Disinformation is a cybersecurity threat

So far cybersecurity has mainly focused on protecting and defending computer systems, networks, and our digital lives from disruption.

The main focus of Cybersecurity has been to defend against cyberattacks executed using malware, viruses, trojans, botnets, and social engineering.

- There has been very little attention to the threat posed by disinformation attacks.
- Also, the industry has treated these attacks (cyberattacks and disinformation attack) independently and
- has separate teams working in silos to protect and defend against these attacks.
- The lack of coordination between teams leaves a huge gap that is exploited by malicious actors.

Disinformation:

- Disinformation attacks are the intentional dissemination of false information, with an end goal of misleading, confusing, or manipulating an audience.

- These attacks are commonly employed to reshape attitudes and beliefs, drive a particular agenda, or elicit certain actions out of a target audience.
- Nation-state actors, ideological believers, violent extremists, and economically motivated enterprises manipulate the information ecosystem to create social discord, increase polarisation, influence the outcome of an election, etc.
- Disinformation attacks can be employed through traditional media outlets such as TV channels or through social media.
- Disinformation attacks use manipulated, miscontextualised, misappropriated information, deep fakes, and cheap fakes.
- They pose the possibility of societal breakdown, business interruption, and violence in the streets.

Cognitive hacking:

- A cognitive hacking attack attempts to change the target audience's thoughts and actions, galvanise societies and disrupt harmony using disinformation.
- Disinformation is used for social engineering threats on a mass scale.

Examples of disinformation attacks and their impacts:

- QAnon spread false information about the U.S. 2020 presidential election. This led to rioting in the nation.
- Conspiracy theorists (in the United Kingdom, the Netherlands, Ireland, Cyprus and Belgium) burned down 5G towers because they believed it caused the novel coronavirus pandemic.
- COVID-19 disinformation campaigns have prevented people from wearing masks, using potentially dangerous alternative cures, and not getting vaccinated, making it even more challenging to contain the virus.

Factors aiding disinformation attacks:

- The advertisement-centric business modes and attention economy allow malicious actors to fill the information channels with disinformation with unprecedented speed and scale.
- Deep fakes add a whole new level of danger to disinformation campaigns.
- With the advent of social media, disinformation attacks have become increasingly widespread and

potent. Digital tools such as bots, algorithms, and AI technology are leveraged to spread and amplify disinformation and micro-target populations on online platforms like Instagram, Twitter, Facebook, and YouTube.

Way forward:

1. Recognizing disinformation as a cybersecurity threat:

- By treating disinformation as a cybersecurity threat we can find effective countermeasures to cognitive hacking.

2. Defense-in-depth:

- We need a defense-in-depth strategy for disinformation. The defense-in-depth model identifies disinformation actors and removes them. Authenticity solutions can intervene before disinformation gets posted online.
- If the disinformation still gets by, detection solutions using humans and artificial intelligence, internal and external fact-checking can label or remove the content.

3. Information sharing:

Patching the gaps in India's cybersecurity

Recently, the Union Power Ministry said that State-sponsored Chinese hacker groups targeted various Indian power centres.

- United States-based cybersecurity firm raised the possibility that the power outage in Mumbai could have been the result of an attack by a Chinese state-sponsored group.

Institutional security:

- In the last two decades, significant efforts have been made by India to craft institutional machinery focusing on cyber resilience spanning several government entities.
- The National Security Council, usually chaired by the National Security Adviser (NSA), plays a key role in shaping India's cyber policy ecosystem.
- The NSA also chairs the National Information Board, which is meant to be the apex body for cross-ministry coordination on cybersecurity policymaking.
- The National Critical Information Infrastructure Protection Centre established under the National

Technical Research Organisation in January 2014 was mandated to facilitate the protection of critical information infrastructure.

- In 2015, the Prime Minister established the office of the National Cyber Security Coordinator who advises the Prime Minister on strategic cybersecurity issues.
- India's Computer Emergency Response Team (CERT-In), which is the nodal entity responding to various cybersecurity threats to non-critical infrastructure comes under the (MEITY).
- The MoD has recently upgraded the Defence Information Assurance and Research Agency to establish the Defence Cyber Agency, a tri-service command of the Indian armed forces to coordinate and control joint cyber operations, and craft India's cyber doctrine.
- The MHA oversees multiple coordination centres that focus on law enforcement efforts to address cybercrime, espionage and terrorism.
- The MEA coordinates India's cyber diplomacy push, both bilaterally with other countries, and at international fora like the United Nations.

