

साइबर क्राइम: एक समाजशास्त्रीय अध्ययन

GAJENDRA KUMAR MALVIYA

H.O.D, DEPT. OF SOCIOLOGY, GOVT. PG COLLEGE, JHALAWAR, RAJASTHAN

सार

साइबर अपराध एक ऐसा अपराध है जिस में कंप्यूटर और नेटवर्क शामिल है। किसी भी कंप्यूटर का अपराधिक स्थान पर मिलना या कंप्यूटर से कोई अपराध करना कंप्यूटर अपराध कहलाता है। कंप्यूटर अपराध में नेटवर्क शामिल नहीं होता है। किसी कि निजी जानकारी को प्राप्त करना और उसका गलत इस्तेमाल करना। किसी की भी निजी जानकारी कंप्यूटर से निकाल लेना या चोरी कर लेना भी साइबर अपराध है। कंप्यूटर अपराध भी कई प्रकार से किये जाते हैं जैसे कि जानकारी चोरी करना, जानकारी मिटाना, जानकारी में फेर बदल करना, किसी कि जानकारी को किसी और को देना या कंप्यूटर के भागो को चोरी करना या नष्ट करना। साइबर अपराध भी कई प्रकार के हैं जैसे कि स्पैम ईमेल, हैकिंग, फिशिंग, वायरस को डालना, किसी की जानकारी को ऑनलाइन प्राप्त करना या किसी पर हर वक्त नजर रखना।

कंप्यूटर अपराध के प्रकार

परिचय

जानकारी चोरी करना- किसी के भी कंप्यूटर से उसकी निजी जानकारी निकालना जैसे की उपयोगकर्ता का नाम या पासवर्ड।

जानकारी मिटाना- किसी के कंप्यूटर से जानकारी मिटाना ताकी उसे नुकसान हो या कोई जरूरी जानकारी को मिटाना।

फेर बदल करना- जानकारी मे कुछ हटाना या जोड़ना उस जानकारी को बदल देना।

बाहरी नुकसान- भागो को नष्ट करना, उसे तोड़ना या भागो की चोरी करना भी कंप्यूटर अपराध में आता है।

साइबर अपराध के प्रकार [1,2,3]

स्पैम ईमेल- अनेक प्रकार के ईमेल आते हैं जिसमें ऐसे ईमेल भी होते हैं जो सिर्फ कंप्यूटर को नुकसान पहुंचाते हैं। उन ईमेल से सारे कंप्यूटर में खराबी आ जाती हैं। हैकिंग- किसी की भी निजी जानकारी को हैक करना जैसे की उपयोगकर्ता नाम या पासवर्ड और फिर उसमें फेर बदल करना।

साइबरफिशिंग- किसी के पास स्पैम ईमेल भेजना ताकी वो अपनी निजी जानकारी दे और उस जानकारी से उसका नुकसान हो सके। यह ईमेल आकर्षित होते हैं।

वायरस फैलाना -साइबर अपराधी कुछ ऐसे सॉफ्टवेयर आपके कम्प्युटर पर भेजते हैं जिसमें वायरस छिपे हो सकते हैं, इनमें वायरस, वर्ग, टार्जन हॉर्स, लॉजिक हॉर्स आदि वायरस शामिल हैं, यह आपके कंप्यूटर को काफी हानि पहुंचा सकते हैं।

सॉफ्टवेयर पाइरेसी - सॉफ्टवेयर की नकल तैयार कर सस्ते दामों में बेचना भी साइबर क्राइम के अन्तर्गत आता है, इससे सॉफ्टवेयर कम्पनियों को भारी नुकसान उठाना पड़ता है साथ ही साथ आपके कीमती उपकरण भी ठीक से काम नहीं करते हैं।

फर्जी बैंक कॉल- आपको जाली ईमेल, मैसेज या फोन कॉल प्राप्त हो जो आपकी बैंक जैसा लगे जिसमें आपसे पूछा जाये कि आपके एटीएम नंबर और पासवर्ड की आवश्यकता है और यदि आपके द्वारा यह जानकारी नहीं दी गयी तो आपको खाता बन्द कर दिया जायेगा या इस लिंक पर सूचना दें। याद रखें किसी भी बैंक द्वारा ऐसी जानकारी कभी भी इस तरह से नहीं माँगी जाती है और भूलकर भी अपनी किसी भी इस प्रकार की जानकारी को इंटरनेट या फोनकॉल या मैसेज के माध्यम से नहीं बताये।

