensics bucket emanating from technology landscape, such as application usage of proxy, virtual private networks, steganography, spoofing, etc. committed by the cyber criminals, a few are discussed below.

- **Data encryption**

Pervasive encryption is widely used for modern communications and data storage. Using encryption would mean that when the LEAs seize articles such as hard disk, mobile phones during the search and seizure operations, the data can be recovered and processed using encryption keys.

- **Data wiping**

There are a wide array of free and proprietary tools specifically designed for data destruction where the investigation officers or agency undertaking forensic analysis fail to recover the required artefact after the data gets wiped.







5 Innovations/Models in cybercrime management

Cybercrime has evolved from the playground of individual hackers to a complex ecosystem of cyber adversaries collaborating in unison carrying out state sponsored cyberattacks against nations. Cyberattacks have become a part of organized crimes like cyber-extortion for financial gains, denial of services for critical ICT infrastructures, gaining unauthorized access, structured query language injection attacks using ransomware, malware, denial of service attacks, etc. Cyber agencies across the globe have envisaged various institutional models and is leveraging state-of-the-art technology capabilities to combat the menace of cybercrime and manage it effectively. A few of these models and developments are discussed below.

5.1. Global context

Law enforcement agencies in developed countries like the UK, the US, Russia and Japan, where cybercrime has been increasing exponentially have started building their dedicated cybercrime control centers, digital forensic labs, threat analytics units and other technology assisted units to catch and convict the cyber criminals. Disruptive technologies like AI, Machine Learning, cloud and Big Data, digital forensics, etc. have played a supreme role in combating cyber criminals. Some of the technological research and cybercrime management initiatives adopted globally are:

(i) **Cybercrime and policing (CARI)**[33] is a research collaboration where Leeds Beckett University works

33 https://www.leedsbeckett.ac.uk/csi/our-research/cybercrime-and-policing-cari/



closely with West Yorkshire Police with the help of external partners from CENTRIC at Sheffield Hallam University and Canterbury Christ Church University. This is gradually improving the frontline policing and incorporating evidence-based approach in digital forensics and cybercrime investigations. The center of excellence (COE) comprises of a training and research program which has the capability of directly impacting the digital forensics and cyber units within West Yorkshire Police to understand, analyze and use research, to help and support the evidence-based practice that these units provide to frontline officers across the region. Academicians also study the police force and conduct primary researches with them, to help them become more efficient and have effective identification, triage, acquisition, analysis and presentation of digital evidences. The research collaboration is also helping in examining the cyber investigation lifecycle from public viewpoint to recognize the gaps and requirements in policing against the cybercrime.

(ii) **The Romanian Center of Excellence for Cybercrime (CYBEREX-RO)**[34] was launched in Bucharest, Romania, in 2015. It was started with the purpose of training not only police officers, but also judges and prosecutors in fighting cybercrime. The center also seeks expertise from other major groups of the country like Computer Emergency Response Team – Romania (CERT-RO), military technical academy, police academy, training center in informatics, as well as actors from private sector (service providers). There are various objectives which is required to be met under this CoE. They are:

- developing the training curricula;
- forming a group of professional trainers
- testing the functionality of the center and circulating the results;
- training the police officers and judges in forensic analysis, criminal investigation, legal issues and legal trails.

(iii) **Cyber Fusion Center**[35] is located at INTERPOLs Global Complex for Innovation, Singapore. This is a specially developed center that brings together cyber experts from law enforcement agencies and industries to gather and examine the data available on cybercrime activities, share the technological constraints in investigations and provide the member countries with comprehensive, functional intelligence along with relative solutions.

34 https://ec.europa.eu/home-affairs/financing/fundings/projects/HOME_2011_ISEC_AG_INT_4000002223_en
35 https://www.interpol.int/en/Crimes/Cybercrime/Investigative-support-for-cybercrime

(iv) **Israel Police** collaborated with the Ben-Gurion University of Negev to develop cutting-edge cyber, Big Data and AI-powered tools[36] that enable detection, analysis and prevention of cybercrime by extrapolating when and where it can happen. These AI tools were trained by cybercrime data sets. Once these tools are trained, they provide analytical capability for crime investigations.