Problems in Institutional Framework:

- The institutional framework, while seeking to create an 'all of government' approach to countering and mitigating cybersecurity threats at the national level, has also resulted in concerns around:
    - Effective coordination
    - Overlapping responsibilities
    - Lack of clear institutional boundaries and accountability.

India has been a target earlier:

- India has been attacked by suspected Chinese state-sponsored groups multiple times in the past.
- In 2009, a suspected cyber espionage network dubbed GhostNet was found to be targeting the Tibetan government in exile in India, and many Indian embassies.
- The vast cyber-espionage operation extensively targeted Indian entities, including military establishments, news publications, and even the National Security Council Secretariat itself.

- There were a number of subsequent attacks that targeted India. Such as:
    - Stuxnet which had also taken down nuclear reactors in Iran.
    - Suckfly, which targeted not just government but also private entities including a firm that provided tech support to the National Stock Exchange.
    - Dtrack which first targeted Indian banks, and later the Kudankulam nuclear power plant (Tamil Nadu) in 2019.

Reports not made public:

- Neither the report from the Shadow Network investigation, nor any other, has ever been tabled in Parliament, nor even an edited version made public.

China's help in deconstructing the attacks:

- While there is much evidence to show that Chinese state-sponsored groups were responsible for many of these attacks, Chinese cybersecurity agencies have also helped the security community in dismantling the infrastructure behind some of these attacks.

False flag attacks:

- Documents released by WikiLeaks show that groups such as the Central Intelligence Agency's UMBRAGE project have advanced capabilities of misdirecting attribution to another nation-state ("false flag attacks").
- They leave behind false fingerprints for investigators to find.

Way Forward:

1.Making the reports public:

- Appraising lawmakers of the scale and depth of the damage wrought is critical to enabling meaningful public discussions and crafting a robust response.

2.Strengthening the Institutional Framework:

- Given that the question of attribution of a certain cyberattack is questionable, a robust institutional posture and political acumen in publicly dealing with these issues are necessary.

- There is a need for clarity about the institutional framework in India's National Cyber Security Strategy, which has been drafted by the NSC and is yet to be released.
- Ensuring coherence and coordination between these different actors should be its primary goal.

3.Doctrine on cyber conflicts:

- India is also yet to clearly articulate a doctrine that holistically captures its approach to cyber conflict. That is, for conducting offensive cyber operations, or the extent and scope of countermeasures against cyber-attacks.
- Unlike India's approach to other global security regimes like the 'No First Use' nuclear posture, the rules of engagement for targeted cyber-attacks are unclear.
- While it might seem like secrecy and ambiguity would provide a tactical advantage when engaging in cyber operations, in an increasingly unstable geopolitical scenario, the absence of a credible cyber deterrence strategy is undesirable.
    - In such a scenario, states and non-state actors alike remain incentivised to undertake low-

scale cyber operations for a variety of purposes – espionage, cyber-crime, and even the disruption of critical information infrastructure.

4. Define the red lines:

- India has been an active participant in processes within the First Committee of the UNGA dealing with issues of disarmament and international security.
- While the Indian delegation has made public some of their intervention, India's long-term strategic thinking on core issues of debate at these fora remains relatively unknown.
- India must involve itself in a precise articulation of how international law applies to cyberspace.
- This could mould the global governance debate to further India's strategic interests and capabilities.

* The world is hardly wired for cyber resilience

- Cyber attacks in the US
  - 2020 – 'Solar Winds' cyberattack
    - believed to be Russian sponspored
    - Data breaches in several US Govt deptts
  - 2021 – Cyber attack by a Chinese group 'Hafnium'
    - exploited serious flaws in Microsoft's software ⇒ gained control over systems.
  - 3 more attacks in 2021 in the US
    - ↳ Ransomware attack on Colonial Pipeline (main supplier of oil to US East Coast)
    - ↳ Phishing attack on 3000 e-mail accounts, targeting US-AID etc by another Russian backed group Nobellium.
    - ↳ Ransomware attack on a meat processing company (paid millions in ransom)
- Cyber warfare ⇒ 5th domain of warfare
  - ↳ earlier was limited to military & strategic targets
  - ↳ but now even civilian targets.

