# साइबर अपराध

## प्रिलिम्स के लिये:

साइबर अपराध, संविधान की सातवीं अनुसूची, इंटरनेट ऑफ थिंग्स, क्रिप्टो-करेंसी, बड़े पैमाने पर ओपन ऑनलाइन पाठ्यक्रम

## मेन्स के लिये:

साइबर अपराध, संबंधित चुनौतियाँ और उससे निपटने के उपाय

## चर्चा में क्यों?

भारत सरकार ने साइबर अपराधों से व्यापक और समन्वित तरीके से निपटने के लिये सिस्टम को मज़बूत करने हेतु महत्त्वपूर्ण कदम उठाए हैं।

## साइबर अपराध:

- **परिचय:**
    - साइबर अपराध को ऐसे अपराध के रूप में परिभाषित किया जाता है जहाँ **कंप्यूटर अपराध का माध्यम होता है या अपराध करने के लिये एक उपकरण** के रूप में प्रयोग किया जाता है।
    - भारतीय संविधान की सातवीं अनुसूची के अनुसार, साइबर अपराध राज्य सूची के अंतर्गत आता है।
    - इसमें अवैध या अनधिकृत गतिविधियाँ शामिल हैं जो **विभिन्न प्रकार के अपराध करने के लिये प्रौद्योगिकी का लाभ उठा**ती हैं।
    - साइबर अपराध में अपराधों की एक विस्तृत शृंखला शामिल है, यह व्यक्तियों, संगठनों के साथ-साथ सरकारों को भी प्रभावित कर सकता है।
- **प्रकार:**
    - **डिस्ट्रीब्यूटेड डिनायल-ऑफ-सर्विस (DDoS) अटैक:** इसका प्रयोग किसी ऑनलाइन सेवा को अनुपलब्ध बनाने और विभिन्न स्रोतों से वेबसाइट पर अत्यधिक ट्रैफिक के माध्यम से नेटवर्क को बाधित करने के लिये किया जाता है।
    - **बॉटनेट:** यह **कंप्यूटर** का एक ऐसा नेटवर्क है जिसे **दूर बैठे हैकर्स द्वारा** बाह्य रूप से **नियंत्रित किया जाता** है। रिमोट हैकर्स या तो स्पैम भेजते हैं या इन बॉटनेट के माध्यम से अन्य कंप्यूटरों पर हमला करते हैं।
    - **पहचान की चोरी (Identity Theft):** यह साइबर अपराध तब होता है **जब कोई अपराधी किसी उपयोगकर्ता की व्यक्तिगत** या गोपनीय जानकारी **तक पहुँच प्राप्त** कर लेता है, जिसके परिणामस्वरूप वह प्रतिष्ठा धूमिल करने या फिरौती मांगने की कोशिश करता है।
    - **साइबर स्टॉकिंग:** इस प्रकार के साइबर अपराध में **ऑनलाइन उत्पीड़न शामिल होता है जहाँ उपयोगकर्ता को ढेर सारे ऑनलाइन संदेशों** और ईमेल का सामना करना पड़ता है। सामान्यतः साइबर स्टॉक किसी उपयोगकर्ता को डराने के लिये सोशल मीडिया, वेबसाइट और सर्च इंजन का उपयोग करते हैं।
    - **फिशिंग:** यह एक प्रकार का **सोशल इंजीनियरिंग हमला** है जिसका उपयोग अक्सर उपयोगकर्ता का डेटा चुराने के लिये किया जाता है, जिसमें लॉगिन क्रेडेंशियल और क्रेडिट कार्ड नंबर शामिल हैं। ऐसा तब होता है जब एक **हमलावर एक विश्वसनीय संस्था के रूप में** किसी पीड़ित को ईमेल, त्वरित संदेश या टेक्स्ट संदेश के माध्यम से धोखा देता है।

## भारत में साइबर सुरक्षा से संबंधित चुनौतियाँ:

- **लाभ-उन्मुख अवसंरचना की मानसिकता:**
    - उदारीकरण के बाद से सूचना प्रौद्योगिकी (IT), बिजली और दूरसंचार क्षेत्र में निजी क्षेत्र द्वारा वृहत निवेश किया गया है।
    - ऑपरेटर सुरक्षात्मक बुनियादी ढाँचे में निवेश नहीं कर रहे हैं, बल्कि वे **केवल लाभदायक बुनियादी ढाँचे पर ध्यान केंद्रित कर रहे हैं,** क्योंकि उन्हें लगता है कि **साइबर हमले की तैयारियों पर निवेश से अच्छा मुनाफा** नहीं हो सकता है।
    - सभी ऑपरेटर लाभ पर अधिक केंद्रित हैं और **अवसंरचना में निवेश नहीं करना चाहते क्योंकि वहाँ उनके लिये लाभ के अवसर नहीं** हैं।
- **पृथक प्रक्रियात्मक संहिता का अभाव:**
    - साइबर या कंप्यूटर संबंधी अपराधों की जाँच के लिये कोई **पृथक प्रक्रियात्मक संहिता** मौजूद नहीं है।
- **साइबर हमलों की अंतर्राष्ट्रीय (ट्रांस-नेशनल) प्रकृति:**

