BACKGROUNDERS
Press Information Bureau
Government of India

सीईआरटी-इन: साइबर खतरों के विरुद्ध भारत का अग्रिम पंक्ति का रक्षक

एक सुरक्षित, भरोसेमंद और जवाबदेह साइबरस्पेस का निर्माण

23 जनवरी, 2026

मुख्य बातें

- वर्ष 2025 में, सीईआरटी-इन ने **29.44 लाख से अधिक साइबर घटनाओं** को संभाला और **1,530 चेतावनियां (अलर्ट), 390 भेद्यता संबंधी विवरण (वल्नरेबिलिटी नोट्स) एवं 65 परामर्शी (एडवाइजरी) जारी कीं**, जो बड़े पैमाने पर राष्ट्रीय साइबर प्रतिक्रिया क्षमता को दर्शाता है।
- **231 साइबर सुरक्षा मूल्यांकन (साइबर सिक्योरिटी ऑडिट) से जुड़े संगठनों को पैनल में शामिल** किया गया है, जिससे महत्वपूर्ण सूचना संचार प्रौद्योगिकी अवसंरचना में मूल्यांकन (ऑडिट) एवं भेद्यता आकलन (वल्नरेबिलिटी असेसमेंट) की क्षमता काफी मजबूत हुई है।
- **98 प्रतिशत डिजिटल आबादी** को साइबर स्वच्छता केन्द्र द्वारा कवर किया गया, **1,427 संगठन शामिल** किए गए और **89.55 लाख** मैलवेयर रिमूवल टूल डाउनलोड किए गए।
- सीईआरटी-इन की साइबर सुरक्षा की निरंतर कोशिशों को **वैश्विक पहचान मिली** है, जिसमें **विश्व आर्थिक मंच (वर्ल्ड इकोनॉमिक फोरम), ऑक्सफोर्ड यूनिवर्सिटी और फ्रांस के एएनएसएसआई** जैसे बड़े अंतरराष्ट्रीय मंचों ने एआई-संचालित खतरे का पता लगाने (थ्रेट डिटेक्शन), साइबर सुदृढ़ता (साइबर रेजिलिएंस), भरोसेमंद एआई ढांचा और नागरिक-केन्द्रित मैलवेयर शमन (मैलवेयर मिटिगेशन) में भारत के नेतृत्व को स्वीकार किया है।

भूमिका

भारत में तेजी से हो रहे डिजिटल बदलावों ने शासन, वाणिज्य और नागरिक सेवाओं को अभूतपूर्व पैमाने पर बदल दिया है। डिजिटल पेमेंट व ई-कॉमर्स से लेकर ऑनलाइन सार्वजनिक सेवाओं की आपूर्ति तक, डिजिटल

तकनीक रोजमर्रा की जिंदगी का एक जरूरी हिस्सा बन गई है। जैसे-जैसे डिजिटल सुविधाओं को अपनाने की गति तेज हो रही है, साइबरस्पेस की सुरक्षा एक राष्ट्रीय प्राथमिकता बन गई है।

ऑनलाइन धोखाधड़ी, फिशिंग, रैंसमवेयर के हमलों, एआई-आधारित घोटालों और जरूरी डिजिटल अवसंरचना पर बढ़ते खतरों को देखते हुए, एक समन्वित एवं सुदृढ़ साइबर सुरक्षा ढांचे की जरूरत पहले से कहीं अधिक हो गई है। इस चुनौती को समझते हुए, भारत सरकार ने एक सुरक्षित, भरोसेमंद और संरक्षित डिजिटल माहौल सुनिश्चित करने हेतु ठोस नीतियां, संस्थागत व्यवस्थाएं और संचालन संबंधी क्षमताएं लागू की हैं।

भारत के साइबर सुरक्षा संरचना के केन्द्र में इंडियन कंप्यूटर इमरजेंसी रिस्पॉन्स टीम (सीईआरटी-इन) है, जो इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) के तहत काम करती है और जिसे सूचना प्रौद्योगिकी अधिनियम, 2000 द्वारा अनिवार्य किया गया है। सीईआरटी-इन घटना प्रबंधन की देखरेख करके, प्रणालीगत मजबूती को बढ़ाकर और सरकार, उद्योग एवं समाज में सुरक्षित डिजिटल तरीकों को बढ़ावा देकर राष्ट्रीय साइबर रक्षा के लिए संस्थागत गहराई प्रदान करती है। इसका काम भारत के तेजी से बढ़ते डिजिटल इकोसिस्टम की सुरक्षा को मजबूत करना और डिजिटल प्लेटफॉर्म एवं सेवाओं में विश्वास को बढ़ावा देना है।