(v) **Internet Crime Complaint Center (IC3)**[37] is an initiative by the FBI that involves itself in a large range of cybercrime schemes that affects victims, both domestically and abroad. It also provides a portal to file complaints in cybercrime spectrum along with all forms of online frauds. Actual victims as well as third-party merchants can file complaint/s on the portal.

(vi) **Digital Forensics Laboratory**[38] is located at INTERPOL Global Complex for Innovation in Singapore. It enhances the ability of member countries to extract and use digital media in major cybercrime cases and helps building robust evidences against the suspects. The lab helps in malware analysis, examining digital devices, training police personnel in latest digital forensic tools and techniques, in providing support in digital investigations, etc.

(vii) **Research and Innovation Department** brings together cyber threat researchers at INTERPOL, to help policemen understand how diverse technologies like blockchain and AI work thereby helping them demystify the world of dark web and cryptocurrencies. The department also spreads awareness about the malicious use of technology in security community and shares advisory on the same y undertaking continuous research.

(viii) **Joint Cybercrime Action Taskforce (J-CAT)**[39] is an organized response to cybercrime prevailing across the international borders. Launched by European Cybercrime Center (EC3), it aims to drive an intelligence-led, coordinated action against major cybercrimes facilitated by joint identification, prioritization, research and commencement of cross-border investigations and operations.

5.2. Indian context

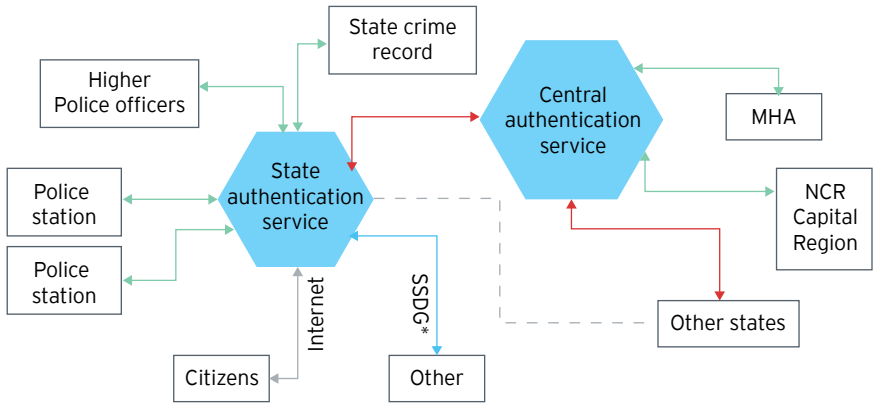
Cybercrime combatting initiatives and models have been adopted within India to help LEAs and government. Some of the technological research and cybercrime management initiatives adopted in India are:

Key highlights

Sl. No.	Learnings
1.	Use of technologies like AI and Big Data to develop tools which help in reducing cybercrime by predicting when and where the cybercrime will happen again.
2.	Centers of Excellence involving academic institutes conducting research to support evidence-based investigations and working towards capacity building of the police force to help them being more efficient in tackling cybercrimes.
3.	A central portal to register complaints on all forms of cyber and online frauds with its integration with state units and threat intelligence sources.
4.	Cyber centers, technology assisted units with state-of-the-art technology infrastructure which will also bring cyber experts from industry and police forces together to examine cybercrime activities and provide threat intelligence.
5.	Joint taskforce can be put into action where police from all the member nations or states can jointly address international and national issue of cybercrime management.

36 https://cyber.bgu.ac.il/israel-developing-cutting-edge-artificial-intelligence-crime-fighting-tools-2/
37 https://www.ic3.gov/media/IC3-Brochure.pdf
38 https://www.interpol.int/content/download/5267/file/Cybercrime.pdf

Figure 1: Crime and Criminal Tracking Network System (CCTNS)