सोशल नेटवर्किंग साइटों पर अफवाह फैलाना बहुत से लोग सोशल नेटवर्किंग साइटों पर सामाजिक, वैचारिक, धार्मिक और राजनैतिक अफवाह फैलाने का काम करते हैं, लेकिन यूजर्स उनके इरादें समझ नहीं पाते हैं और जाने-अनजाने में ऐसे लिंक्स को शेयर करते रहते हैं, लेकिन यह भी साइबर अपराध और साइबर-आतंकवाद की श्रेणी में आता है।

साइबर बुलिंग - फेसबुक जैसी सोशल नेटवर्किंग पर अशोभनीय कमेंट करना, इंटरनेट पर धमकियाँ देना किसी का इस स्तर तक मजाक बनाना कि तंग हो जाये, इंटरनेट पर दूसरों के सामने शर्मिंदा करना, इसे साइबर बुलिंग कहते हैं। अक्सर बच्चे इसका शिकार हाते हैं। इससे इनके सेहत पर भी असर पड़ता है [4,5,6]

विश्लेषण

जब भी अपराध होता है, अपराधी कितना भी होशियार क्यों न हो फिर भी कोई न कोई सबूत छोड़ देता है।

कंप्यूटर पर आने वाले स्पैम ईमेल में कोई न कोई वर्तनी में गलती मिल जाएगी। मूल ईमेल में ऐसी गलती कभी नहीं मिलेगी। सूचना तकनीक कानून, 2000 के अंतर्गत साइबरस्पेस में क्षेत्राधिकार संबंधी प्रावधान

मानव समाज के विकास के नज़रिए से सूचना और संचार तकनीकों की खोज को बीसवीं शताब्दी का सबसे महत्वपूर्ण अविष्कार माना जा सकता है। सामाजिक विकास के विभिन्न क्षेत्रों, खासकर न्यायिक प्रक्रिया में इसके इस्तेमाल की महत्ता को कम करके नहीं आंका जा सकता, क्योंकि इसकी तेज गति छोटी-मोठी दिक्कतों से छुटकारा, मानवीय गलतियों की कमी, कम खर्चीला होना जैसे गुणों के चलते यह न्यायिक प्रक्रिया को विश्वसनीय बनाने में अहम भूमिका निभा सकती है। इतना ही नहीं, ऐसे मामलों के निष्पादन में, जहां सभी संबंध पक्षों की शारीरिक उपस्थिति अनिवार्य न हो, यह सर्वश्रेष्ठ विकल्प सिद्ध हो सकता है। सूचना तकनीक कानून के अंतर्गत उल्लिखित आरोपों की सूची निम्नवत है।

कंप्यूटर संसाधनों से छेड़छाड़ की कोशिश-धारा 65

कंप्यूटर में संग्रहित डाटा के साथ छेड़छाड़ कर उसे हैक करने की कोशिश-धारा 66

संवाद सेवाओं के माध्यम से प्रतिबंधित सूचनाएं भेजने के लिए दंड का प्रावधान-धारा 66 ए

कंप्यूटर या अन्य किसी इलेक्ट्रॉनिक गैजेट से चोरी की गई सूचनाओं को ग़लत तरीके से हासिल करने के लिए दंड का प्रावधान-धारा 66 बी

किसी की पहचान चोरी करने के लिए दंड का प्रावधान-धारा 66 सी

अपनी पहचान छुपाकर कंप्यूटर की मदद से किसी के व्यक्तिगत डाटा तक पहुंच बनाने के लिए दंड का

प्रावधान- धारा 66 डी

किसी की निजता भंग करने के लिए दंड का प्रावधान-धारा 66 द

साइबर आतंकवाद के लिए दंड का प्रावधान-धारा 66 एफ

आपत्तिजनक सूचनाओं के प्रकाशन से जुड़े प्रावधान-धारा 67

इलेक्ट्रॉनिक माध्यमों से सेक्स एवं अश्लील सूचनाओं को प्रकाशित या प्रसारित करने के लिए दंड का प्रावधान-धारा 67 ए

इलेक्ट्रॉनिक माध्यमों से ऐसी आपत्तिजनक सामग्री का प्रकाशन या प्रसारण, जिसमें बच्चों को अधीत अवस्था में दिखाया गया हो-धारा 67 वी [7,8,9]

मध्यस्थों द्वारा सूचनाओं को बाधित करने या रोकने के लिए दंड का प्रावधान-धारा 67 ती

सुरक्षित कंप्यूटर तक अनाधिकार पहुंच बनाने से संबंधित प्रावधान-धारा 70

डाटा या आंकड़ों को ग़लत तरीके से पेश करना-धारा आपसी विश्वास और निजता को भंग करने से संबंधित प्रावधान-धारा 72 ए

