भारत सरकार
गृह मंत्रालय
राज्य सभा
अतारांकित प्रश्न संख्या 2800
दिनांक 12 अगस्त, 2026 / 21 श्रावण, 1948 (शक) को उत्तर के लिए

कृत्रिम बुद्धिमत्ता (एआई) आधारित साइबर अपराध निवारण तथा डिजिटल पहचान का संरक्षण

2800 श्री विनोद श्रीधर तावड़े:

क्या गृह मंत्री यह बताने की कृपा करेंगे कि:

(क) कृत्रिम बुद्धिमत्ता (एआई) आधारित साइबर अपराधों की रोकथाम तथा नागरिकों की डिजिटल पहचान की सुरक्षा के लिए कौन-कौन सी प्रमुख पहलें की गई हैं;
(ख) भारतीय साइबर अपराध समन्वय केंद्र (आई4सी) द्वारा जन-जागरूकता, शिकायत दर्ज करने के तंत्रों तथा संस्थागत क्षमता को सुदृढ़ करने के लिए क्या-क्या उपाय किए गए हैं;

(ग) क्या ऐसे अपराधों से निपटने के लिए कानून प्रवर्तन एजेंसियों, वित्तीय संस्थाओं तथा डिजिटल सेवा प्रदाताओं के बीच समन्वित कार्रवाई हेतु कोई ढांचा विकसित किया गया है; और

(घ) साइबर प्रत्यास्थता को सुदृढ़ करने तथा उभरती प्रौद्योगिकियों के सुरक्षित उपयोग को बढ़ावा देने के लिए और कौन-कौन से कदम प्रस्तावित हैं?

उत्तर

गृह मंत्रालय में राज्य मंत्री
(श्री बंडी संजय कुमार)

(क) से (घ): 'पुलिस' और 'लोक व्यवस्था' भारत के संविधान की सातवीं अनुसूची के अनुसार राज्य के विषय हैं। तदनुसार, राज्य और संघ राज्य क्षेत्र साइबर अपराध की रोकथाम, उनका पता लगाने, जांच और अभियोजन के लिए मुख्य रूप से जिम्मेदार हैं। केंद्र सरकार, गृह मंत्रालय के माध्यम से, साइबर अपराध प्रबंधन और प्रवर्तन क्षमताओं को मजबूत करने के लिए नीतिगत मार्गदर्शन, तकनीकी सहायता, क्षमता निर्माण संबंधी सहायता और वित्तीय संसाधन प्रदान करके राज्यों और संघ राज्य क्षेत्रों के प्रयासों में सहायता करती है।

राज्य सभा अतारांकित प्रश्न सं. 2800, दिनांक 12.08.2026

केंद्र सरकार ने एआई-सक्षम साइबर अपराधों सहित साइबर अपराधों से व्यापक और समन्वित ढंग से निपटने तथा साइबर प्रतिरोध क्षमता को सुदृढ़ करने हेतु तंत्र को सुदृढ़ बनाने के लिए निम्नलिखित कदम उठाए हैं:

i. गृह मंत्रालय ने देश में सभी प्रकार के साइबर अपराधों से समन्वित और व्यापक ढंग से निपटने के लिए एक संबद्ध कार्यालय के रूप में 'भारतीय साइबर अपराध समन्वय केंद्र' (आई4सी) स्थापित किया है।

ii. महिलाओं और बच्चों के प्रति साइबर अपराधों पर विशेष बल देते हुए, सभी प्रकार के साइबर अपराधों से संबंधित घटनाओं की सूचना देने में जनता को समर्थ बनाने हेतु आई4सी के भाग के रूप में 'राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल' (एनसीआरपी) (https://cybercrime.gov.in) शुरू किया गया है।