आज के आपस में जुड़े डिजिटल माहौल में, साइबर सुरक्षा अब महज एक तकनीकी चिंता भर नहीं रह गई है, बल्कि यह राष्ट्रीय सुरक्षा, आर्थिक स्थिरता और जनता के भरोसे का एक बुनियादी स्तंभ बन गई है। डिजिटल प्रणाली के बड़े पैमाने और उसकी जटिलताओं को देखते हुए निरंतर सतर्कता, मिलकर काम करने और मजबूत संस्थागत नेतृत्व की जरूरत है। नीतिगत निर्देशों को संचालन संबंधी तैयारियों के साथ मिलाकर, सीईआरटी-इन न सिर्फ उभरते हुए साइबर खतरों का जवाब देता है, बल्कि जोखिमों का अनुमान भी लगाता है, सुदृढ़ता का निर्माण करता है और भारत की डिजिटल प्रगति का सुरक्षित, समावेशी एवं टिकाऊ बने रहना सुनिश्चित करता है।

भारत का फैलता डिजिटल परिदृश्य

पिछले एक दशक में, भारत में डिजिटल प्रसार तेजी से बढ़ा है। इस प्रसार की वजह इंटरनेट का बढ़ते उपयोग, स्मार्टफोन का बड़े पैमाने पर अपनाए जाने और डिजिटल सार्वजनिक सेवाओं में हुए तेज विस्तार में निहित है। वर्ष 2025 तक, भारत में इंटरनेट कनेक्शन 100 करोड़ का आंकड़ा पार करते हुए मार्च 2014 के **25.15 करोड़** की तुलना में **100.29 करोड़** तक पहुंच गया। प्रति वायरलेस डेटा ग्राहक औसत मासिक डेटा खपत लगभग 399 गुना बढ़ गई, जो **2014 में 61.66 एमबी** से बढ़कर **2025 में 24.01 जीबी** हो गई। यह दुनिया में सबसे अधिक खपतों में से एक है।

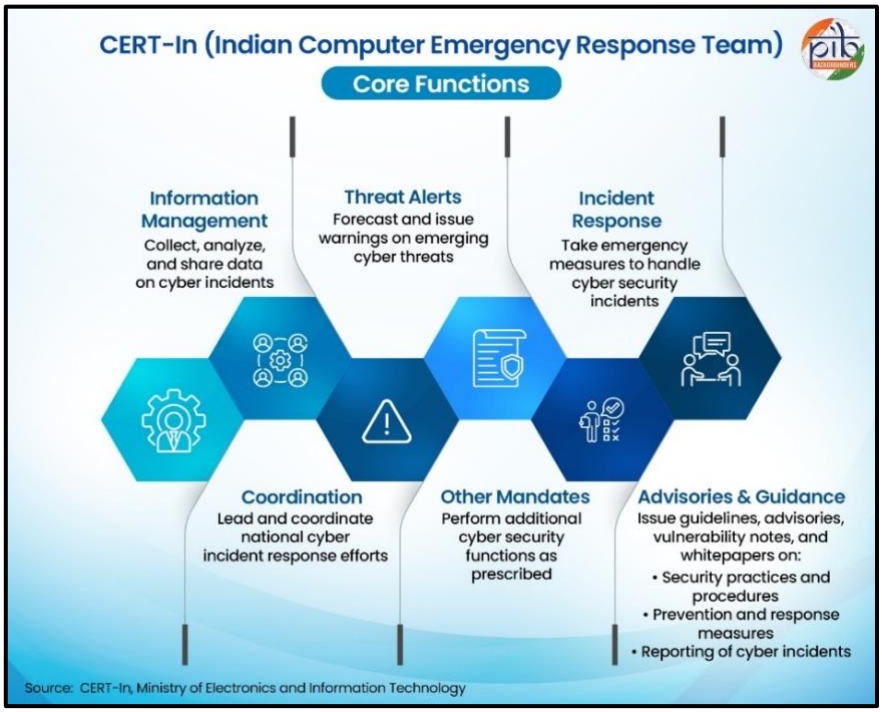
इस ठोस डिजिटल बुनियाद ने डिजिटल भुगतान के क्षेत्र में जबरदस्त वृद्धि को संभव बनाया है। यूनिफाइड पेमेंट्स इंटरफेस (यूपीआई) भारत के डिजिटल भुगतान इकोसिस्टम का मुख्य स्तंभ बनकर उभरा है। अकेले दिसंबर 2025 में, यूपीआई ने 27 लाख करोड़ रुपये से अधिक के 21 बिलियन से अधिक लेन-देन किए। इस डिजिटल प्रसार से सुविधा एवं समावेशन काफी बढ़ा तो है, लेकिन इसने साइबर खतरों के लिए हमले की सतह को भी फैला दिया है। इन जोखिमों से निपटने हेतु, केन्द्रीय बजट 2025-26 में साइबर सुरक्षा के लिए 782 करोड़ रुपये आवंटित किए गए, जो भारत की डिजिटल अवसंरचना को सुरक्षित करने पर सरकार के ठोस ध्यान को दर्शाता है।