- Zero day Vulnerabilities
  - ↳ cyber attacks capable of crippling an entire system & could lie undetected for a long time
  - ↳ Eg: Stuxnet → almost crippled Iran's Uranium enrichment programme.
  - ↳ Govts are busy erecting defences against such Zero day attacks.
  - ↳ While the civilian world is left to fend for itself.
    Eg: Shamoon virus attack on Saudi Aramco
    ↓
    Wiped out memories of 30K computers
- Types of cyber attack in civilian domain -

- Ransomware
  - ↳ A user or organization's critical data is encrypted so that they cannot access files, databases, or applications
  - ↳ A ransom is then demanded to provide access.
  - ↳ Recovery costs in India has tripled.
  - ↳ Catastrophic situation for mid size companies
  - ↳ Banking & finance ⇒ most prone to attacks
  - ↳ Also oil, electricity grids & lately healthcare

- Phishing (incl. spear phishing)
  - ↳ Targets are contacted by email, phone or text messages by someone posing as a legitimate institution to lure individuals into providing sensitive data.
  - ↳ can result in identity theft & financial loss.
  - ↳ Spear phishing is targeted & personalised to a specific individual, group or institution

— Healthcare

↳ Recent phenomena of cyber attacks in this sector

↳ Health information being used by criminals as a commodity for trade.

↳ Patient's data leaks creates risk for not just the individual but entire communities

— Motives behind cyber attacks -

- Geopolitical transformation → nation-states
- Profit seeking → (cyber criminals & terrorists)
- Insider threats → discontentment with management

— Need for data protection —

- Zero Trust based Environment
  - ↳ i.e. zero trust on end point devices,

identity & network to protect all sensitive data

- Software designed solutions
  ↳ perimeter security, secure gateways, cloud access security etc
- Threat intelligence platforme
- Using machine learning, AI & quantum computing
- Regular vulnerability assessments for public officials & company boards.

- Conclusion
  ↳ Value lies in the data and people are going to come after that data.

* Ransomware to dominate cybercrime landscape

- Latest ransomware operators of concern
  - Ransomware Evil, REvil or Sodinokibi, a ransomware-as-a-service (RaaS) operation
- Ransomware:
  - Ransomware is malware that employs encryption to hold a victim's info at ransom.
  - A user or organization's critical data is encrypted so that they cannot access it.
  - A ransom is then demanded to provide access.
  - Ransomware uses asymmetric encryption.
  - It uses a pair of keys to encrypt and decrypt a file.
- REvil Platform
  - Provides adaptable encryptors and decryptors, infra and services for negotiation .
  - Also provides a leak site for publishing stolen data when victims don't pay.

- REvil and its affiliates have pulled in a payment of $2.25 million during the first six months of 2021

– Ransomware situation globally

- Cyber experts warn that ransomware is going to be the major cybercrime
- High growth in data created in 2020. This data is vulnerable to ransomware attacks.
- Healthcare -> most targeted and vulnerable sector in 2020
- More sophisticated and complex Cyberthreats Attackers use real-world events to deceive victims.

– Fighting ransomware:

1. Use of deep technology to counter cyber threats. Integrated platform using ML and AI
2. Quantum computing to hasten the computing speed

Taking a byte out of cyber threats

What are Cyberthreats?

- It is a malicious act that includes threats like computer viruses, data breaches, and Denial of Service (DoS) attacks.
- A cyber threat damages data, steals data, or disrupts digital life in general.

Global Examples of Cyber Attacks:

- The advent of the Stuxnet Worm in 2010 resulted in large-scale damage to Iran's centrifuge capabilities.
- In 2012, data from Saudi Aramco Oil Company computers were wiped out by Iranian operatives by employing malware.
- Ransomware attack on Colonial Pipeline in 2021 was the largest cyberattack on an oil infra.

Indian Examples of Cyber Attacks:

- The data from an exam for the recruitment of police officers in 2019 in India was hacked which resulted in a leak of sensitive information of all the participants.

- In 2021, a huge leak of customer data was experienced by the famous pizza brand namely, Dominos, India.
- In 2021, the records of over 10 crore users were leaked from India-based digital payment company MobiKwik.

Concerns with Emerging Cyber Threats:

- Wide Coverage: Cyber threat is likely to be among concerns for both companies and govts across the globe.
- Targeted Sectors: Among the most targeted sectors in the coming period are likely to be: health care, education and research, communications and govts.
- Health-care ransomware: The ransomware attacks have led to longer stays in hospitals, apart from delays in procedures and tests, resulting in an increase in patient mortality.
- Ransomware as a Service (RaaS): Emergence of 'Ransomware as a Service' (RaaS) — a business

model for ransomware developers — is no mere idle threat.

