

**GOVERNMENT OF INDIA  
MINISTRY OF HOME AFFAIRS**

**RAJYA SABHA  
UNSTARRED QUESTION NO. 398**

**TO BE ANSWERED ON THE 22<sup>ND</sup> JULY, 2026/ ASHADHA 31, 1948 (SAKA)**

**RISING CYBERCRIME AND CROSS-BORDER DIGITAL THREATS**

**398      SHRI AKHILESH PRASAD SINGH:**

**Will the Minister of HOME AFFAIRS be pleased to state:**

- (a) whether Government has undertaken a comprehensive assessment of the increasing incidence of cyber frauds, ransomware attacks and cross-border cyber threats affecting citizens, financial institutions and critical infrastructure;**
- (b) whether a coordinated national mechanism exists for real-time information sharing among Central agencies, States and financial regulators;**
- (c) the measures taken to strengthen digital forensic capabilities and cybercrime investigation across the country; and**
- (d) whether Government proposes to introduce additional safeguards to counter emerging cyber threats powered by Artificial Intelligence?**

**ANSWER**

**MINISTER OF STATE IN THE MINISTRY OF HOME AFFAIRS  
(SHRI BANDI SANJAY KUMAR)**

**(a) to (d) : The National Crime Records Bureau (NCRB) compiles and publishes the statistical data on crimes in its publication “Crime in India”. The latest published report is for the year 2024. As per the data published by the NCRB, Crime Head-wise cases registered under cyber Crimes (involving communication devices as medium/target) during the period from 2022 to 2024 is at Annexure-I.**

**‘Police’ and ‘Public Order’ are State subjects under the Seventh Schedule to the Constitution of India. Accordingly, the States and Union Territories (UTs) are primarily responsible for the prevention, detection, investigation, and prosecution of cybercrime. The Central Government, through the Ministry of Home Affairs (MHA), supplements the efforts of States and UTs by providing policy guidance, technological support, capacity-building assistance, and financial resources to strengthen cybercrime management and enforcement capabilities.**

**To strengthen the coordinated mechanism, digital forensic capabilities and to counter emerging cyber threats in a comprehensive and coordinated manner, the Central Government has taken steps which, inter-alia, include the following:**

- i. The Ministry of Home Affairs has set up the ‘Indian Cyber Crime Coordination Centre’ (I4C) as an attached office to deal with all types of cyber crimes in the country, in a coordinated and comprehensive manner.**
- ii. The ‘National Cyber Crime Reporting Portal’ (NCRP) (<https://cybercrime.gov.in>) has been launched, as a part of the I4C, to enable public to report incidents pertaining to all types of cyber crimes, with special focus on cyber crimes against women and children. Cyber crime incidents reported on this portal, their conversion into FIRs and**

**subsequent action thereon are handled by the State/UT Law Enforcement Agencies concerned as per the provisions of the law.**

- iii. The 'Citizen Financial Cyber Fraud Reporting and Management System' (CFCFRMS), under I4C, has been launched in year 2021 for immediate reporting of financial frauds and to stop siphoning off funds by the fraudsters. As per CFCFRMS operated by I4C, till 30.06.2026, financial amount of more than Rs. 11,158 Crore has been saved in more than 32.80 lakh complaints. A toll-free Helpline number '1930' has been operationalized to get assistance in lodging online cyber complaints.**
- iv. A State of the Art, Cyber Fraud Mitigation Centre (CFMC) has been established at I4C where representatives of major banks, Financial Intermediaries, Payment Aggregators, Telecom Service Providers, IT Intermediaries and representatives of States/UTs Law Enforcement Agency are working together for immediate action and seamless cooperation to tackle cybercrime.**
- v. Samanvaya Platform has been made operational to serve as an Management Information System (MIS) platform, data repository and a coordination platform for LEAs for cybercrime data sharing and analytics. It provides analytics based interstate linkages of crimes and criminals, involved in cybercrime complaints in various States/UTs. The module 'Pratibimb' maps locations of criminals and crime infrastructure on a map**