iii. वित्तीय धोखाधड़ियों की तत्काल सूचना देने और धोखाधड़ी करने वालों के द्वारा निधियों की चोरी को रोकने के लिए वर्ष 2021 में आई4सी के तहत 'नागरिक वित्तीय साइबर धोखाधड़ी रिपोर्टिंग और प्रबंधन प्रणाली' (सीएफसीएफआरएमएस) शुरू की गई है। आई4सी द्वारा संचालित सीएफसीएफआरएमएस के अनुसार, दिनांक 30.06.2026 तक, 32.80 लाख से अधिक शिकायतों में 11,158 करोड़ रुपये से अधिक की राशि को बचाया गया है। साइबर शिकायतों को ऑनलाइन दर्ज करने में सहायता प्राप्त करने के लिए एक टोल-फ्री हेल्पलाइन नम्बर '1930' शुरू किया गया है।

iv. साइबर अपराध की जांच, फॉरेंसिक, अभियोजन आदि के महत्वपूर्ण पहलुओं पर ऑनलाइन पाठ्यक्रम के माध्यम से पुलिस अधिकारियों/न्यायिक अधिकारियों के क्षमता निर्माण हेतु आई4सी के तहत 'साइट्रेन' पोर्टल नामक "वृहत ओपन ऑनलाइन कोर्स (एमओओसी)" प्लेटफॉर्म विकसित किया गया है। दिनांक 30.06.2026 तक, इस पोर्टल के माध्यम से राज्यों/संघ राज्य-क्षेत्रों के 1,63,344 से अधिक पुलिस अधिकारियों/न्यायिक अधिकारियों का पंजीकरण किया गया है और 1,61,957 से अधिक प्रमाण-पत्र जारी किए गए हैं।

v. देश में साइबर सुरक्षा खतरों का मुकाबला करने के लिए विशेष प्रशिक्षण से लैस साइबर कमांडो की एक विशेष शाखा स्थापित करने के लिए माननीय गृह मंत्री द्वारा साइबर कमांडो कार्यक्रम शुरू किया गया था। इस कार्यक्रम का उद्देश्य एक समर्पित, कुशल कार्यबल का सृजन करना है जो महत्वपूर्ण सूचना अवसंरचना को सुरक्षित रखने तथा राष्ट्रीय साइबर सुरक्षा प्रयासों को समर्थन देने में सक्षम हो। 281 साइबर कमांडो ने सफलतापूर्वक प्रशिक्षण पूरा कर लिया है।

vi. आई4सी, गृह मंत्रालय सर्वोत्तम प्रथाओं को साझा करने, क्षमता निर्माण को बढ़ाने आदि के लिए नियमित रूप से 'स्टेट कनेक्ट', 'थाना कनेक्ट' , 'बैंक कनेक्ट' और सहकर्मी शिक्षण सत्र आयोजित कर रहा है।

राज्य सभा अतारांकित प्रश्न सं. 2800, दिनांक 12.08.2026

vii. आई4सी में एक अत्याधुनिक साइबर धोखाधड़ी शमन केंद्र (सीएफएमसी) स्थापित किया गया है, जहां प्रमुख बैंकों, वित्तीय मध्यस्थों, भुगतान एग्रीगेटर्स, दूरसंचार सेवा प्रदाताओं, आईटी मध्यस्थों के प्रतिनिधि और राज्यों/संघ राज्य क्षेत्रों की विधि प्रवर्तन एजेंसियों के प्रतिनिधि साइबर अपराध से निपटने के लिए तत्काल कार्रवाई और निर्बाध सहयोग के लिए साथ मिलकर काम कर रहे हैं।

viii. आई4सी के तहत मेवात, जामताड़ा, अहमदाबाद, हैदराबाद, चंडीगढ़, विशाखापट्टनम और गुवाहाटी के लिए सात संयुक्त साइबर समन्वय टीमों (जेसीसीटी) का गठन किया गया है, जो राज्यों/संघ राज्य क्षेत्रों की विधि प्रवर्तन एजेंसियों के बीच समन्वय ढांचे को बढ़ाने के लिए राज्यों/संघ राज्य क्षेत्रों को शामिल करते हुए बहु-न्यायिक मुद्दों वाले साइबर अपराध हॉटस्पॉट/क्षेत्रों के आधार पर पूरे देश को कवर करती हैं।