- Work From Home: The huge security impact of working from home is likely to further accelerate the pace of cyberattacks.
- Cloud Storage: A tendency seen more recently to put everything on the Cloud could backfire, causing many security holes, challenges, misconfigurations and outages.
- Dark Web: The dark web is vulnerable to abuse by malicious actors as part of cyber threats.
- Lack of Implementation: Many companies fail to realize that inadequate corporate protection and defense could have huge external costs for national security.

Way Forward:

- Every enterprise should incorporate Secure Access Service Edge (SASE) to reduce the risk of cyberattacks.

- Cloud Access Security Broker (CASB) and Secure Web Gateway (SWG) – aimed at limiting the risks to users from web-based threats.
- The Zero Trust Model and Micro Segmentation as a means to limit cyberattacks can again be self-limiting.
- Nations & institutions should actively prepare for cyberattacks by prioritizing the defense of data.
- The law enforcement agencies would need to play a vital role in providing an effective defense against cyber attacks.
- Need to prioritize resilience through decentralized and dense networks, hybrid cloud structures, redundant applications and backup processes.
- Need to prioritize building trust in systems and creating backup plans including strategic decisions about what should be online or digital and what needs to stay analogue or physical.

The status of India's National Cyber Security Strategy

The Data Security Council of India (DSCI) has prepared a report focussing on different areas to ensure a safe and vibrant cyberspace for India.

Need of a cybersecurity strategy for India:

- As per American cybersecurity firm Palo Alto Networks' 2021 report,
    - India is among the more economically profitable regions for hacker groups.
    - Maharashtra faces 42% of all ransomware attacks.
    - One in four Indian organizations suffered a ransomware attack in 2021.
    - Indian organizations witnessed a 218% increase in ransomware.
- Increase in such attacks has brought to light the urgent need for strengthening cybersecurity.

National Cyber Security Strategy

- Conceptualized by the DSCI.
- It focuses on 21 areas.

The main sectors of focus of the report are:-

1.Large scale digitisation of public services:

- Security in the early stages of design in all digitisation initiatives
- Developing institutional capability for assessment, evaluation, certification & rating of core devices.

2.Supply chain security:

- Robust monitoring and mapping of the supply chain
- Product testing and certification.

3.Critical information infrastructure protection:

- Integrate supervisory control and data acquisition (SCADA) security with enterprise security.
- Maintain a repository of vulnerabilities.