SSDG*- State e-Governance Service Delivery Gateway

Source: EY analysis

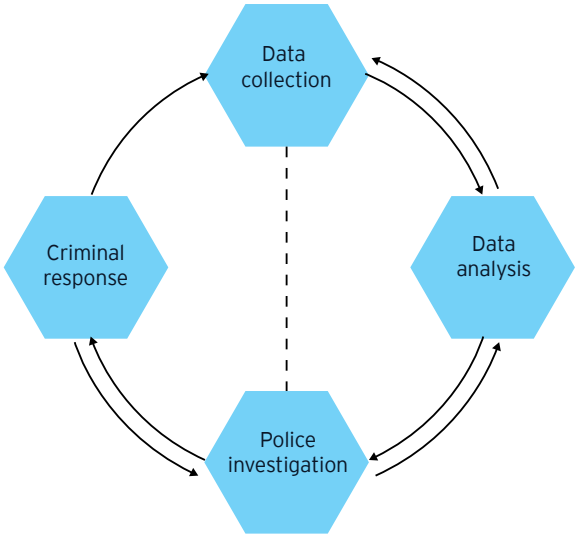
(i) Crime and Criminal Tracking Network System (CCTNS)[40] is an e-governance mission mode project under the National e-Governance Plan (NeGP) of Government of India. This project pursues better establishment of citizen-centric services and envisions to connect nearly 14,000 police stations across the country to accelerate investigation, detection and prevention of crime. The government also aims to roll out CCTNS 2.0 that aims at building up citizen portal, national integrated repository of FIRs, equipping police with state-of-the-art technology capabilities, trend reporting of cybercrimes and setting up test beds for state police stations to leverage.

(ii) Kerala Police Cyberdome[41] is an established Center of Excellence initiated by the state government to enhance the cyber security skill set and aiding them with latest technological changes and innovations in the cyberspace. It operates as an online office with technical specialists, ethical hackers and proficient cyber security professionals, who assist the police around cyber security, investigation of cybercrimes and domain knowledge, thus helping in discovering the cybercrimes and supporting in identifying the identities of cyber-criminals.

(iii) Predictive policing encompasses usage of Machine Learning algorithm to predict crimes based on four major data points: crime type, crime location and crime date/time and crime opportunities. Proactive interventions for the predicted crime scenarios can result in less crime rates. A similar concept of predictive policing is now under consideration for many of the state police in India especially, Assam Police and Karnataka Police.

(iv) Cyber Peace Research Center[42] is established by Cyber Peace Foundation. It is a community-driven collaborative open source framework for R&D, which aims to cultivate and develop awareness, recommendations, trainings and innovations in cyber space. The foundation is working on many useful projects like preparing an online dashboard known as e-kawach, which is an early warning system for cyber threats across the globe; a cyber security mobile application for kids, a project that deals with fake news on social media platforms, building ethical hacking and malware hunting courses, etc.

Figure 2: Predictive policing algorithm



Source: EY analysis

39 https://www.europol.europa.eu/activities-services/services-support/joint-cybercrime-action-taskforce

40 http://ncrb.gov.in/BureauDivisions/cctnsnew/index.html

41 http://www.cyberdome.kerala.gov.in/

42 https://www.cyberpeace.org/centre-of-excellence-e-raksha-research-center/

(v) **Cyber forensics** is another scientific area where India has evolved. Tools under cyber forensics domain help investigators in extracting, analyzing and presenting data/ evidence from digital sources, which might have recorded or logged some information related to crime. Many countries have established a cyber forensics lab to provide support services to government and law enforcement agencies. Recently, Delhi Police has established a National Cyber Forensic Lab in New Delhi to support the LEAs and other authorized agencies in India. Some of the common services provided by cyber forensics labs/units are:

- On-site support to identify, examine and preserve electronic devices and data
- Cyber forensic intelligence
- Complex electronic data recovery
- Audio and video analysis
- Malware related analysis

(vi) **Cryptocurrency course for IPS officers**[43] aims to educate IPS officers on the introduction of the functioning of deep and dark web, cryptocurrencies and blockchain technologies, legal aspects of cryptocurrencies and modus operandi on crimes committed using these technologies involving cryptocurrencies transactions. Started by the National Police Academy of India, these courses offer an insight on dark net monitoring and cryptocurrencies and are meant for Indian Police Service (IPS) officers.

