डिजिटल भारतातील सायबर फसवणुकीला आळा

नवी दिल्ली, 8 ऑक्टोबर 2025

मी एका अशा डिजिटल भारताचे स्वप्न पाहिले आहे, जिथे सायबर सुरक्षा हा आपल्या राष्ट्रीय सुरक्षेचा अविभाज्य घटक असेल.

-पंतप्रधान नरेंद्र मोदी

ठळक मुद्दे

देशातील 86 टक्क्यांपेक्षा जास्त घरांमध्ये आता इंटरनेटची जोडणी पोहोचली आहे.

भारतात सायबर सुरक्षा विषयक घटनांचे प्रमाण 2022 मधील 10.29 लाखावरून 2024 मध्ये 22.68 लाखांपर्यंत वाढले आहे.

2025-2026 च्या केंद्रीय अर्थसंकल्पात सायबर सुरक्षा प्रकल्पांसाठी 782 कोटी रुपये निधीची तरतूद करण्यात आली आहे.

सायबर फसवणुकीशी संबंधित 9.42 लाखांपेक्षा जास्त सिम कार्ड आणि 2 लाख 63 हजार 348 आयएमईआय (IMEI - आंतरराष्ट्रीय मोबाईल उपकरण ओळख क्रमांक) रोखण्यात आले आहेत.

1930 या समर्पित हेल्पलाइनच्या माध्यमातून तातडीचे सायबर सुरक्षा सहाय्य पुरवले जाते.

प्रस्तावना

भारताचे सायबर विश्व (Cyberspace) आता पूर्वीपेक्षा अधिक व्यस्त आहे. इथे दररोज कोट्यवधी व्यवहार आणि संवाद होतात. 86 टक्क्यांपेक्षा जास्त घरांमध्ये इंटरनेटची जोडणी पोहोचली असून, या आकडेवारीतून डिजिटल इंडिया उपक्रमाअंतर्गत झालेली उल्लेखनीय प्रगती दिसून येते. या विस्तारत असलेल्या डिजिटल अवकाशामुळे आता नागरिकांना त्यांच्या हाताच्या बोटावर वर डिजिटल सेवा उपलब्ध झाल्या आहेत. मात्र, याच बरोबर सायबर फसवणुकीसंदर्भातील हल्ल्यांच्या दृष्टीने पूरक परिस्थितीचाही तितकाच विस्तार झाला असून, यामुळे सायबर सुरक्षा हा राष्ट्रीय प्राधान्याचा मुद्दा बनला आहे.

सायबर फसवणूक म्हणजे डिजिटल व्यासपीठांच्या माध्यमातून केल्या जाणाऱ्या फसवणुकीच्या कृती. यामध्ये अनधिकृत प्रवेश, माहितीसाठ्याची चोरी किंवा ऑनलाइन घोटाळे यांचा समावेश असतो. पीडितांचे आर्थिक नुकसान करणे हाच यामागचा हेतू असतो.

2022 मध्ये भारतातील सायबर सुरक्षा विषयक घटनांचे प्रमाण 10.29 लाख होते, त्यात वाढ होऊन 2024 मध्ये ते 22.68 लाख पर्यंत पोहोचले. या आकडेवारून भारतातील डिजिटल धोक्याची वाढती व्याप्ती आणि त्यातली क्लिष्टता दिसून येते. त्याचवेळी, आर्थिक नुकसानीचे प्रमाणही वाढत आहे. 28 फेब्रुवारी 2025 पर्यंत, राष्ट्रीय सायबर गुन्हे नोंदणी पोर्टलवर (NCRP) सायबर फसवणुकीमुळे 36.45 लाख रुपये इतके नुकसान झाल्याची नोंद झाली आहे. ही आकडेवारी वाढत्या आव्हानांकडे निर्देश करत असली, तरी त्यातून देशाच्या शोध आणि नोंदणी व्यवस्थेअंतर्गत साधलेली उल्लेखनीय प्रगती देखील दिसून येते.

सायबर फसवणुकीच्या पद्धतींचा माग काढणे

सायबर फसवणुकीचे विकसित होत असलेले स्वरूप पाहिले तर, या फसवणूक केवळ एकाच पद्धतीपुरत्या मर्यादित नसून, त्या विविध स्वरुपात केल्या जात असल्याचे, तसेच नवीन तंत्रज्ञान आणि वापरकर्त्यांच्या प्रवृत्तीनुसार त्या सातत्याने बदल होत असल्याचेही दिसून येते. अशावेळी प्रतिबंधात्मक उपाययोजना राबण्यासाठी या पद्धतींचे आलेखन तयार करणे गरजेचे आहे. अशा फसवणुकीचा जगभरातील आर्थिक परिणाम मोठा आहे, शिवाय त्यात संघटित गुन्हेगारीचा सहभागही मोठा आहे, यावरून बहुतांशवेळा अशी प्रकरणे आग्नेय आशियातील फसवणूक केंद्रांशी जोडलेली असल्याचेही दिसून येते.