इस संदर्भ में, सीईआरटी-इन की भूमिका भारत के साइबर सुरक्षा ढांचे की बुनियाद के तौर पर बेहद महत्वपूर्ण हो जाती है। सीईआरटी-इन के तहत काम करने वाली **सीएसआईआरटी-फिन** यानी कंप्यूटर सिक्योरिटी इंसिडेंट रिस्पॉन्स टीम फॉर फाइनेंशियल सेक्टर घटनाओं का समन्वित जवाब देकर, जानकारी साझा करके और बैंकिंग, वित्तीय सेवा एवं बीमा (बीएफएसआई) क्षेत्र को मार्गदर्शन व सहायता प्रदान कर वित्तीय क्षेत्र में साइबर सुरक्षा को मजबूत करती है। इसी तरह, सीईआरटी-इन के एक विस्तारित अंग के रूप में काम करने वाला **सीएसआईआरटी-पावर** साइबर घटनाओं का समन्वय व विश्लेषण करके, सीईआरटी-इन से प्राप्त साइबर खतरे की खुफिया जानकारी पर कार्रवाई करके, सीईआरटी-इन द्वारा प्रदान किए गए स्थितिजन्य जागरूकता विवरण के आधार पर रोकथाम के सक्रिय उपाय करके, साइबर सुरक्षा मूल्यांकन सुनिश्चित करके एवं सीईआरटी-इन के साइबर स्वच्छता केन्द्र (सीएसके) द्वारा रिपोर्ट की गई कमजोरियों को कम करके ऊर्जा क्षेत्र में साइबर सुरक्षा की स्थिति को सुदृढ़ करता है।

राष्ट्रीय साइबर सुरक्षा हेतु सीईआरटी-इन के मुख्य कार्य

सीईआरटी-इन भारत में साइबर घटनाओं पर जवाबी कार्रवाई करने वाली राष्ट्रीय एजेंसी है। **सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70बी के तहत इसके कार्यों** में साइबर हमलों को रोकना, साइबर खतरों की वास्तविक समय में निगरानी और साइबर घटनाओं को कम करने व रोकने हेतु विभिन्न हितधारकों के साथ तेजी से समन्वय स्थापित करना शामिल है।

सीईआरटी-इन के मुख्य कार्यों में शामिल हैं :



- संगठनों और नागरिकों के बीच साइबर सुरक्षा संबंधी **जागरूकता को बढ़ावा** देना,
- अपने स्वचालित साइबर खतरे से संबंधित सूचना प्लेटफॉर्म के जरिए **जानकारी साझा करने की सुविधा** देना,
- सभी क्षेत्रों को कवर करने वाले संगठनों के साथ मौजूदा और संभावित साइबर खतरों के बारे में **लगभग वास्तविक-समय में जानकारी साझा** करना,
- अंतरराष्ट्रीय भागीदारों, उद्योग जगत और शिक्षाविदों के साथ **सहयोग करना**,
- नियमित प्रशिक्षण कार्यक्रम, साइबर सुरक्षा अभ्यास/ड्रिल **आयोजित करना**,
- साइबर स्वच्छता सुनिश्चित करने के लिए **सीएसके का संचालन** करना और साइबर खतरों और हमले अभियानों की निगरानी की सुविधा के लिए **एक कमांड एंड कंट्रोल सेंटर** का संचालन करना,
- महत्वपूर्ण राष्ट्रीय और अंतरराष्ट्रीय गतिविधियों के दौरान संगठनों और हितधारकों के साथ शमन के उपायों का **समन्वय करना**,
- जिम्मेदार भेद्यता प्रकटीकरण को **संस्थागत बनाना**,
- घटना की जांच में **सहायता करना** और अपनी साइबर फोरेंसिक क्षमताओं के माध्यम से कानून प्रवर्तन एजेंसियों का समर्थन करना,
- **संगठनों को सक्षम बनाना** और राष्ट्रीय तैयारी को बढ़ाने हेतु साइबर संकट प्रबंधन योजना कार्यान्वयन पर **मार्गदर्शन प्रदान** करना।