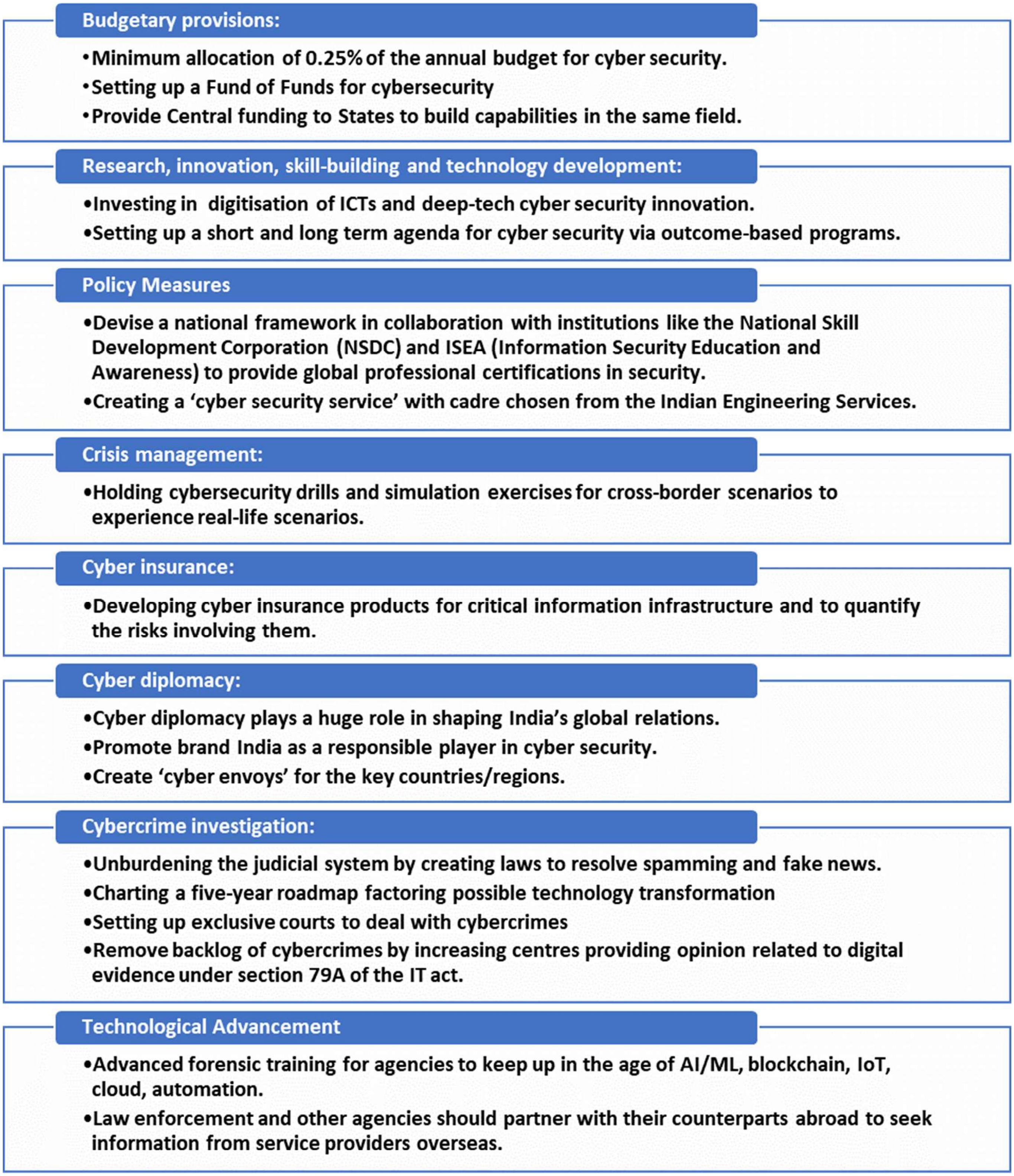
4.Digital payments:

- Mapping and modeling of devices and platforms.
- Threat research and sharing of threat intel.

5.State-level cyber security:

- Develop State-level cybersecurity policies and guidelines for security architecture & governance.

Recommendations by the DSCI Report:



Budgetary provisions:

- Minimum allocation of 0.25% of the annual budget for cyber security.
- Setting up a Fund of Funds for cybersecurity
- Provide Central funding to States to build capabilities in the same field.

Research, innovation, skill-building and technology development:

- Investing in digitisation of ICTs and deep-tech cyber security innovation.
- Setting up a short and long term agenda for cyber security via outcome-based programs.

Policy Measures

- Devise a national framework in collaboration with institutions like the National Skill Development Corporation (NSDC) and ISEA (Information Security Education and Awareness) to provide global professional certifications in security.
- Creating a ‘cyber security service’ with cadre chosen from the Indian Engineering Services.

Crisis management:

- Holding cybersecurity drills and simulation exercises for cross-border scenarios to experience real-life scenarios.

Cyber insurance:

- Developing cyber insurance products for critical information infrastructure and to quantify the risks involving them.

Cyber diplomacy:

- Cyber diplomacy plays a huge role in shaping India’s global relations.
- Promote brand India as a responsible player in cyber security.
- Create ‘cyber envoys’ for the key countries/regions.

Cybercrime investigation:

- Unburdening the judicial system by creating laws to resolve spamming and fake news.
- Charting a five-year roadmap factoring possible technology transformation
- Setting up exclusive courts to deal with cybercrimes
- Remove backlog of cybercrimes by increasing centres providing opinion related to digital evidence under section 79A of the IT act.

Technological Advancement

- Advanced forensic training for agencies to keep up in the age of AI/ML, blockchain, IoT, cloud, automation.
- Law enforcement and other agencies should partner with their counterparts abroad to seek information from service providers overseas.

India's cyber infrastructure

NCRB has released its report 'Crime In India 2021' on cybercrime.

About Cybercrime

- Cybercrime: Any offences committed against individuals or groups of individuals to harm their reputation or cause physical or mental trauma through electronic means.
- In India, cybercrime is increasing with the increased use of information and communication technology (ICT).
- Internationally, both governmental and non-state actors engage in cybercrimes, including espionage, financial theft, and other cross-border crimes.
- Cyberwarfare: Cybercrimes crossing international borders and involving the actions of at least one nation-state are sometimes referred to as.