उदयोन्मुख सायबर धोके

अनेक प्रकरणांमध्ये स्पूफिंग (Spoofing) सारख्या तंत्रांचा, म्हणजे गुन्हेगार विश्वासार्ह स्त्रोत असल्याचा बनाव रचून फसवणूक करतात असे दिसून आले आहे. त्याचप्रमाणे, कृत्रिम बुद्धिमत्ता तंत्रज्ञानाचा वापर करून केलेल्या डीपफेक्स (Deepfakes - हुबेहुब प्रतिकृतीचा वापर करणे) आणि फिशिंग (Phishing - फसवणूकीच्या जाळ्यात ओढणे) संबंधीत प्रकरणांचे प्रमाणही वाढते आहे. फिशिंगमध्ये व्यक्तींना फसवे ईमेल किंवा संदेश पाठवून संवेदनशील माहिती उघड करण्यासाठी प्रवृत्त केले जाते. यामुळे संबंधित घोटाळ्यांच्या एकूण प्रभावाची व्याप्तीही वाढते.

युनिफाइड पेमेंट्स इंटरफेस (UPI), ही आर्थिक देयकांच्या व्यवहारासाठी भारतात सर्वात जास्त वापरली जाणारी डिजिटल पेमेंट पद्धत आहे. फसवणूकदारांनी या पद्धतीला देखील सुरक्षा भेदलेल्या(compromised) मोबाईल क्रमांकांचा वापर करून लक्ष्य केले आहे. या समस्येचे निराकरण करण्यासाठी, दूरसंचार विभागाने आर्थिक फसवणूक जोखीम निर्देशक (Financial Fraud Risk Indicator - FRI) ही इशारा देणारी सुविधा सुरू केली आहे. हा निर्देशक संशयास्पद क्रमांकांचे मध्यम, उच्च किंवा अतिउच्च जोखीमाअंतर्गतचे क्रमांक म्हणून वर्गीकरण करतो.

ऑनलाइन सट्टेबाजीच्या ॲप्सच्या स्वरूपात अवैध डिजिटल उद्योगक्षेत्र देखील उभे राहिले आहे. हे ॲप्स मोठ्या परताव्याची खोटी आश्वासने देऊन वापरकर्त्यांना त्यांच्या ऑनलाइन वॉलेटमध्ये (पाकिटामध्ये) निधी जमा करण्यासाठी प्रवृत्त करतात. अशा प्रकरणांमधून आत्तापर्यंत 400 कोटी रुपयांपेक्षा जास्त गुन्हेगारी उत्पन्न निर्माण केले गेले असल्याचे समोर आले आहे.

सायबर फसवणुकीविरुद्धचा भारताचा लढा बळकट करण्याच्या उद्देशाने, 21 ऑगस्ट 2025 रोजी ऑनलाइन गेमिंग प्रोत्साहन आणि नियमन विधेयक, 2025, मंजूर करण्यात आले. ई-क्रीडा आणि समाजमाध्यमांवरील ऑनलाइन खेळांना प्रोत्साहन देण्याच्या अनुषंगानेच या विधेयकाची आखणी केली गेली आहे. त्याच वेळी ऑनलाइन पैसे द्यावे लागत असलेल्या गेमिंगच्या बाबतीत, जाहिराती आणि संबंधित आर्थिक व्यवहारांवर पूर्णतः बंदी घातली गेली आहे.

भारताचा सायबर सुरक्षा आराखडा

भारत सरकारने देशातील आपल्या विशाल ऑनलाइन समुदायाच्या संरक्षणासाठी एक मजबूत संरक्षण यंत्रणा लागू केली आहे. भारतीय नागरिक आता उद्योग व्यवसायाशी संबंधित व्यवहार, शिक्षण, आर्थिक व्यवहार आणि सरकारी सेवा डिजिटल पद्धतीने वापरण्यासाठी आपल्या दैनंदिन जीवनात इंटरनेटचा अधिकाधिक वापर करू लागले आहेत.

आघाडीच्या फळीत तैनात असलेल्या कर्मचाऱ्यांना सायबर गुन्हेगारी विषय अत्यावश्यक तपास कौशल्यांनी सुसज्ज करण्याच्या उद्देशाने सुरु केलेल्या CyTrain या सायबर प्रशिक्षण पोर्टलवर 1 लाख 5 हजार 796 पेक्षा जास्त पोलीस अधिकारी नोंदणीकृत आहेत, आणि 82 हजार 704 पेक्षा जास्त प्रमाणपत्रे जारी केली गेली आहेत.