    - अधिकांश साइबर अपराध प्रकृति में **ट्रांस-नेशनल** होते हैं। विदेशी क्षेत्रों से साक्ष्य एकत्र करना न केवल कठिन बल्कि एक धीमी प्रक्रिया भी है।
- **डिजिटल पारितंत्र का विस्तार:**
    - पिछले कुछ वर्षों में भारत अपने **विभिन्न आर्थिक घटकों** के डिजिटलीकरण के मार्ग पर आगे बढ़ा है और इसने इस क्षेत्र में सफलतापूर्वक अपना स्थान बनाया है।
    - **5G और इंटरनेट ऑफ थिंग्स** जैसी नवीनतम प्रौद्योगिकियाँ इंटरनेट से जुड़े पारितंत्र के कवरेज में वृद्धि करेंगी।
    - डिजिटलीकरण के आगमन के साथ उपभोक्ता एवं नागरिक डेटा को डिजिटल प्रारूप में संग्रहीत किया जाएगा और लेन-देन ऑनलाइन माध्यम से संपन्न होगा, **जो भारत को हैकर्स तथा साइबर अपराधियों के लिये एक सक्षम ब्रीडिंग ग्राउंड बना सकता** है।
- **सीमित विशेषज्ञता और प्राधिकार:**
    - **क्रिप्टोकरेंसी** से संबंधित अपराधों की **कम रिपोर्टिंग** की जाती है क्योंकि ऐसे अपराधों को हल करने की क्षमता सीमित रहती है।
    - यद्यपि अधिकांश राज्य स्तरीय साइबर लैब हार्ड डिस्क और मोबाइल फोन का विश्लेषण करने में सक्षम हैं,**फिर भी उन्हें केंद्र सरकार द्वारा 'इलेक्ट्रॉनिक साक्ष्य के परीक्षक' (Examiners of Electronic Evidence) के रूप में मान्यता दिया जाना अभी शेष है।** जब तक उन्हें मान्यता प्राप्त नहीं प्राप्त होगी, वे इलेक्ट्रॉनिक डेटा पर विशेषज्ञ राय नहीं दे सकते।

## भारत में साइबर अपराधों से निपटने के लिये किये जाने वाले उपाय:

- **साइबर सुरक्षा जागरूकता अभियान:**
    - सरकारों को विभिन्न स्तरों पर **साइबर धोखाधड़ी** के संबंध में बड़े पैमाने पर साइबर सुरक्षा जागरूकता अभियान चलाने, मज़बूत, अद्वितीय पासवर्ड एवं **सार्वजनिक वाई-फाई का उपयोग** करने आदि में सावधानी बरतने की आवश्यकता है।
- **साइबर बीमा:**
    - ऐसी साइबर बीमा पॉलिसियाँ विकसित की जानी चाहिये जो **विभिन्न व्यवसायों** और उद्योगों **की विशिष्ट आवश्यकताओं के अनुरूप हों।** अनुकूलित नीतियाँ यह सुनिश्चित करने में सहायता करेंगी कि संगठनों के पास **उनके सामने आने वाले सबसे प्रासंगिक साइबर जोखिमों** के लिये कवरेज है।
        - **साइबर बीमा** साइबर घटनाओं से होने वाले नुकसान के खिलाफ वित्तीय कवरेज प्रदान करता है तथा इन घटनाओं के **वित्तीय प्रभाव को कम करके** संगठन **अधिक तेज़ी से सुचारु रूप से अपना संचालन जारी रख सकते हैं।**
- **डेटा संरक्षण कानून:**
    - डेटा को नई मुद्रा कहा जाता है, इसलिये भारत में **एक सख्त डेटा सुरक्षा व्यवस्था** की आवश्यकता है।
        - इस संदर्भ में **यूरोपीय संघ का सामान्य डेटा संरक्षण विनियमन** और भारत का व्यक्तिगत डेटा संरक्षण विधेयक, 2019 सही दिशा में उठाए गए कदम हैं।
- **सहयोगात्मक त्वरित प्रतिक्रिया तंत्र:**
    - भारत जैसे देश में जहाँ **नागरिक** साइबर अपराध के प्रति **अधिक संवेदनशील हैं,** एक सहयोगात्मक त्वरित प्रतिक्रिया तंत्र की आवश्यकता है।
        - यह तंत्र सभी पक्षों को संगठित करेगा तथा कानून लागू करने वालों को त्वरित कार्रवाई करने तथा नागरिकों एवं व्यवसायों को तेज़ी से बढ़ते खतरे से बचाने में सक्षम बनाएगा।
        - इस संदर्भ में भारतीय **साइबर अपराध समन्वय केंद्र साइबर सुरक्षा जाँच को केंद्रीकृत करने,** प्रतिक्रिया उपकरणों के विकास को प्राथमिकता देने तथा इस खतरे को रोकने के लिये निजी कंपनियों को एक साथ लाने में **सहायता करेगा।**