संचालन संबंधी निरंतर जुड़ाव और समन्वित प्रतिक्रिया तंत्र के जरिए, सीईआरटी-इन साइबर घटनाओं को तेजी से नियंत्रित करना सुनिश्चित करता है और सभी क्षेत्रों में प्रभावित प्रणालियों को ठीक करने में मदद करता है। इसकी कार्रवाई योग्य खुफिया जानकारियों एवं मार्गदर्शन का निरंतर प्रवाह हितधारकों को तैयारियों को सुदृढ़ करने, प्रणालीगत जोखिम को कम करने और बदलते खतरों का प्रभावी ढंग से जवाब देने में सक्षम बनाता है।

संयुक्त रूप से, ये प्रयास व्यवधानों को कम करने, सामान्य स्थिति में लौटने में तेजी लाने और भारत के डिजिटल इकोसिस्टम में विश्वास को मजबूत करने में योगदान करते हैं।

भारत की साइबर सुदृढ़ता रणनीति के केंद्र में सीईआरटी-इन

सीईआरटी-इन खतरों की सक्रियता से पहचान, घटनाओं के विरुद्ध तेज प्रतिक्रिया और बड़े पैमाने पर क्षमता के विकास के जरिए भारत की राष्ट्रीय साइबर रक्षा संरचना का आधारस्तंभ बना हुआ है। वर्ष 2025 में इसकी उपलब्धियां संस्थागत मजबूती को बढ़ाने, जरूरी डिजिटल अवसंरचना को सुरक्षित करने और भारत के तेजी से बढ़ते डिजिटल इकोसिस्टम में विश्वास को मजबूत करने के इसके निरंतर एवं व्यवस्थित प्रयासों को दर्शाती हैं।

सीईआरटी-इन की 2025 की मुख्य उपलब्धियों का एक अवलोकन

1. राष्ट्रीय साइबर घटना के विरुद्ध प्रतिक्रिया एवं खतरे की खुफिया जानकारी

- वर्ष 2025 में, सीईआरटी-इन ने **29.44 लाख से अधिक साइबर घटनाओं को संभाला** और **1,530 चेतावनियां (अलर्ट), 390 भेद्यता संबंधी विवरण (वल्नरेबिलिटी नोट्स) एवं 65 परामर्शी (एडवाइजरी) जारी कीं**, जो बड़े पैमाने पर राष्ट्रीय साइबर प्रतिक्रिया क्षमता को दर्शाता है।
- सीईआरटी-इन द्वारा **29 साझा कमजोरियों एवं जोखिमों (सीवीई)** की पहचान की गई और उन्हें प्रकाशित किया गया।

2. साइबर सुरक्षा का मूल्यांकन

- सीईआरटी-इन ने सरकार, सार्वजनिक एवं निजी क्षेत्र के आईसीटी प्रणाली में साइबर सुरक्षा को मजबूत करने हेतु **231 प्रमाणित सुरक्षा मूल्यांकन संगठनों को पैनल में शामिल किया** है।
- इनमें से अधिकांश मूल्यांकन **बैंकिंग एवं वित्तीय संस्थानों, विद्युत एवं ऊर्जा और परिवहन क्षेत्र** में किए गए।

3. क्षमता विकास

- सीईआरटी-इन ने सरकार, पीएसयू और निजी क्षेत्र के हितधारकों के लिए **32 विशिष्ट तकनीकी प्रशिक्षण कार्यक्रम** और 95 साइबर सुरक्षा जागरूकता सत्र आयोजित किए।
- **विशिष्ट क्षमता विकास कार्यक्रमों के जरिए सरकार, पीएसयू और उद्योग जगत के 20,799 अधिकारियों और साइबर सुरक्षा पेशेवरों को प्रशिक्षण दिया गया।**