सायबर अवकाशाला सुरक्षित करणारे सायबर कायदे

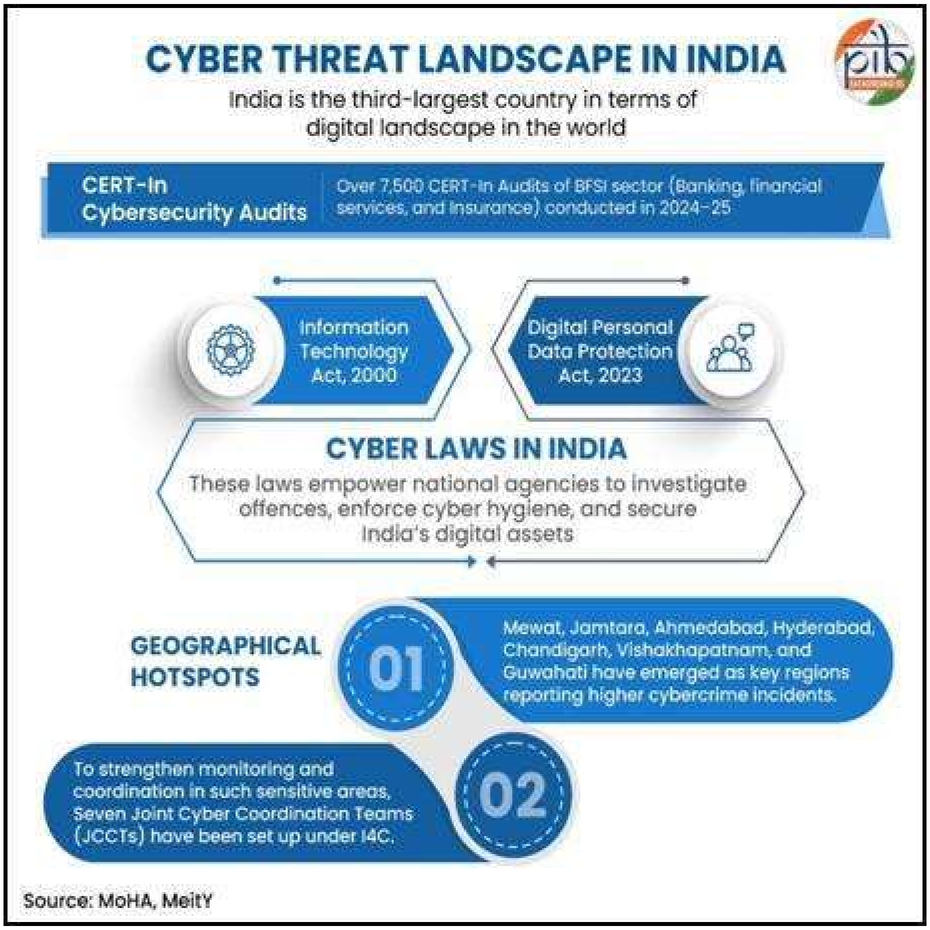
सुरक्षित डिजिटल वातावरणाची गरज आणि महत्त्व लक्षात घेऊन, भारताचा सायबर सुरक्षा आराखडा तयार केला गेला आहे. हा आराखडा खाली नमूद प्रमुख कायद्यांवर आधारित आहे:

माहिती तंत्रज्ञान कायदा, 2000 (Information Technology Act, 2000) हा भारताच्या सायबर कायद्याच्या आराखड्याचा पाया आहे. या कायद्याअंतर्गत ओळख चोरी, तोतयागिरी, संगणकीय संसाधनांद्वारे फसवणूक तसेच अश्लील अथवा नुकसानकारक साधनसामग्रीचा प्रसार यांसारख्या गुन्ह्यांवर भर दिला गेला आहे. यात डिजिटल व्यासपीठांचा आर्थिक फायद्यासाठी गैरवापर करणाऱ्या फसवणूकदारांवर खटला चालवण्यासाठीच्या महत्वाच्या तरतुदी आहेत. यासोबतच संबंधित

अधिकाऱ्यांना नुकसानकारक संकेतस्थळे आणि फसवणूक करणारे ॲप्लिकेशन्स ब्लॉक करण्याचे अधिकारही याअंतर्गत दिले गेले आहेत

माहिती तंत्रज्ञान (मध्यस्थ मार्गदर्शक तत्त्वे आणि डिजिटल माध्यम नीतिमूल्य संहिता) नियम, 2021 (Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021), या कायद्याच्या माध्यमातून समाज माध्यम मध्यस्थी, डिजिटल व्यासपीठे आणि ऑनलाइन बाजारपेठांचे उत्तरदायित्व सुनिश्चित केले गेले आहे. या नियमाअंतर्गत कृत्रिम बुद्धिमत्तेसह उदयोन्मुख तंत्रज्ञानाच्या गैरवापरावरही भर दिला गेला आहे, तसेच संबंधित व्यासपीठांवरून बेकायदेशीर आशयसामग्री काढून टाकणे बंधनकारक केले गेले आहे.