(vii) **Indian Cybercrime Coordination Center (I4C) Scheme**[44] was started by the Ministry of Home Affairs (MHA), India, which acts as one of the apex bodies for fighting against cybercrime. The most important function of I4C is to identify the needs of LEAs and to perform R&D activities for developing forensic tools using new technologies. They also recommended changes and amendments in the sections of cyber laws to keep pace with the technological changes. Some of the key components envisaged under I4C are:

- National Cybercrime Threat Analytics Unit (TAU)
- National Cybercrime Reporting
- Platform for Joint Cybercrime Investigation Team
- National Cybercrime Forensic Laboratory (NCFL) Ecosystem
- National Cybercrime Training Center (NCTC)
- Cybercrime Ecosystem Management Unit
- National Cyber Research and Innovation Center

(viii) **Cyber Swachhta Kendra**[45], also known as Botnet Cleaning and Malware Analysis Center, is part of the Government of India's Digital India initiative under the Ministry of Electronics and Information Technology (MeitY). It is aimed to develop protected cyber space by identifying botnet infections in India, to advise and help cleaning and securing the systems of end users such that it prevents further infections. This kendra or center is a set up in accordance with the objectives of the "National Cyber Security Policy, 2013", which aims at creating a secure cyber ecosystem in India by generating trust in IT systems of cyber space and thereby help in enhancing the economy.

(ix) **Cybercrime Prevention against Women and Children Scheme (CCPWC)**[46] by Ministry of Home Affairs, India, is a scheme with an objective to provide an effective mechanism to handle cybercrimes against women and children in the country. Some of the key components of CCPWC are:

- An online cybercrime reporting platform for victims
- A national level cyber forensic laboratory to carry out deep forensic analysis
- Capacity building programs to train police officers, judges and prosecutors

43 https://koinpost.com/national-police-academy-of-india-launches-cryptocurrency-course-educate-ips-officers/
44 https://mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-Indian-Cybercrime-Coordination-Centre-I4C-Scheme
45 https://www.cyberswachhtakendra.gov.in/
46 https://mha.gov.in/division_of_mha/cyber-and-information-security-cis-division/Details-about-CCPWC-CybercrimePrevention-against-Women-and-Children-Scheme

- Cybercrime awareness communications and campaigns
- A CoE for research and development
- Cybercrime awareness communications and campaigns
- A CoE for research and development

(x) **Assam Police Cyberdome and Digital Intelligence and Training and Analysis Center (DITAC)**[46] is a CoE for Assam Police. It is designed to address and encounter long-term security challenges in the digital space and for capacity building of police personnel and developing basic cyber awareness and understanding among citizens of the state. Some of the major functions of this cyberdome are:

- To support cyber investigation, cyber intelligence and cyber forensics
- Internet monitoring, Skype call analysis, counter cyber terrorism, darknet exploring, investigation of crimes related to the social media, Big Data analytics and cyber security of the digital infrastructure
- To train police personnel in advanced digital investigations besides social media monitoring and digital forensics
- Research and development wing of the cyberdome aims to take up futuristic and need-based IT projects for use in policing

The above are few of the examples of initiatives being carried out to tackle cybercrime. There are many more which state and central LEA's are conceptualizing as well as working towards implementation of the same.

Key differentiators

Sl. No.	Differentiators
1.	A cyber forensics lab deployed at national level to support cyber police and other state forensic labs.
2.	Schemes like I4C and CCPWC to develop police expertise and to address special segments vulnerable to cybercrimes.
3.	Research centers, trainings and Cyberdome developed to help police adapt latest technological changes in the cyberspace.
4.	Models like CCTNS and Predictive Policing to help police accelerate cybercrime investigation.
5.	Distinctive threat and malware analysis centers, botnet cleaning facilities to save citizens from already identified cyber malware and infections.