4. साइबर सुरक्षा ड्रिल और तैयारी अभ्यास

- सीईआरटी-इन ने **अलग-अलग जटिलताओं वाली 122 साइबर सुरक्षा ड्रिल और अभ्यास** कीं, जिसमें टेबलटॉप अभ्यास भी शामिल थीं। इनमें सरकार, सार्वजनिक और निजी क्षेत्रों (रक्षा, अर्द्धसैनिक बलों, अंतरिक्ष, परमाणु

ऊर्जा, दूरसंचार (आईएसपी), वित्त, विद्युत, तेल एवं प्राकृतिक गैस, परिवहन, आईटी/आईटीईएस क्षेत्र और राज्य डेटा सेंटर) के लगभग 1,570 संगठनों ने हिस्सा लिया।

5. जागरूकता संबंधी पहल

- सीईआरटी-इन ने **95 जागरूकता सत्र** आयोजित किए, जिनमें **91,065 प्रतिभागियों** [**राष्ट्रीय साइबर सुरक्षा जागरूकता माह (एनसीएसएएम) अक्टूबर 2025** सहित] ने हिस्सा लिया।

वर्ष 2025 में, सीईआरटी-इन ने **रिपोर्ट, श्वेत-पत्र, दिशा-निर्देश, परामर्शी और भेद्यता संबंधी विवरण (वल्नरेबिलिटी नोट्स)** का एक पूरा सेट भी प्रकाशित किया, जो संगठनों और हितधारकों को साइबर जोखिम को कम करने व मज़बूती बनाने के लिए समय पर तथा काम आने वाले मार्गदर्शन देता है।

वर्ष 2025 में प्रकाशित रिपोर्ट और दिशानिर्देश

- स्मार्ट सिटी अवसंरचना के लिए साइबर सुरक्षा दिशानिर्देश (फरवरी 2025)
- उपग्रह आधारित संचार के लिए साइबर सुरक्षा खतरों और सर्वोत्तम कार्यप्रणाली से संबंधित परामर्श (फरवरी 2025)
- भारत रैंसमवेयर रिपोर्ट (मार्च 2025)
- बीएफएसआई (बैंकिंग, वित्तीय सेवा एवं बीमा) क्षेत्र के लिए डिजिटल खतरा रिपोर्ट 2024 (अप्रैल 2025)
- "साइबर सुरक्षा खतरों से मानवरहित विमान प्रणालियों (यूएएस) की सुरक्षा के लिए अच्छी कार्यप्रणाली" पर श्वेत पत्र (अप्रैल 2025)
- एसबीओएम (सॉफ्टवेयर बिल ऑफ मटीरियल्स), क्यूबीओएम तथा सीबीओएम (क्वांटम बिल ऑफ मटीरियल्स और क्रिप्टोग्राफिक बिल ऑफ मटीरियल्स), एचबीओएम (हार्डवेयर बिल ऑफ मटीरियल), एआईबीओएम (आर्टिफिशियल इंटेलिजेंस बिल ऑफ मटीरियल्स) संस्करण 2 से संबंधित तकनीकी दिशानिर्देश (जुलाई 2025)
- व्यापक साइबर सुरक्षा मूल्यांकन नीति दिशानिर्देश (जुलाई 2025)
- क्वांटम साइबर तैयारी की दिशा में बदलाव पर श्वेत पत्र (जुलाई 2025)
- सूक्ष्म, लघु एवं मध्यम उद्यमों (एमएसएमई) के लिए 15 मौलिक साइबर रक्षा नियंत्रण - (सितंबर 2025)
- एनसीएसएएम अक्टूबर 2025 के दौरान, एक "साइबर स्मार्ट किड्स: सुरक्षा गाइड" प्रकाशित किया गया।
- वरिष्ठ नागरिकों के लिए साइबर सुरक्षा संबंधी उत्कृष्ट कार्यपणालियां - पुस्तिका।

वर्ष 2025 में सीईआरटी-इन की उपलब्धियां भारत के तेजी से बढ़ते डिजिटल इकोसिस्टम की सुरक्षा में उसकी अहम भूमिका को दर्शाती हैं। बड़े पैमाने पर क्षमता विकास, सख्त मूल्यांकन, जागरूकता की निरंतर कोशिशों और भविष्योन्मुखी दिशा-निर्देश एवं तकनीकी रूपरेखा जारी करके, सीईआरटी-इन ने सरकार, उद्योग जगत और समाज में संस्थागत तैयारियों को मजबूत किया है।