डिजिटल वैयक्तिक माहितीसाठा संरक्षण कायदा, 2023 (Digital Personal Data Protection Act, 2023) : या कायद्याअंतर्गत यासाठी सर्व वैयक्तिक माहितीचे कायदेशीररित्या आणि वापरकर्त्याच्या संमतीने हाताळणी बंधकारक केले गेले आहे. यामुळे भारताचे डिजिटल अवकाश सर्वांसाठी सुरक्षित आणि अधिक उत्तरदायी बनले आहे. सुरक्षा विषयक उपाययोजनांची सुनिश्चिती करण्याच्या उद्देशाने या कायद्याअंतर्गत माहितीसाठ्याचा ताबा असलेल्यांवर कठोर जबाबदाऱ्या दिल्या गेल्या आहेत. यामुळे अशा माहितीसाठा अनधिकृतपणे हाताळणेन अथवा त्याचा गैरवापर होण्यासारखे धोके कमी झाले आहेत. या कायद्यामुळेच आजपर्यंत, फसवणूकीच्या घडामोडींशी संबंधित असलेले ९.42 लाखांपेक्षा जास्त सिम कार्ड आणि 2 लाख 63 हजार 348 आयएमईआय (International Mobile Equipment Identity - आंतरराष्ट्रीय मोबाईल उपकरण ओळख क्रमांक) वापरापासून रोखण्यात आले आहेत.



सायबर विषयक घटनांना प्रतिसाद

इंडियन कॉम्प्युटर इमर्जन्सी रिस्पॉन्स टीम (CERT-In) ही सायबर सुरक्षा घटनांना प्रतिसाद देणारी राष्ट्रीय संस्था आहे. ही संस्था सायबर धोक्यांवर देखरेख ठेवते, असुरक्षिततेचा शोध घेते आणि आवश्यक मार्गदर्शक तत्वे जारी करते. माहितीसाठ्याशी संबंधित छेडछाड, डेटा भंग (Data Breaches), फिशिंग मोहिम किंवा मालवेअर घुसखोरी यांसारख्या घटनांबाबत कळल्यानंतर CERT-In द्वारे संबंधित प्रभावित संस्थांना सूचना प्रसारित केली जाते तसेच त्यावरच्या उपाययोजना देखील सुचवते. या सक्रिय यंत्रणेमुळे धोक्यांचा वेळेवर प्रतिबंध सुनिश्चित होतो, परिणामी सरकार, उद्योग क्षेत्र आणि महत्त्वाच्या सेवा प्रदात्यांच्या लवचिकतेतही सुधारणा घडून येते. मार्च 2025 पर्यंत, CERT-In च्या वतीने सायबर सुरक्षा विषयक 109 सराव प्रात्यक्षिकांच्या आयोजन केले होते. याअंतर्गत आपल्या सायबर सज्जता चाचणी करून घेण्याच्या तसेच लवचिकता निर्माण करण्याच्या उद्देशाने विविध राज्ये आणि क्षेत्रांमधील 1,438 संस्था सहभागी झाल्या होत्या.

अत्यावश्यक पायाभूत सुविधांचे संरक्षण

राष्ट्रीय अत्यावश्यक माहिती पायाभूत सुविधा संरक्षण केंद्राची (NCIIPC) निर्मिती माहिती तंत्रज्ञान कायदा, 2000 च्या कलम 70A अंतर्गत केली गेली आहे. हे केंद्र भारतातील अत्यावश्यक माहितीच्या पायाभूत सुविधांच्या संरक्षणासाठीची राष्ट्रीय समन्वयक यंत्रणा आहे. हे केंद्र राष्ट्रीय सुरक्षा आणि सार्वजनिक सुरक्षिततेसाठी महत्त्वच्या असलेल्या बँकिंग, दूरसंवाद, ऊर्जा आणि वाहतूक यांसारख्या क्षेत्रातील भागधारकांसोबत अत्यंत दृढतेने संपर्क आणि समन्वय साधून काम करत असते. या केंद्राद्वारे सातत्यपूर्ण देखरेख, जोखीम मूल्यांकन आणि प्रत्येक क्षेत्रासाठी विशिष्ट मार्गदर्शक तत्त्वे जारी करण्याची जबाबदारी पार पाडली जाते. अशा उपाययोजनांच्या माध्यमातून NCIIPC बचावात्मक क्षमतेला बळकटी देते, त्यासोबतच अत्यावश्यक सेवांना धोकादायक ठरू शकतील असे धोके संपुष्टात आणण्याचे काम करते.

कायदा अंमलबजावणी क्षमतेचे बळकटीकरण

भारतीय सायबर गुन्हे सन्मवय केंद्राची स्थापना (I4C) गृह मंत्रालयाच्या अखत्यारीत केली गेली आहे. हे केंद्राद्वारे कायद्याची अंमलबजावणी करणाऱ्या यंत्रणांना (LEAs) संघटित आणि समन्वित पद्धतीने सायबर गुन्हेगारी हाताळण्यासाठी एक सर्वसमावेशक आराखडा आखून दिला जातो. या केंद्राच्या माध्यमातून विशेष प्रशिक्षण कार्यक्रम, संशोधन आणि तंत्रज्ञानाधारीत साधने विकसित करण्यासारख्या उपाययोजनांच्या माध्यमातून क्षमता निर्मितीसाठी पाठबळ पुरवले जाते. यासोबतच वास्तव वेळेतील माहितीची देवाणघेवाण आणि समन्वित तपासाची सुविधा उपलब्ध करून दिली जाते, यामुळे आर्थिक फसवणूक आणि इतर संघटित सायबर गुन्ह्यांशी संबंधित सायबर गुन्हेगारी व्यवस्थेविरोधात परिणामकारक कारवाई करणे शक्य होते. आजपर्यंत, I4C च्या माध्यमातून सायबर फसवणुकीशी संबंधित 3,962 स्काईप आयडी आणि 83,668 व्हॉट्सॲप खाती सक्रिय कारवाईअंतर्गत ब्लॉक केली गेली आहेत.