कॉन्ट्रैक्ट की शर्तों का उल्लंघन कर सूचनाओं को सार्वजनिक करने से संबंधित प्रावधान-धारा 72 ए

फर्जी डिजिटल हस्ताक्षर का प्रकाशन-धारा 73

सूचना तकनीक कानून की धारा 78 में इंस्पेक्टर स्तर के पुलिस अधिकारी को इन मामलों में जांच का अधिकार हासिल है।

भारतीय दण्ड संहिता (आईपीसी) में साइबर अपराधों से संबंधित प्रावधान

ईमेल के माध्यम से धमकी भरे संदेश भेजना-आईपीसी की धारा 503

ईमेल के माध्यम से ऐसे संदेश भेजना, जिससे मानहानि होती हो-आईपीसी की धारा 499

फर्जी इलेक्ट्रॉनिक रिकॉर्ड्स का इस्तेमाल आईपीसी की धारा 165

फर्जी वेवसाइट्स या साइबर फ़ॉड आईपीसी की धारा 420

चोरी-छुपे किसी के ईमेल पर नज़र रखना-आईपीसी की धारा 465

वेव जैकिंग-आईपीसी की धारा 385

ईमेल का ग़लत इस्तेमाल-आईपीसी की धारा 500

दवाओं को ऑनलाइन बेचना-एनडीपीएस एक्ट

हथियारों की ऑनलाइन खरीद - बिक्री-आर्म्स एक्ट

66-एफ : साइबर आतंकवाद के लिए दंड का प्रावधान

साइबर आतंकवाद के मामलों में दंड विधान के लिए सूचना तकनीक कानून, 2000 में धारा 66-एफ को जगह दी गई है।

(१) यदि कोई-

(अ) भारत की एकता, अखंडता, सुरक्षा या संप्रभुता को भंग करने या इसके निवासियों को आतंकित करने के लिए-

(क). किसी अधिकृत व्यक्ति को कंप्यूटर के इस्तेमाल से रोकता है या रोकने का कारण बनता है।

(ख) बिना अधिकार के या अपने अधिकार का अतिक्रमण कर जबरन किसी कंप्यूटर के इस्तेमाल की कोशिश करता है। [10,11,12]

(ग) कंप्यूटर में वायरस जैसी कोई ऐसी चीज डालता है या डालने की कोशिश करता है. जिससे लोगो की जान को खतरा पैरोने की आशंका हो या संपत्ति के नकसान का खतरा हो जीवन के लिए आवश्यक सेवाओं में जानबूझकर खाने की कोशिश करता हो या धारा 20 के तहत संवेदन जानकारीयों पर बुरा असर पड़ने की आशंका हो या-

(भा) अनाधिकार या अधिकारों का अतिक्रमण करते हुए जानबूझकर किसी सुरक्षा कंप्यूटर हैक करने में कामयाब होता है. जो देश की सुरक्षा या अन्य देशों के साथ उसके संबंधों के संवेदनशीलता को भी सेना इरादे के साथ मिल करता है भारत की सुरक्षा, एकता, अखंडता एवं संप्रभुता, अन्य देशों के साथ इसके संबंध, सार्वजनिक जीवन या नैतिकता पर बुरा असर पड़ता हो या ऐसा होने की आशंका हो, देश की अदालतों की अवमानना अथवा मानहानि होती हो या ऐसा होने की आशंका हो, किसी अपराध को बढ़ावा मिलता हो या इसकी आशंका हो, किसी विदेशी राष्ट्र अथवा व्यक्तियों के समूह अथवा किसी अन्य को ऐसी सूचना में फायदा पहुंचता हो, तो उसे साइबर आतंकवाद का आरोपी माना जा सकता है।

(२) यदि कोई व्यक्ति साइबर आतंकवाद फैलाता है या ऐसा करने की किसी साजिश में शामिल होता है तो उसे आजीवन कारावास की सजा सुनाई जा सकती है।

2005 में प्रकाशित एडवांस्ड लॉ लेक्सिकॉन के तीसरे संस्करण में साइबरस्पेस शब्द को भी इसी तर्ज पर परिभाषित किया गया है। इसमें इलेक्ट्रॉनिक माध्यमों में फ्लोटिंग शब्द पर खासा जोर दिया गया है, क्योंकि दुनिया के किसी भी हिस्से से इस तक पहुंच बनाई जा सकती है। लेखक ने आगे इसमें माइवर येफ्ट (साइबर चोरी) शब्द को ऑनलाइन कंप्यूटर सेवाओं के इस्तेमाल के परिप्रेक्ष्य में परिभाषित हुवा है। इस शब्दकोश में साइबर कानून की इस