सीईआरटी-इन द्वारा समर्थित संस्थागत ढांचे

राष्ट्रीय साइबर सुरक्षा नीति को लागू करने और रणनीतिक इरादों को जमीनी कार्रवाई में बदलने हेतु, सीईआरटी-इन कुछ खास संस्थागत ढांचे को संभालता है। ये तंत्र सभी क्षेत्रों, राज्यों और नागरिकों के बीच व्यवस्थित समन्वय, बचाव के उपाय और तेजी से प्रतिक्रिया करने की क्षमता प्रदान करते हैं।

1. **साइबर स्वच्छता केन्द्र (सीएसके)** सीएसके (बॉटनेट क्लीनिंग और मैलवेयर एनालिसिस सेंटर) को सीईआरटी-इन ने नागरिकों के बीच साइबर स्वच्छता को बेहतर बनाने के उद्देश्य से स्थापित किया है। यह केन्द्र कंप्यूटर, मोबाइल फोन, आईओटी डिवाइस और होम राउटर जैसे इंटरनेट से जुड़े उन उपकरणों के नेटवर्क की निगरानी करता है, जो मैलवेयर से संक्रमित हैं। यह उपयोगकर्ताओं को संक्रमित उपकरण को साफ करने में मदद करने के लिए मुफ्त टूल एवं मार्गदर्शन देता है और छेड़छाड़ की गई प्रणाली की पहचान करने और उपयोगकर्ताओं को सतर्क करने हेतु उद्योग जगत, अकादमिक जगत और इंटरनेट सेवा प्रदाताओं के साथ मिलकर काम करता है। नियमित जागरूकता अभियान सुरक्षित ऑनलाइन व्यवहार और जिम्मेदार डिजिटल तरीकों को बढ़ावा देते हैं।

दिसंबर 2025 तक, सीएसके भारत की 98 प्रतिशत डिजिटल आबादी को कवर करता है और बॉटनेट एवं मैलवेयर संक्रमण के बारे में बड़े पैमाने पर नोटिफिकेशन भेजता है। यह प्रमुख क्षेत्रों के 1,427 संगठनों के साथ मिलकर मैलवेयर का पता लगाने और उसे ठीक करने में मदद करता है, जबकि इसके फ्री बॉटनेट-रिमूवल टूल्स के 89.55 लाख डाउनलोड एक नागरिक-केन्द्रित निवारक साइबर सुरक्षा पहल के रूप में इसकी भूमिका को दर्शाते हैं।

2. सुरक्षा आश्वासन ढांचा सीईआरटी-इन सरकारी और महत्वपूर्ण क्षेत्रों की प्रणालियों की सुरक्षा को मजबूत करने हेतु एक सुरक्षा आश्वासन ढांचे को संचालित करता है। इस ढांचे के तहत; प्रमाणित आईटी सुरक्षा मूल्यांकन संगठन नियमित रूप से मूल्यांकन करते हैं; भेद्यता आकलन (वल्नरेबिलिटी असेसमेंट) और भेदन परीक्षण (पेनिट्रेशन टेस्टिंग) की जाती है; और आम कमज़ोरियों की पहचान करने के लिए मूल्यांकन के नतीजों का विश्लेषण किया जाता है। इन जानकारियों के आधार पर, सीईआरटी-इन सुरक्षित डिजाइन संबंधी दिशा निर्देश जारी करता है और उत्कृष्ट कार्यप्रणालियों को बढ़ावा देता है। इस ढांचे के तहत नियमित मूल्यांकन सभी क्षेत्र की साइबर तैयारी और मज़बूती को काफी बढ़ाते हैं।

3. राष्ट्रीय साइबर समन्वय केन्द्र (एनसीसीसी) एनसीसीसी, जिसे सीईआरटी-इन ने लागू किया है, स्थिति के अनुसार जागरूकता के लिए संभावित साइबर सुरक्षा के खतरों का पता लगाने हेतु मेटाडेटा स्तर पर साइबरस्पेस की निगरानी करता है। यह संबंधित संगठनों, राज्य सरकारों और अन्य हितधारकों के साथ वास्तविक समय में जानकारी साझा करने में मदद करता है, जिससे समय रहते बचाव और जवाबी कार्रवाई की जा सके।