सायबर सुरक्षाविषयक उपक्रम : कृतीशील प्रशासन

भारताच्या सायबर संरक्षण व्यवस्थेला बळ देण्यासाठी, 2025च्या केंद्रीय अर्थसंकल्पात सायबर सुरक्षा विषयक प्रकल्पांसाठी 782 कोटी रुपये निधीची तरतूद करण्यात आली आहे. सरकारने उचचलेल्या या महत्त्वाच्या पावलातून राष्ट्रीय सुरक्षेला धोका निर्माण करणाऱ्या सायबर धोक्यांवर सरकारने दिलेला भर अधोरेखित होतो. नागरिक आर्थिक सायबर फसवणूक तक्रार नोंदणी आणि व्यवस्थापन व्यवस्थेच्या (CFCFRMS) माध्यमातून 17.82 लाखांपेक्षा जास्त तक्रारींची नोंद झाली, यामुळे तक्रा, वित्तीय संस्थांची 5,489 कोटी रुपये पेक्षा जास्त रक्कम वाचवणे शक्य झाले.

राष्ट्रीय सायबर गुन्हे तक्रारनोंदणी पोर्टल

सायबर गुन्ह्यांविरुद्धच्या लढ्यात नागरिकांचा सहभागाला बळकटी देण्यासाठी, सरकारने राष्ट्रीय सायबर गुन्हे तक्रार नोंदणी पोर्टल (www.cybercrime.gov.in) कार्यान्वित केले आहे. या पोर्टलच्या माध्यमातून नागरिकांना विविध प्रकारच्या सायबर गुन्हेगारीशी संबंधित तक्रारी नोंदवण्याची सुविधा उपलब्ध करून दिली आहे. याअंतर्गत विशेषतः महिला आणि मुलांना लक्ष्य करून केलेल्या जाणाऱ्या गुन्ह्यांवर विशेष भर दिला जातो. या जोडीला 1930 ही समर्पित सायबर गुन्हे हेल्पलाइनही उपलब्ध करून दिली असून, त्याद्वारे ऑनलाइन आर्थिक फसवणुकीला बळी पडलेल्या पीडितांना तातडीने मदत उपलब्ध करून दिली जाते. याअंतर्गत तातडीने तक्रारीची नोंद करणे आणि शक्य असल्यास फसवणूक झालेले व्यवहार गोठवण्याची सुविधा उपलब्ध करून दिली आहे. एकत्रितपणे, हे उपक्रम नागरिकांसाठी एक सुलभ आणि प्रतिसादात्मक तक्रार निवारण यंत्रणा म्हणून उपयुक्त ठरले आहेत.

आंतरशाखीय भौतिक सायबर व्यवस्था विषयक राष्ट्रीय अभियान (National Mission on Interdisciplinary Cyber-Physical Systems (NM-ICPS)

आंतरविद्याशाखीय सायबर-फिजिकल प्रणालीवर राष्ट्रीय अभियानाअंतर्गत (NM-ICPS) सायबर सुरक्षा, कृत्रिम बुद्धिमत्ता विषयक प्रगत संशोधन आणि नवोन्मेषाला चालना देण्याच्या माध्यमातून, सायबर फसवणुकीला आळा घालण्याचे महत्वाचे प्रयत्न केले जात आहेत. याअंतर्गत धोक्यांचा शोध घेण्यासाठी साधने, व्यासपीठे आणि कार्यप्रद्धती विकसित करण्यासाठी पाठबळ पुरवले जाते. यामुळे व्यक्ती, उद्योग - व्यवसाय आणि महत्त्वाच्या पायाभूत सुविधांना लक्ष्य करणाऱ्या सायबर फसवणुक ओळखणे आणि ते रोखण्यासंबंधीची भारताची क्षमता बळकट होण्यात मदत होत आहे. या राष्ट्रीय अभियानाअंतर्गत शैक्षणिक संस्था, उद्योग व्यवसाय आणि सरकार यांच्यातील सहकार्यपूर्ण भागिदारीतून आर्थिक फसवणूक, फिशिंग आणि ओळखीशी संबंधीत गुन्ह्यांसह, उदयाला येत असलेले इतर आणि अत्याधुनिक सायबर धोक्यांविरोधात उपाययोजना करण्याच्या प्रक्रियेलाही गती मिळू लागली आहे.