Sl. No.	Key innovations
1.	Usage of capabilities such as internet monitoring, voice call analysis, dark web analytical tools, integration of open source intelligence and big data analytics
2.	Malware analysis to demystify working of cyber threats
3.	AI tools trained by cybercrime data sets, providing analytical capability for crime investigations
4.	Fusion and integration of multiple set of data lakes for robust analytical scenarios
5.	Emergence in usage of next generation forensic tools for blockchain and IoT

47 https://www.telegraphindia.com/states/north-east/assam-cops-get-cyber-edge/cid/1454202



6 Way forward

With the increase in adaption of digital technologies across the country, be it individual, organizational and at the national level, it is fairly expected that all the records, documents, personal information will be available online, thus the evidence for any criminal activity would be found online for conducting investigations and analysis., The paradigm shift and challenges have the potential to hinder the investigation of LEAs and impede criminal proceedings and inhibit cybercrime management.

There is a need for participants from LEAs, academia and industry to collaborate to keep up the pace of the technological advancements, crime sophistications and coordination and also to ensure that international and national entities cooperate with each other. This thought leadership provides impetus to that there are number of challenges which needs to be addressed immediately and measures that need to be taken to progress towards successful closure of burning problems like encryption of communications, extraction of cloud data, data retention laws and illegal transactions in the dark markets, etc. Way forward in Indian context is captured below with emphasis only on the major thrust areas.



Short-term goals	Long-term goals
Expedited LEA modernization at central and state level leveraging emerging cyber technologies and building up integrated institutional cybercrime management infrastructure.	Charting out next generation technological strategy to be leveraged by central and state LEA functions. Understand emerging technologies like Blockchain, Cloud Models, IoT, Big Data, Analytics, AI and ML with respect to cybercrime management.
Formulation of a standard cybercrime taxonomy, which is to be followed by state and central LEAs, to homogenize the cybercrime management in the nation.	Setting up of central and state technology analytic units which would act as information technology functions for LEAs, enabling accelerated investigation and thwarting cybercrimes at national level.
A joint India-based taskforce may be formulated where police from all the member nations jointly address international issues pertaining to cybercrimes and India can derive the benefit from it. The end objective is to elevate India in the space of cybercrime management by collaborating with other countries.	Setting up of state and central centers of excellences (CoEs) equipping LEAs with investigative capabilities and aiding in continuous capacity building.
Cybercrime research and test beds to be built for investigations' experimentation, introducing LEAs to simulated crime scenarios for effective investigation and closure of cases.	Envisioning a national roadmap on cybercrime management with the help of pertinent stakeholders' consultation. Strengthening current institutions such as Ministry of Home Affairs, National Crime Record Bureau, Central Bureau of Investigation and state police functions with additional manpower and budgets.
A formal institutional framework to be built focusing on resolving challenges involving cybercrime threat intelligence sharing through collaboration between central and state police.	Setting up of cybercrime forensics laboratories in each state to address the challenge of delay in examination of case data.
Revisiting current law of the land such as the IT Act and IPC with respect to emerging use cases, crime and technology scenarios.	Conduct a nationwide campaign to enable the end citizens understand cybercrimes and sensitize them on the culture of reporting cybercrimes.
Constitute a focused task force to study dark web ecosystem and present its findings to central and state functions.	Setting up of cyber police cadre in the formal police recruitment system.

Management team

- **Gaurav Taneja**
  National Director - Government and Public Services
  Email: Gaurav.Taneja@in.ey.com

- **Rahul Rishi**
  Partner & Leader - Advisory Services, Government and Public Services
  Email: Rahul.Rishi@in.ey.com

- **Rohit Mathur**
  Risk Advisory Leader
  Email: Rohit.Mathur@in.ey.com

- **Murali Rao**
  India Cyber Leader
  Murali.Rao@in.ey.com

- **Vidur Gupta**
  Partner – Cyber Security
  Email: Vidur.Gupta@in.ey.com

- **Burgess Cooper**
  Partner – Cyber Security
  Email: Burgess.Cooper@in.ey.com

- **Jaspreet Singh**
  Partner – Cyber Security
  Email: Jaspreet.Singh@in.ey.com

- **Kartik Shinde**
  Partner – Cyber Security
  Email: Kartik.Shinde@in.ey.com

- **Mini Gupta**
  Partner – Cyber Security
  Email: Mini.Gupta@in.ey.com

- **Prashant Choudhary**
  Partner – Cyber Security
  Email: Prashant.Choudhary@in.ey.com