**to give visibility to jurisdictional officers. The module also facilitates seeking and receiving of techno-legal assistance by Law Enforcement Agencies from I4C and other SMEs. It has lead to arrest of more than 29,837 accused and more than 2,33,593 Cyber Investigation assistance request.**

- vi. 'Sahyog' Portal has been launched to expedite the process of sending notices to IT intermediaries by the Appropriate Government or its agency under clause (b) of sub-section (3) of section 79 of the IT Act, 2000 to facilitate the removal or disabling of access to any information, data or communication link being used to commit an unlawful act.**
- vii. A Suspect Registry of identifiers of cyber criminals has been launched by I4C on 10.09.2024 in collaboration with Banks/Financial Institutions. Till 30.06.2026, more than 30.48 lakh suspect identifier data received from Banks and 32.08 lakh Layer 1 mule accounts have been shared with the participating entities of Suspect Registry and declined transactions worth Rs. 25,698 crores.**
- viii. Seven Joint Cyber Coordination Teams (JCCTs) have been constituted for Mewat, Jamtara, Ahmedabad, Hyderabad, Chandigarh, Vishakhapatnam, and Guwahati under I4C covering the whole country based upon cyber crime hotspots/ areas having multi jurisdictional issues by onboarding States/UTs to enhance the coordination framework among the Law Enforcement Agencies of the States/UTs.**

- ix. **I4C, MHA is regularly organising ‘State Connect’, ‘Thana Connect’ and ‘Peer learning session’ to share best practices, enhance capacity building, etc.**
- x. **The state of the art National-Digital Investigation Support Centre (previously known as National Cyber Forensic Laboratory (Investigation) {NCFL(I)}) has been established, as a part of the I4C, at New Delhi (on 18.02.2019) and at Assam (on 29.08.2025) to provide early stage cyber forensic assistance to Investigating Officers (IOs) of State/UT Police. Till 30.06.2026, National-Digital Investigation Support Centre, New Delhi has provided its services to State/UT LEAs in more than 14,064 cases pertaining to cyber crimes.**
- xi. **The Ministry of Home Affairs has released financial assistance to the tune of Rs. 132.93 crores under the ‘Cyber Crime Prevention against Women and Children (CCPWC)’ Scheme, to the States/UTs for their capacity building such as setting up of cyber forensic-cum-training laboratories, hiring of junior cyber consultants and training of LEAs’ personnel, public prosecutors and judicial officers. Cyber forensic-cum-training laboratories have been commissioned in 33 States/UTs and more than 24,600 LEAs’ personnel, judicial officers and prosecutors have been provided training on cyber crime awareness, investigation, forensics etc.**
- xii. **At present, 07 Central Forensic Science Laboratories and 28 State Forensic Science Laboratories are operational across the country to**

**assist in investigation of cybercrime cases. Assistance has been provided to 20 States / UTs for strengthening of cyber forensic capacities in State FSLs under the Nirbhaya funded scheme for strengthening of DNA Analysis and cyber forensic capacities in State FSLs.**

- xiii. The Ministry of Home Affairs has established CyMAC (Cyber Multi Agency Centre) under the MAC (Multi Agency Centre) platform on 22.01.2025 with the objective to effectively address cybersecurity threats, cyber espionage, misuse of emerging technologies and similar concerns against national security.**
- xiv. CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.**
- xv. National Cyber Coordination Centre (NCCC) implemented by CERT-In, examines the cyberspace to detect cyber security threats. It shares the information with concerned State Governments, organisations across sectors, and stakeholder agencies for taking action.**
- xvi. CERT-In operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with State Governments and organisations across sectors for proactive threat mitigation actions by them.**

- xvii. Cyber Swachhta Kendra (CSK) is a service provided by CERT-In, which extends the vision of Swachh Bharat to the cyber space. Cyber Swachhta Kendra helps to detect malicious programs and vulnerable services and provide remedial measures to organisations across States and sectors.**
- xviii. Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government (Central & States) and critical sectors. Workshops along with these drills are conducted in States for facilitating coordination and information sharing in the area of cyber security.**