महिला आणि मुलांविरोधातील सायबर गुन्ह्ये प्रतिबंध (CCPWC) योजना

महिला आणि मुलांविरोधातील सायबर गुन्हे प्रतिबंध योजने (CCPWC) अंतर्गत, धोक्याच्या दृष्टीने संवेदनशील असलेल्या घटकांना, विशेषतः महिला आणि मुलांना लक्ष्य करणाऱ्या सायबर फसवणुकीच्या गुन्ह्यांवर भर दिला गेला आहे. या योजनेसाठी सरकारने 132.93 कोटी रुपयांच्या आर्थिक तरतुदीचे बळही उपलब्ध करून दिले आहे. या योजनेअंतर्गत देशभरातील 33 राज्ये आणि केंद्रशासित प्रदेशांमध्ये सायबर न्यायवैद्यक आणि प्रशिक्षण प्रयोगशाळा स्थापित केल्या आहेत. या प्रयोगशाळांच्या माध्यमातून सायबर गुन्हे तपास, डिजिटल न्यायवैद्यक आणि प्रतिबंधात्मक उपाययोजना अशा विषयांतर्गत 24 हजार 600 पेक्षा जास्त कर्मचाऱ्यांना प्रशिक्षित केले आहे. वाढलेली जागरूकता, अगदी सुरुवातीच्या टप्प्यावरील शोध आणि जलद प्रतिसाद क्षमतांच्या माध्यमातून, या

योजनेअंतर्गत महिला आणि मुलांविरोधात होणारी ऑनलाइन फसवणूक, घोटाळे आणि शोषण रोखण्याच्या उद्देशाने कायद्यांची प्रभावी अंमलबजावणी करण्याची क्षमताही मजबूत होऊ लागली आहे. यामुळे अधिक सुरक्षित डिजिटल वातावरणाची सुनिश्चिती होऊ शकली आहे.

सायबर संकट व्यवस्थापन आराखडा (CCMP)

सायबर हल्ले आणि सायबर-दहशतवादाविरुद्धच्या सज्जतेला बळकटी देण्याच्या उद्देशाने, केंद्र सरकारने सर्व सरकारी संस्थांकरता सायबर संकट व्यवस्थापन आराखडा (CCMP) लागू केला. या आराखड्यामुळे कोणतेही सायबर संकट उद्भवल्यास, परिस्थिती समन्वित रितीने पूर्वपदावर येऊल याची सुनिश्चित करण्यासाठी एक धोरणात्मक चौकट उपलब्ध झाली आहे. या आराखड्याअंतर्गत आजवर क्षमता निर्मिती आणि जागरूकता वाढवण्यासाठी देशभरात 205 कार्यशाळांचे आयोजन केले गेले आहे.

समन्वय प्लॅटफॉर्म (व्यासपीठ)

समन्वय प्लॅटफॉर्म या व्यासपीठ हे गुन्हेगार तसेच गुन्ह्यांशी सं◌ंबधीत विश्लेषणावर आधारित माहिती उपलब्ध करून देणारा एक आंतरराज्यीय दुवा ठरला आहे. यामुळे सायबर फसवणूक विषयक प्रकरणांच्या तपासणीला बळकटी मिळाली आहे. या व्यासपीठाअंतर्गत उपलब्ध करून दिलेल्या प्रतिबिंब या प्रारुपावर गुन्हेगार आणि गुन्हेगारीशी संबंधीत पायाभूत सुविधांच्या ठिकाणांची माहिती मिळते. यामुळे संबंधीत अधिकाऱ्यांना कृती करण्यायोग्य दृश्यमानता उपलब्ध होते. आजपर्यंत, या व्यासपीठाच्या सहकार्यामुळे 12 हजार 987 आरोपींना अटक करता आली आहे, 1 लाख 51 हजार 984 गुन्हेगारांचा माग काढता आला आहे आणि 70 हजार 584 सायबर तपास सहाय्यता विनंत्या मिळाल्या आहेत. यामुळे संघटित स्वरुपातील सायबर फसवणूकीचे जाळे परिणामकारकतेने नष्ट करण्यात मोठी मदत झाली आहे.

सहयोग पोर्टल

सहयोग पोर्टलच्या माध्यमातून बेकायदेशीरपणे ऑनलाइन आशय सामग्री हाताळण्याच्या समस्येचा सामना करण्यासाठी एक एकात्मिक व्यासपीठ उपलब्ध झाले आहे. या व्यासपीठाच्या माध्यमातून मध्यस्थांना संबंधित आशय सामग्री हटवण्याची सूचना स्वयंचलितपणे जारी करण्याची सुविधा उपलब्ध झाली आहे. यामुळे सायबर जगतात सातत्याने उद्भवत राहणाऱ्या नुकसानकारक आशय सामग्रीविरोधात जलद गतीने कारवाई होईल याची सुनिश्चिती होऊ शकली आहे. या व्यासपीठाच्या माध्यमातून भारतातील सर्व अधिकृत संस्थांना एकाच इंटरफेसवर आणणे शक्य झाले असून, यामुळे

बेकायदेशीर आशय सामग्रीविरोधात योग्य वेळेत प्रभावीपणे कार्यवाही करण्याची सरकारची क्षमताही मजबूत होऊ लागली आहे.