- **Tiffy Isaac**
  Partner – Cyber Security
  Email: Tiffy.Isaac@in.ey.com

- **Sambit Sinha**
  Partner – Cyber Security
  Email: Sambit.Sinha@in.ey.com

Contributors:

- **Pavan CJ**
- **Shantanu Rastogi**
- **Sarthak Kohli**
- **Prashant**
- **Aseem Mukhi**
- **Mayank Lau**
- **Sunil K Agarwal**
- **Hijaz Ali Shaik**

FICCI Homeland Security Department

FICCI has many specialised committees where key concerns of the industry are debated and discussed with the specific aim of presenting the recommendations to the Government for favourable decisions.

Considering internal security is the backbone of growth and overall development of the nation, FICCI has constituted a Committee on Homeland Security (HLS), which is working towards bridging the gap between policing and technology.

Some of the focus areas:

SMART Policing: FICCI has instituted the first ever SMART Policing Awards in India for best practices in SMART Policing, with the objective to promote initiatives taken by the Police for safety and security of Indian citizens. This can change public perception and build positive and progressive image of the police among people. FICCI SMART Policing Awards provide a platform to police officials across India to learn from the experiences of other states and also for possible adoption of the best practices to further enhance policing in their respective states.

Police Modernisation: FICCI is working towards bridging the gap between policing and technology. We engage with various enforcement agencies and provide them a platform to interact with industry, to articulate their requirements and to understand new technologies for security. This initiative is under our umbrella theme of "Modernisation of India's Internal Security Mechanism".

Smart Border Management: FICCI is working towards addressing the emerging challenges faced by India in smart border management, by bringing stakeholders together to discuss how India can create smart borders that, on the one hand, allow enhanced trans-border movement of peoples, goods and ideas, and on the other, minimise potential for cross-border security challenges.

Policy for Public Procurement in Internal Security: FICCI is working towards advocacy for bringing well-defined procedures for fair and transparent procurement of security products and solutions, so as to provide level playing field to the industry. Although the Central Armed Police Forces (CAPFs) and State Police Forces are guided by the same policies and guidelines for public procurement as other government organizations, the nature and requirements of public procurement process for police forces is different from that of the general government departments. FICCI has provided policy inputs to the Government of India for numerous challenges in regard to procurement by Internal Security forces, in the areas of policies and regulations, processes, technological advancements and capacity-building.

Cyber Crime Management: FICCI has initiated working towards promoting development and implementation, of systems and concepts to combat cyber-crime as well as improve cyber security.

Road Safety: United Nations has proclaimed 2011-20 as the Decade of Action on Road Safety. FICCI feels that the Indian Industry can play a significant role in addressing the issue of road safety.

Contact

Mr. Sumeet Gupta
Senior Director
sumeet.gupta@ficci.com

Mr. Ankit Gupta
Deputy Director – Homeland Security
ankit.gupta@ficci.com
+91-99900 89493

Ms. Sonali Hansda
Research Associate – Homeland Security
sonali.hansda@ficci.com
+91- 96543 87211

FICCI
Federation House, Tansen Marg, New Delhi 110 001
T: +91-11- 23487212, 23487474
www.ficci.com





Our offices

Ahmedabad
22nd Floor, B Wing, Privilon,
Ambli BRT Road, Behind Iskcon
Temple, Off SG Highway,
Ahmedabad - 380 015
Tel: + 91 79 6608 3800

Bengaluru
6th, 12th & 13th floor
"UB City", Canberra Block
No.24 Vittal Mallya Road
Bengaluru - 560 001
Tel: + 91 80 6727 5000

Ground Floor, 'A' wing
Divyasree Chambers
11, O'Shaughnessy Road
Langford Gardens
Bengaluru - 560 025
Tel: + 91 80 6727 5000

Chandigarh
1st Floor, SCO: 166-167
Sector 9-C, Madhya Marg
Chandigarh - 160 009
Tel: + 91 172 331 7800

Chennai
Tidel Park, 6th & 7th Floor
A Block, No.4, Rajiv Gandhi Salai
Taramani, Chennai - 600 113
Tel: + 91 44 6654 8100