ix. बैंकों/वित्तीय संस्थाओं के सहयोग से आई4सी द्वारा साइबर अपराधियों की पहचान की एक संदिग्ध रजिस्ट्री शुरू की गई है। दिनांक 30.06.2026 तक, बैंकों से प्राप्त 30.48 लाख से अधिक संदिग्ध पहचानकर्ता डेटा और 32.08 लाख लेयर 1 म्युल खातों को संदिग्ध रजिस्ट्री की भाग लेने वाली संस्थाओं के साथ साझा किया गया है और 25,698 करोड़ रुपये के लेनदेन को रोका गया है।

x. समन्वय प्लेटफॉर्म को प्रचालनात्मक बनाया गया है जो साइबर अपराध संबंधी डेटा के आदान-प्रदान और विश्लेषण के लिए विधि प्रवर्तन एजेंसियों (एलईए) हेतु प्रबंधन सूचना प्रणाली (एमआईएस) प्लेटफॉर्म, डेटा भंडार और समन्वय प्लेटफॉर्म के रूप में कार्य करता है। यह विभिन्न राज्यों/संघ राज्य क्षेत्रों में साइबर अपराध की शिकायतों में शामिल अपराधों और अपराधियों के अंतर्राज्यीय संबंधों पर आधारित विश्लेषण प्रदान करता है। मॉड्यूल 'प्रतिबिंब' अपराधियों और अपराध संबंधी अवसंरचना के स्थानों को मानचित्र पर प्रदर्शित करता है, ताकि क्षेत्राधिकारियों को इसकी जानकारी मिल सके। यह मॉड्यूल विधि प्रवर्तन एजेंसियों द्वारा आई4सी और अन्य एसएमई (SME) से तकनीकी-कानूनी सहायता मांगने तथा प्राप्त करने की सुविधा भी प्रदान करता है। इससे 29,837 से अधिक आरोपियों की गिरफ्तारी और 2,33,593 से अधिक साइबर जांच सहायता अनुरोध प्राप्त हुए हैं।

xi. गैरकानूनी कार्य करने के लिए उपयोग की जा रही किसी भी जानकारी, डेटा या संचार लिंक को हटाने या अक्षम करने की सुविधा के लिए, सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 79 की उप-धारा (3) के खंड (ख) के तहत उपयुक्त सरकार या उसकी एजेंसी द्वारा आईटी मध्यस्थों को नोटिस भेजने की प्रक्रिया में तेजी लाने के लिए 'सहयोग' पोर्टल शुरू किया गया है।

राज्य सभा अतारांकित प्रश्न सं. 2800, दिनांक 12.08.2026

xii. गृह मंत्रालय ने साइबर सुरक्षा संबंधी खतरों, साइबर जासूसी, राष्ट्रीय सुरक्षा के विरुद्ध उभरती प्रौद्योगिकियों के दुरुपयोग और इसी तरह की चिंताओं से प्रभावी ढंग से निपटने के उद्देश्य से दिनांक 22.01.2025 को MAC (मल्टी एजेंसी सेंटर) प्लेटफॉर्म के अंतर्गत CyMAC (साइबर मल्टी एजेंसी सेंटर) को स्थापित किया है।

xiii. CERT-In (सीईआरटी-इन) आर्टिफिशियल इंटेलिजेंस का उपयोग करके दुर्भावनापूर्ण हमलों और कंप्यूटर, नेटवर्क और डेटा की सुरक्षा के लिए निरंतर आधार पर नवीनतम साइबर खतरों/कमजोरियों के संबंध में अलर्ट और एडवाइजरी जारी करता है।