सायबर सुरक्षा विषयक सराव

21 जुलै ते 01 ऑगस्ट या कालावधी दरम्यान भारत राष्ट्रीय सायबर सुरक्षा सराव 2025 चे आयोजन करण्यात आले होते. या सरावाच्या माध्यमातून भारताची सायबर क्षेत्रविषयक लवचिकतेला बळकटी देण्याची वचनबद्धता पुन्हा एकदा अधोरेखीत झाली. सायबर सुरक्षेशी संबंधीत व्यावसायिक तज्ञ, नियामक आणि धोरणकर्ते यांच्यासह 600 पेक्षा जास्त प्रतिनिधी या सरावात सहभागी झाले होते. स्ट्रॅटेक्स (STRATEX) हा एक कृत्रिमतेने रचनेला सायबर जगतातील छेडछाडीचा प्रसंग हे या सरावाचे मुख्य वैशिष्ट्य ठरले. वास्तव वेळेतील आंतर-यंत्रणा समन्वय आणि निर्णय घेण्याच्या क्षमतेची चाचणी घेण्याच्या उद्देशाने अशा वातावरणाची निर्मिती करण्यात आली होती.

इंडिया मोबाईल कॉँग्रेस 2025 मध्ये सायबर सुरक्षेवर भर

९व्या इंडिया मोबाईल कॉँग्रेसमध्ये, सायबर सुरक्षा हे प्रमुख्याने भर दिला जाणार असलेल्या क्षेत्रांपैकी एक क्षेत्र असणार आहे. यातून डिजिटल व्यवस्था आणि उदयोन्मुख तंत्रज्ञानाचे सायबर धोक्यांपासून संरक्षण करण्याचे भारताचे प्रयत्न अधोरेखित होणार आहेत. परिवर्तनासाठी नोवोन्मेष ही ९व्या इंडिया मोबाईल कॉँग्रेसची संकल्पना असणार आहे. 8 ते 11 ऑक्टोबर असे तीन दिवस चालणाऱ्या या ९व्या इंडिया मोबाईल कॉँग्रेसचे, नवी दिल्ली इथे पंतप्रधान नरेंद्र मोदी यांच्या हस्ते या उपक्रमाचे उद्घाटन होईल.

९व्या इंडिया मोबाईल कॉँग्रेस मध्ये सायबर सुरक्षा शिखर परिषद आणि भारत 6G सिम्पोजियम यांसह सहा जागतिक शिखर परिषदा होणार आहेत. यातून नेक्स्ट-जनरेशन डिजिटल तंत्रज्ञानातील भारताचे वाढती आघाडी दिसून येईल. 6G, सायबर सुरक्षा, उपग्रह संप्रेषण, कृत्रिम बुद्धिमत्ता, इंटरनेट ऑफ थिंग्ज (IoT) आणि दूरसंसंवाद उत्पादने या प्रमुख क्षेत्रांवर यात भर दिला जाणार आहे.

9व्या इंडिया मोबाईल कॉंग्रेससाठी 1.5 लाखांपेक्षा जास्त अभ्यागत, 7,000 पेक्षा जास्त आंतरराष्ट्रीय प्रतिनिधी, 400 पेक्षा जास्त प्रदर्शक भेट देतील, तसेच 1,600 पेक्षा जास्त प्रत्यक्ष वापरात असलेल्या साधने प्रदर्शीत केली जातील अशी अपेक्षा आहे. या आयोजनाअंतर्गत 100 पेक्षा जास्त सत्रे होणार असून, 800 पेक्षा जास्त वक्त्येही त्यात सहभागी होतील. एका अर्थाने 9 वी इंडिया मोबाईल कॉंग्रेस ही जागतिक सहकार्य आणि नवोन्मेषासाठीचे एक प्रमुख व्यासपीठ म्हणून कामी येणार आहे.

भारतात आजमितीला 1.2 अब्ज मोबाईल ग्राहक आणि 970 दशलक्ष इंटरनेट वापरकर्ते आहेत. यासोबतच देशात 5G ची अंमलबजावणी अत्यंत वेगाने सुरु आहे. अशावेळी सुरक्षित, सर्वसमावेशक आणि विस्तारता येईल अशा डिजिटल परिसंस्थेच्या निर्मितीवर भर दिला जात आहे. यामुळे एक विश्वसार्ह आणि परिवर्तनकारी डिजिटल पायाभूत सुविधांचे जागतिक केंद्र म्हणून देशाचे स्थान अधिक बळकट होत आहे.

पुढील दिशा : सायबर जागरूकता

सायबर गुन्हेगारीबद्दल सार्वजनिक जागरूकता वाढवण्यासाठी, सरकारने बहु-व्यासपीठीय प्रचार प्रसाराच्या धोरणाचा अवलंब केला आहे.