\*\*\*\*\*

**Crime Heads-wise Cases Registered under Cyber Crimes during 2022-2024**

| SL       | Crime Head                                                                                                       | 2022         | 2023         | 2024          |
|----------|------------------------------------------------------------------------------------------------------------------|--------------|--------------|---------------|
| 1        | Tampering computer source documents                                                                              | 65           | 71           | 162           |
| 2        | Computer Related Offences                                                                                        | 23894        | 35329        | 36920         |
| 3        | Cyber Terrorism                                                                                                  | 12           | 11           | 18            |
| 4        | Publication/transmission of obscene / sexually explicit act in electronic form                                   | 6896         | 7893         | 6990          |
| 5        | Interception or Monitoring or decryption of Information                                                          | 1            | 1            | 4             |
| 6        | Un-authorized access/attempt to access to protected computer system                                              | 1            | 1            | 2             |
| 7        | Breach of Confidentiality & Privacy                                                                              | -            | -            | 37            |
| 8        | Publication of Electronic Signatures for fraudulent purposes                                                     | -            | -            | 5             |
| 9        | Abetment to Commit Offences                                                                                      | 4            | 0            | 2             |
| 10       | Attempt to Commit Offences                                                                                       | 18           | 11           | 14            |
| 11       | Other Sections of IT Act                                                                                         | 1017         | 920          | 718           |
| <b>A</b> | <b>Total Offences under I.T. Act</b>                                                                             | <b>31908</b> | <b>44237</b> | <b>44872</b>  |
| 12       | Abetment of Suicide (Online)                                                                                     | 24           | 30           | 12            |
| 13       | Cyber Stalking/Bullying of Women/Children                                                                        | 1471         | 1305         | 1240          |
| 14       | Sexual Intercourse by Deceitful Means                                                                            | -            | -            | 99            |
| 15       | Organized Cyber Crimes                                                                                           | -            | -            | 60            |
| 16       | Publishing false or misleading information jeopardizing the Sovereignty Unity and integrity or security of India | -            | -            | 2             |
| 17       | Data theft                                                                                                       | 97           | 113          | 88            |
| 18       | Fraud                                                                                                            | 17470        | 19466        | 29758         |
| 19       | Cheating                                                                                                         | 10509        | 16943        | 19296         |
| 20       | Forgery                                                                                                          | 224          | 444          | 702           |
| 21       | Defamation/Morphing                                                                                              | 61           | 36           | 28            |
| 22       | Fake Profile                                                                                                     | 157          | 225          | 266           |
| 23       | Counterfeiting                                                                                                   | 2            | 0            | 3             |
| 24       | Cyber Blackmailing/Threatening                                                                                   | 696          | 689          | 601           |
| 25       | Fake News on Social Media                                                                                        | 230          | 209          | 483           |
| 26       | Other Offences                                                                                                   | 2857         | 2389         | 4109          |
| <b>B</b> | <b>Total Offences under IPC/BNS</b>                                                                              | <b>33798</b> | <b>41849</b> | <b>56747</b>  |
| 27       | Gambling Act (Online Gambling)                                                                                   | 37           | 87           | 37            |
| 28       | Lotteries Act (Online Lotteries)                                                                                 | 6            | 0            | 0             |
| 29       | Copy Right Act                                                                                                   | 27           | 23           | 30            |
| 30       | Trade Marks Act                                                                                                  | 14           | 1            | 6             |
| 31       | Other SLL Crimes                                                                                                 | 103          | 223          | 236           |
| <b>C</b> | <b>Total Offences under SLL</b>                                                                                  | <b>187</b>   | <b>334</b>   | <b>309</b>    |
|          | <b>Total Cyber Crimes (A+B+C)</b>                                                                                | <b>65893</b> | <b>86420</b> | <b>101928</b> |

Source: 'Crime in India' published by NCRB.

\*\*\*\*\*