Delhi NCR
Golf View Corporate Tower B
Sector 42, Sector Road
Gurgaon - 122 002
Tel: + 91 124 443 4000

3rd & 6th Floor, Worldmark-1
IGI Airport Hospitality District
Aerocity, New Delhi - 110 037
Tel: + 91 11 4731 8000

4th & 5th Floor, Plot No 2B
Tower 2, Sector 126
NOIDA - 201 304
Gautam Budh Nagar, U.P.
Tel: + 91 120 671 7000

Hyderabad
Oval Office, 18, iLabs Centre
Hitech City, Madhapur
Hyderabad - 500 081
Tel: + 91 40 6736 2000

Jamshedpur
1st Floor, Shantiniketan Building
Holding No. 1, SB Shop Area
Bistupur, Jamshedpur – 831 001
Tel: + 91 657 663 1000

Kochi
9th Floor, ABAD Nucleus
NH-49, Maradu PO
Kochi - 682 304
Tel: + 91 484 433 4000

Kolkata
22 Camac Street
3rd Floor, Block 'C'
Kolkata - 700 016
Tel: + 91 33 6615 3400

Mumbai
14th Floor, The Ruby
29 Senapati Bapat Marg
Dadar (W), Mumbai - 400 028
Tel: + 91 22 6192 0000

5th Floor, Block B-2
Nirlon Knowledge Park
Off. Western Express Highway
Goregaon (E)
Mumbai - 400 063
Tel: + 91 22 6192 0000

Pune
C-401, 4th floor
Panchshil Tech Park
Yerwada
(Near Don Bosco School)
Pune - 411 006
Tel: + 91 20 4912 6000

Ernst & Young LLP

EY | Assurance | Tax | Transactions | Advisory

About EY

EY is a global leader in assurance, tax, transaction and advisory services. The insights and quality services we deliver help build trust and confidence in the capital markets and in economies the world over. We develop outstanding leaders who team to deliver on our promises to all of our stakeholders. In so doing, we play a critical role in building a better working world for our people, for our clients and for our communities.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity. Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. For more information about our organization, please visit ey.com.

Ernst & Young LLP is one of the Indian client serving member firms of EYGM Limited. For more information about our organization, please visit www.ey.com/in.

Ernst & Young LLP is a Limited Liability Partnership, registered under the Limited Liability Partnership Act, 2008 in India, having its registered office at 22 Camac Street, 3rd Floor, Block C, Kolkata - 700016

© 2019 Ernst & Young LLP. Published in India.
All Rights Reserved.

EYIN1908-013
ED None

This publication contains information in summary form and is therefore intended for general guidance only. It is not intended to be a substitute for detailed research or the exercise of professional judgment. Neither Ernst & Young LLP nor any other member of the global Ernst & Young organization can accept any responsibility for loss occasioned to any person acting or refraining from action as a result of any material in this publication. On any specific matter, reference should be made to the appropriate advisor.

JG

About FICCI

Established in 1927, FICCI is the largest and oldest apex business organisation in India. Its history is closely interwoven with India's struggle for independence, its industrialisation, and its emergence as one of the most rapidly growing global economies.

A non-government, not-for-profit organisation, FICCI is the voice of India's business and industry. From influencing policy to encouraging debate, engaging with policy makers and civil society, FICCI articulates the views and concerns of industry. It serves its members from the Indian private and public corporate sectors and multinational companies, drawing its strength from diverse regional chambers of commerce and industry across states, reaching out to over 2,50,000 companies.

FICCI provides a platform for networking and consensus building within and across sectors and is the first port of call for Indian industry, policy makers and the international business community.

© Federation of Indian Chambers of Commerce and Industry (FICCI) 2019. All rights reserved.

The information in this publication has been obtained or derived from sources believed to be reliable. Though utmost care has been taken to present accurate information, FICCI makes no representation towards the completeness or correctness of the information contained herein. This document is for information purpose only.

This publication is not intended to be a substitute for professional, legal or technical advice. FICCI does not accept any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents

ey.com/in

@EY_India EY YouTube EY India EY Careers India ey_indiacareers