सायबर फसवणुकीबद्दल लोकांना सावध करण्यासाठी सरकारने रेडिओ, वर्तमानपत्रे आणि मेट्रो घोषणांद्वारे नागरिक-केंद्रित संपर्क मोहिमा सुरू केल्या आहेत.

अस्तित्वात असलेल्या आणि संभाव्य सायबर सुरक्षा धोक्यांच्या स्थितीगतीबाबत जागरूकता निर्माण करण्यासाठी CERT-In च्या वतीने राष्ट्रीय सायबर समन्वय केंद्र स्थापन करण्यात आले आहे.

MyGov या व्यासपीठाच्या माध्यमातून सायबर सुरक्षितता आणि सुरक्षा जागरूकता सप्ताह सारख्या उपक्रमाच्या आयोजनाच्या माध्यमातून सातत्याने नागरिकांसोबतचा संवाद आणि सहभाग वाढवला जात आहे.

युवा वर्गाला सायबर सुरक्षितता आणि सुरक्षेविषयी मार्गदर्शन करण्यासाठी किशोरवयीन मुले तसेच विद्यार्थ्यांसाठी एका पुस्तिकेचे प्रकाशन केले गेले आहे.

सायबर जगताविषयक जागरूकता निर्माण करणे आणि सायबर गुन्हे रोखण्याच्या अनुषंगाने सुरक्षित कार्य पद्धतींचा प्रचार प्रसार करण्यासाठी समाज माध्यमांचा वापर केला जात आहे.

सारांश

भारत डिजिटल परिवर्तन आणि सायबर धोक्यांच्या काठावर उभा आहे, आणि त्याला समांतरपणेच तो डिजिटल प्रगतीचा आधारस्तंभ बनला आहे, आणि त्याचवेळी सायबर फसवणूक करणाऱ्यांसाठीच्या आकर्षणाचे केंद्रही बनला आहे. डिजिटल इंडियाचे स्वप्न साकार करण्यासाठी, सरकारचे बहु-स्तरीय सायबर प्रतिसाद पथक फसवणूकाला प्रतिबंध करत असून, हजारोंच्या संख्यने घोटाळ्यांना कारणीभूत ठरू शकणाऱ्या क्रिया प्रक्रियांना रोखत आहे.

प्रगत न्यायवैद्यकशास्त्र, प्रचंड मोठ्या प्रमाणातील माहितीसाठ्याचे विश्लेषण (Big Data Analytics) आणि स्वदेशी साधनांमुळे राष्ट्रीय सायबर जगताची लवचिकता वाढली आहे. असे असले तरी, भारताचे सायबर अवकाश सुरक्षित करणे ही सगळ्यांची परस्पर सामायिक जबाबदारी आहे, आणि त्यासाठी सायबर फसवणुकीविरुद्धच्या या लढ्यात सरकार आणि नागरिकांनी एकत्रितपणे काम करत राहणे गरजेचे असणार आहे.

संदर्भ

सांख्यिकी आणि कार्यक्रम अंमलबजावणी मंत्रालय
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2132330

इलेक्ट्रॉनिक्स आणि माहिती तंत्रज्ञान मंत्रालय
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2154268
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2115416
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2051934

गृह मंत्रालय
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2112244
https://www.pib.gov.in/PressReleseDetail.aspx?PRID=2146786
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2152495
https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2110359
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2101613
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2158408

दळणवळण मंत्रालय
https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2153524
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2130249
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2175355

महिला आणि बालविकास मंत्रालय
https://www.pib.gov.in/PressReleasePage.aspx?PRID=2085609

पत्रसूचना कार्यालय Backgrounders
https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=155075&ModuleId=3

जागतिक आर्थिक मंच
https://www.weforum.org/stories/2024/04/cybercrime-target-sectors-cybersecurity-news/

राष्ट्रीय सुरक्षा परिषद सचिवालय
https://www.pib.gov.in/PressReleseDetailm.aspx?PRID=2151613

सक्तवसुली संचालनालय वार्षिक अहवाल 2024-2025
https://enforcementdirectorate.gov.in/sites/default/files/2025-05/Annual_Report_24-25.pdf

भारताचा अर्थसंकल्प
https://www.indiabudget.gov.in/doc/eb/vol1.pdf

आंतरशाखीय भौतिक सायबर व्यवस्था विषयक राष्ट्रीय अभियान (NM-ICPS)

https://nmicps.gov.in/#mission

भारतीय सायबर गुन्हे समन्वय केंद्र (I4C)
https://i4c.mha.gov.in/cyber-crime-categories.aspx

भारतीय ओपन गव्हर्नमेंट डेटा प्लॅटफॉर्म (OGD)
https://www.data.gov.in/resource/stateut-wise-details-statistics-national-cyber-crime-reporting-portal-ncrp-related-cyber

पीडीएफ पाहण्यासाठी इथे क्लिक करा.

हर्षल आकुदे/तुषार पवार /प्रिती मालंडकर