xiv. सीईआरटी-इन द्वारा कार्यान्वित राष्ट्रीय साइबर समन्वय केंद्र (एनसीसीसी) साइबर सुरक्षा संबंधी खतरों का पता लगाने के लिए साइबर स्पेस की जांच करता है। यह कार्रवाई करने के लिए संबंधित राज्य सरकारों, विभिन्न क्षेत्रों के संगठनों और हितधारक (स्टेकहोल्डर) एजेंसियों के साथ जानकारी को साझा करता है।

xv. आवश्यक शमन के लिए दुर्भावनापूर्ण डोमेन और फिशिंग गतिविधियों का पता लगाने के लिए सीईआरटी-इन द्वारा एआई संचालित स्थितिजन्य जागरूकता प्रणालियों को तैनात किया गया है।

xvi. सीईआरटी-इन राज्य सरकारों और संगठनों के साथ सक्रिय रूप से जानकारी एकत्र करने, उसका विश्लेषण करने और विशेष रूप से तैयार अलर्ट को उनके साथ साझा करने के लिए एक स्वचालित साइबर थ्रेट एक्सचेंज प्लेटफॉर्म का संचालन करता है ताकि उनके द्वारा खतरे को कम करने की सक्रिय कार्रवाई की जा सके।

xvii. साइबर स्वच्छता केंद्र (सीएसके) सीईआरटी-इन द्वारा प्रदान की जाने वाली एक सेवा है, जो साइबर स्पेस में स्वच्छ भारत के दृष्टिकोण का विस्तार करती है। साइबर स्वच्छता केंद्र मैलिशस प्रोग्रामों और संवेदनशील सेवाओं का पता लगाने और राज्यों और क्षेत्रों के संगठनों को उपचारात्मक उपाय प्रदान करने में मदद करता है।

xviii. सूचना सुरक्षा की सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और जांच करने के लिए सीईआरटी-इन ने 237 सुरक्षा जांच संगठनों को सूचीबद्ध किया है।

xix. साइबर सुरक्षा स्थिति का मूल्यांकन करने तथा सरकार (केंद्र और राज्य) और महत्वपूर्ण क्षेत्रों में संगठनों की तैयारी को सक्षम बनाने के लिए नियमित रूप से साइबर सुरक्षा संबंधी मॉक अभ्यास आयोजित किए जाते हैं। साइबर सुरक्षा के क्षेत्र में समन्वय और सूचना साझा करने की सुविधा के लिए राज्यों में इन अभ्यासों के साथ कार्यशालाएं आयोजित की जाती हैं।

राज्य सभा अतारांकित प्रश्न सं. 2800, दिनांक 12.08.2026

xx. केंद्र सरकार ने साइबर अपराध के बारे में और जागरूकता बढ़ाने के लिए कई कदम उठाए हैं, जिनमें अन्य बातों के साथ-साथ कॉलर ट्यून अभियान, एसएमएस, आई4सी सोशल मीडिया अकाउंट जैसे कि एक्स (पूर्व में ट्विटर) (@CyberDost), फेसबुक (CyberDostI4C), इंस्टाग्राम (CyberDostI4C), टेलीग्राम (cyberdosti4c) के माध्यम से संदेश प्रसारित करना, एसएमएस अभियान, टीवी अभियान, रेडियो अभियान, स्कूल अभियान, सिनेमा हॉल में विज्ञापन, सेलिब्रिटी एंडोर्समेंट, आईपीएल अभियान, कई माध्यमों से प्रचार हेतु माईगव का उपयोग करना, राज्यों/संघ राज्य-क्षेत्रों के सहयोग से साइबर सुरक्षा एवं संरक्षा जागरूकता सप्ताह का आयोजन करना, मेट्रो स्टेशनों, रेलवे स्टेशनों और हवाई अड्डों पर डिजिटल प्रदर्शन (Displays) आदि शामिल हैं।

*****