Findings of the report:

- Steady spike in cases of cybercrime in the last 05 years

12,317 cases in 2016	50,035 cases in 2020

- Over 70% of the cases were reported from Telangana, UP, Karnataka, Maharashtra and Assam.
- Avg. rate of cybercrime incidents is 3.9/lakh population.
    - Highest in Telangana at 27/lakh followed by Assam at 13.8/lakh population.

- Major motives behind these crimes: Fraud in 60.8% of cases, sexual exploitation in 8.6% of cases and extortion in 5.4% of cases.
- Total of 15 cases of 'cyber terrorism' were lodged across the country in 2021.

Addressing the shortfall in cyberinfrastructure:

- Despite the steady spike in cybercrime cases, the capacity of the enforcement agencies to investigate cybercrime remains limited.
- There is no separate procedural code for the investigation of cyber-related offences.
- It is necessary to have a distinct code for electronic evidence as they are different in nature compared to traditional crimes.
    - Guidelines issued by the BIS for the identification, collection, acquisition and preservation of digital evidence must be followed properly to ensure proper handling of digital evidence.
- Shortage of technical staff for the investigation of cybercrime.
    - A regular police officer can only act as a first responder who could identify digital evidence and secure the scene of the crime or preserve digital evidence.
    - It is only a technically qualified staff who could acquire and analyse digital evidence.
    - Information Technology (IT) Act, 2000 insists that offences registered under the Act should

be investigated by a police officer, not below the rank of an inspector.

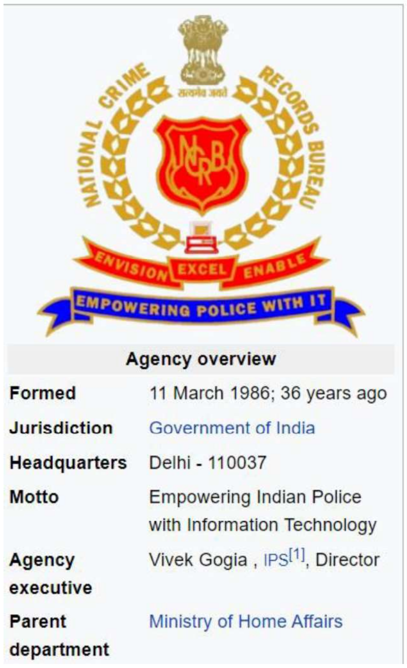
- Cyber forensic laboratories of States must be upgraded with new technologies to augment the capacity to solve cybercrimes.
    - Centre shall focus on upgrading the State laboratories by providing modernisation funds.
    - States should get their cyber labs notified as 'Examiner of Electronic Evidence' by the union govt. to enable them to provide expert opinions on electronic records.
- 'Data localisation' provisions for all kinds of data shall be included in the proposed Personal Data Protection law to empower enforcement agencies for timely access to the data of suspected Indian citizens.
    - Most cyber crimes are transnational in nature with extra-territorial jurisdiction.
    - Collection of evidence from foreign territories is difficult and time-consuming.
- India must develop its own agency to identify and remove online Child Sexual Abuse Material (CSAM).
- Indian police still get reports on online CSAM from a non-profit agency in the U.S.

Recommendations

- Create the necessary cyberinfrastructure lies with States as 'police' and 'public order' come under State List.

- Legislation such as the IT Act puts further responsibility on the central govt. to evolve uniform statutory procedures for the enforcement agencies.

NCRB



Agency overview	
Formed	11 March 1986; 36 years ago
Jurisdiction	Government of India
Headquarters	Delhi - 110037
Motto	Empowering Indian Police with Information Technology
Agency executive	Vivek Gogia , IPS[1], Director
Parent department	Ministry of Home Affairs

Mission

To Empower Indian Police with Information Technology and criminal Intelligence to enable them to uphold law and protect people. To provide leadership and excellence in crime analysis particularly for serious and organized crime.

Objectives

- Create and maintain **secure sharable National Databases** on crimes and criminals for law enforcement agencies and promote their use for **public service delivery.**
- Collect and process crime statistics at the national level and clearing house of information on crime and criminals both at National and International levels.

- Lead and coordinate development of IT applications and create an enabling IT environment for Police organizations.
- National repository of fingerprints of all criminals.
- To evaluate, modernize and promote automation in State Crime Records Bureau and State Finger Print Bureau.
- Training and capacity building in Police Forces in Information Technology and Finger Print Science.