4. कंप्यूटर सिक्योरिटी इंसिडेंट रिस्पॉन्स टीम्स (सीएसआईआरटी) सीईआरटी-इन विभिन्न क्षेत्रों और राज्य/केन्द्र-शासित प्रदेशों के स्तर पर काम करने वाली सीएसआईआरटी के नेटवर्क की देखरेख करता है। क्षेत्र विशेष से संबंधित सीएसआईआरटी वित्त, विद्युत और दूरसंचार जैसे डोमेन को सपोर्ट करती हैं, जबकि राज्य सीएसआईआरटी संबंधित राज्य और केन्द्र-शासित प्रदेश सरकारों के तहत काम करती हैं।

5. साइबर संकट प्रबंधन योजना (सीसीएमपी) सीईआरटी-इन ने सरकारी संस्थाओं के लिए एक सीसीएमपी भी बनाया है, जो बड़े साइबर हमलों और साइबर-आतंकवाद की घटनाओं के दौरान व्यवस्थित मार्गदर्शन देता है। यह योजना खासकर महत्वपूर्ण अवसंरचना के लिए तेजी से प्रतिक्रिया, रिकवरी और जरूरी सेवाओं की निरंतरता को समर्थन प्रदान करती है।

कुल मिलाकर, ये संस्थागत ढांचे साइबर सुरक्षा के लिए संपूर्ण सरकार एवं संपूर्ण समाज वाले दृष्टिकोण को संभव बनाते हैं। रोकथाम, तैयारी, प्रतिक्रिया और रिकवरी को एकीकृत करके। यह बदलते साइबर खतरों के बीच भारत के डिजिटल इकोसिस्टम का सुदृढ़, अनुकूल और सुरक्षित बना रहना सुनिश्चित करता है। विभिन्न परतों वाला यह संस्थागत डिजाइन राष्ट्रीय तैयारियों को मजबूत करने के साथ-साथ महत्वपूर्ण अवसंरचनाओं तथा नागरिकों, दोनों की सुरक्षा भी करता है।

साइबर सुरक्षा के क्षेत्र में भारत के नेतृत्व को वैश्विक मान्यता

घरेलू मोर्चे पर सीईआरटी-इन की निरंतर कोशिशों का प्रभाव अब वैश्विक स्तर पर भी दिख रहा है। इसके संचालन के पैमाने, तकनीक-आधारित तरीके और सहयोगी साइबर शासन पर जोर ने भारत को अंतरराष्ट्रीय साइबर सुरक्षा व्यवस्था में एक भरोसेमंद एवं जिम्मेदार हिस्सेदार के तौर पर स्थापित किया है।

- **विश्व आर्थिक मंच (डब्ल्यूईएफ)** द्वारा प्रकाशित *ग्लोबल साइबरसिक्योरिटी आउटलुक 2025* में, सीईआरटी-इन के योगदान को दुर्भावनापूर्ण डोमेन तथा फिशिंग गतिविधियों का आकलन एवं पता लगाने के लिए एआई-संचालित स्थिति के अनुरूप जागरूकता प्रणाली को तैनात करने के साथ-साथ वैश्विक स्तर पर खतरों की खुफिया जानकारी को वास्तविक समय में साझा करने के लिए रेखांकित किया गया है।

- अप्रैल 2025 में, सीईआरटी-इन ने **डब्ल्यूईएफ और ऑक्सफोर्ड यूनिवर्सिटी** द्वारा संयुक्त रूप से प्रकाशित किए गए *साइबर रेजिलिएंस कम्पास* शीर्षक शोध-पत्र में योगदान दिया, जिसमें साइबर सुदृढ़ता के सात जरूरी क्षेत्रों की पहचान की गई थी।

- फरवरी 2025 में, सीईआरटी-इन उन अंतरराष्ट्रीय साझेदारों में से एक था जिन्होंने फ्रांस की राष्ट्रीय साइबर सुरक्षा एजेंसी (एएनएसएसआई) द्वारा प्रकाशित आर्टिफिशियल इंटेलिजेंस पर "बिल्डिंग ट्रस्ट इन एआई थ्रू ए साइबर-रिस्क-बेस्ड अप्रोच" शीर्षक संयुक्त उच्चस्तरीय जोखिम आकलन रिपोर्ट पर हस्ताक्षर किए। यह रिपोर्ट भरोसेमंद एआई प्रणाली को समर्थ करने, एआई मूल्य श्रृंखला को सुरक्षित करने और एआई से जुड़े उभरते साइबर जोखिमों से निपटने हेतु जोखिम-आधारित दृष्टिकोण की हिमायत करती है।