## भारत में साइबर अपराधों से निपटने हेतु सरकार की पहल:

- **भारतीय साइबर अपराध समन्वय केंद्र (I4C):** यह केंद्र पूरे देश में सभी प्रकार के साइबर अपराधों से निपटने के प्रयासों का समन्वय करता है।
- **राष्ट्रीय साइबर फोरेंसिक प्रयोगशाला:** यह ऑनलाइन तथा ऑफलाइन दोनों तरीकों से सभी राज्य/केंद्रशासित प्रदेश पुलिस के जाँच अधिकारियों को प्रारंभिक चरण की साइबर फोरेंसिक सहायता प्रदान करती है।
- **साइट्रेन पोर्टल (CyTrain Portal):** साइबर अपराध जाँच, फोरेंसिक और अभियोजन के महत्त्वपूर्ण पहलुओं पर ऑनलाइन पाठ्यक्रमों के माध्यम से पुलिस अधिकारियों, न्यायिक अधिकारियों तथा अभियोजकों की क्षमता निर्माण हेतु एक **विशाल ओपन ऑनलाइन पाठ्यक्रम (MOOC)** मंच।
- **राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल:** एक ऐसा मंच जहाँ जनता साइबर अपराध की घटनाओं की रिपोर्ट कर सकती है, जिसमें **महिलाओं एवं बच्चों के प्रति अपराधों** पर विशेष ध्यान दिया जाता है।
- **नागरिक वित्तीय साइबर फ्रॉड रिपोर्टिंग और प्रबंधन प्रणाली:** यह **वित्तीय धोखाधड़ी की तत्काल रिपोर्टिंग** और टोल-फ्री हेल्पलाइन के माध्यम से ऑनलाइन साइबर शिकायतें दर्ज करने में सहायता हेतु एक **प्रणाली** है।
- **महिलाओं एवं बच्चों के प्रति साइबर अपराध निवारण (CCPWC) योजना:** साइबर अपराधों की जाँच में **कानून प्रवर्तन एजेंसियों की क्षमताओं को विकसित करने के लिये** राज्यों/केंद्रशासित प्रदेशों को वित्तीय सहायता प्रदान की जाती है।
- **संयुक्त साइबर समन्वय दल:** राज्यों/केंद्रशासित प्रदेशों की कानून प्रवर्तन एजेंसियों के बीच, विशेष रूप से साइबर-अपराधों से संबंधित बहु-क्षेत्राधिकार वाले क्षेत्रों में समन्वय बढ़ाने के लिये इस दल का गठन करना।
- **पुलिस के आधुनिकीकरण के लिये केंद्रीय सहायता: आधुनिक हथियार, उन्नत संचार/फोरेंसिक** उपकरण तथा साइबर पुलिसिंग उपकरण प्राप्त करने के लिये राज्यों/केंद्रशासित प्रदेशों को वित्तीय सहायता प्रदान करना।

## निष्कर्ष

- सूचना साझा करने तथा साइबर सुरक्षा अनुसंधान एवं विकास में संयुक्त प्रयासों को मज़बूत कर वैश्विक सहयोग सुनिश्चित करना आवश्यक है क्योंकि अधिकांश साइबर हमले सीमाओं के पार से होते हैं।
- कॉरपोरेट्स या **संबंधित सरकारी विभागों के लिये** यह महत्त्वपूर्ण है कि वे **अपने संगठनों में कमियों का पता लगाएँ** और उन कमियों को दूर करें तथा एक स्तरित सुरक्षा प्रणाली बनाएँ जिसमें विभिन्न स्तर पर सुरक्षा खतरे की खुफिया जानकारी साझा की जा सके।

## स्रोत: पी.आई.बी.

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/cyber-crime-4