कुल मिलाकर, ये मान्यताएं वैश्विक साइबर सुरक्षा और एआई संबंधी जोखिम के प्रशासन को आकार देने में सीईआरटी-इन के बढ़ते प्रभाव एवं नेतृत्व को दर्शाती हैं। ये साइबर सुदृढ़ता, खतरों से जुड़ी खुफिया जानकारियों के साझाकरण और एआई संबंधी जोखिम के जिम्मेदार प्रशासन से संबंधित वैश्विक चर्चाओं को आकार देने में सीईआरटी-इन की उभरती भूमिका को रेखांकित करती हैं।

निष्कर्ष

साइबर खतरों की बढ़ती जटिलता और पैमाने के बीच, सीईआरटी-इन भारत के साइबर सुरक्षा इकोसिस्टम को मजबूती प्रदान कर रहा है। साइबर जोखिमों की निरंतर पहचान करके व उन्हें कम करके, सीईआरटी-इन ने

राष्ट्रीय साइबर सुदृढ़ता को काफी मजबूत किया है। संस्थागत ढांचे और क्षेत्र-विशिष्ट एवं राज्य सीएसआईआरटी से लेकर नागरिक-केन्द्रित जागरूकता कार्यक्रमों तक, इसकी विभिन्न पहलें भारत की आईसीटी अवसंरचना को सुरक्षित करने और उपयोगकर्ताओं की सुरक्षा हेतु एक व्यापक एवं दूरदर्शी दृष्टिकोण का प्रदर्शन करती हैं। सीईआरटी-इन के एआई-आधारित नवाचारों को अंतरराष्ट्रीय पहचान मिलना साइबर सुरक्षा के क्षेत्र में भारत के नेतृत्व को और भी मजबूत करता है। कुल मिलाकर, ये निरंतर प्रयास साइबरस्पेस की सुरक्षा करने और सभी नागरिकों के लिए एक सुरक्षित, भरोसेमंद एवं सुरक्षित डिजिटल भविष्य सुनिश्चित करने के प्रति भारत सरकार की प्रतिबद्धता की पुष्टि करते हैं।

संदर्भ

इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय

- https://www.cert-in.org.in/
- https://www.cert-in.org.in/- Annual Report 2024
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2203387&reg=3&lang=1
- https://www.csk.gov.in/about.html
- https://www.cert-in.org.in/CSIRT.jsp
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2148943&reg=3&lang=2
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2109192&reg=3&lang=2
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2026677&reg=3&lang=2
- https://www.pib.gov.in/Pressreleaseshare.aspx?PRID=2115416&reg=3&lang=2
- UPI: https://www.npci.org.in/product/upi/product-statistics
- IMPS: https://www.npci.org.in/product/imps/product-statistics
- NETC: https://www.npci.org.in/product/netc/product-statistics
- DigiLocker: https://www.digilocker.gov.in/web/statistics
- https://www.cert-in.org.in/PDF/Guidelines_for_Smart_City_Infrastructure.pdf
- https://www.cert-in.org.in/PDF/RANSOMWARE_Report_2024.pdf
- https://www.cert-in.org.in/PDF/Digital_Threat_Report_2024.pdf
- https://www.cert-in.org.in/PDF/CIWP-2025-0001.pdf
- https://www.cert-in.org.in/PDF/TechnicalGuidelines-on-SBOM,QBOM&CBOM,AIBOM_and_HBOM_ver2.0.pdf
- https://www.cert-in.org.in/ (Guidelines)
- https://www.pib.gov.in/PressReleaseIframePage.aspx?PRID=2144023&reg=3&lang=2
- https://www.cert-in.org.in/PDF/Elemental_Cyber_Defense_Controls_for_MSME.pdf

दूरसंचार मंत्रालय

- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2057035&reg=3&lang=2
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2198285&reg=3&lang=2

गृह मंत्रालय

- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2197529&reg=3&lang=2

पीआईबी मुख्यालय:

- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2176146&reg=3&lang=2
- https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=156294&ModuleId=3&reg=3&lang=1
- https://www.pib.gov.in/PressNoteDetails.aspx?ModuleId=3&NoteId=154788&reg=3&lang=1
- https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=154912&ModuleId=3&reg=3&lang=1
- https://www.pib.gov.in/PressReleasePage.aspx?PRID=2206477&reg=3&lang=1

द420.इन

- https://the420.in/cert-in-ai-praised-world-economic-forum-cyber-fraud-report

पीआईबी शोध

पीके/केसी/आर