तरह व्याख्या की है, कानून का वह क्षेत्र, जो कंप्यूटर और इंटरनेट से संबंधित है और उसके दायरे में इंटेलिक्चुअल प्रॉपर्टी राइट्स, अभिव्यक्ति की स्वतंत्रता और सूचनाओं तक निर्वाध पहुंच आदि आते हैं।

सूचना तकनीक कानून में कुछ और चीजों को परिभाषित किया गया है, जो इस प्रकार हैं, कंप्यूटर से तात्पर्य किसी भी ऐसे इलेक्ट्रॉनिक, मैग्नेटिक, ऑप्टिकल या तेज़ गति से डाटा का आदान-प्रदान करने वाले किसी भी ऐसे यंत्र से है, जो विभिन्न तकनीकों की मदद से गणितीय, तार्किक या संग्रहणीय कार्य करने में सक्षम है। इसमें किसी कंप्यूटर तंत्र से जुड़ा या संबंधित हर प्रोग्राम और सॉफ्टवेयर शामिल है।

सूचना तकनीक कानून, 2000 की धारा 1 (2) के अनुसार, उल्लिखित अपवादों को छोड़कर इस कानून के प्रावधान पूरे देश में प्रभावी हैं। साथ ही उपरोक्त उल्लिखित प्रावधानों के अंतर्गत देश की सीमा से बाहर किए गए किसी अपराध की हालत में भी उक्त प्रावधान प्रभावी होंगे। [13,14,15]

विचार-विमर्श

आज, दुनिया पहले से कहीं ज्यादा डिजिटल रूप से जुटी हुई है। अपराधी इस ऑनलाइन परिवर्तन का फ़ायदा उठाकर ऑनलाइन सिस्टम, नेटवर्क और बुनियादी ढांचे की कमजोरियों को निशाना बनाते हैं। दुनिया भर में सरकारों, व्यवसायों और व्यक्तियों पर इसका बहुत बड़ा आर्थिक और सामाजिक प्रभाव पड़ता है।

फ़िशिंग, रैनसमवेयर और डेटा उल्लंघन वर्तमान साइबर खतरों के कुछ उदाहरण हैं, जबकि साइबर अपराध के नए प्रकार हर समय सामने आ रहे हैं। साइबर अपराधी तेज़ी से चुस्त और संगठित होते जा रहे हैं- नई तकनीकों का फ़ायदा उठाते हुए, अपने हमलों को नए तरीके से अंजाम देते हुए और नए तरीकों से सहयोग करते हुए।

साइबर अपराध किसी राष्ट्रीय सीमा को नहीं जानते। अपराधी, पीड़ित और तकनीकी ढांचा कई अधिकार क्षेत्रों में फैले हुए हैं, जिससे जांच और अभियोजन में कई चुनौतियां आती हैं।

इसलिए सार्वजनिक और निजी भागीदारों के बीच घनिष्ठ सहयोग आवश्यक है। अपनी वैश्विक पहुंच के साथ इंटरपोल, क्रॉस-सेक्टर साझेदारी बनाने और अंतर्राष्ट्रीय कानून प्रवर्तन सहयोग को सक्षम करने में महत्वपूर्ण भूमिका निभाता है।

इंटरपोल में, हम कानून प्रवर्तन कार्यों का समन्वय करते हैं, और साइबर खतरों को कम करने के लिए सुरक्षित डेटा साझाकरण प्लेटफ़ॉर्म, विश्लेषण और प्रशिक्षण प्रदान करते हैं। साइबर अपराधों को रोकने, पता लगाने, जांच करने और बाधित करने के लिए हमारे सदस्य देशों की क्षमता बढ़ाकर, हम एक सुरक्षित दुनिया के लिए समुदायों की रक्षा करने में मदद कर सकते हैं। [16,17,18]

परिणाम

हम जितनी तेज़ी से डिजिटल दुनिया की ओर बढ़ रहे हैं, ठीक उतनी ही तेज़ी से साइबर अपराध की संख्या में भी वृद्धि हो रही है। जिस गति से तकनीक ने उन्नति की है, उसी गति से मनुष्य की इंटरनेट पर निर्भरता भी बढ़ी है। एक ही जगह पर बैठकर इंटरनेट के ज़रिये मनुष्य की पहुँच, विश्व के हर कोने तक आसान हुई है। आज के समय में हर वो चीज़ जिसके विषय में इंसान सोच सकता है, उस तक उसकी पहुँच इंटरनेट के माध्यम से हो सकती है, जैसे कि सोशल नेटवर्किंग, ऑनलाइन शॉपिंग, डेटा स्टोर करना, गेमिंग, ऑनलाइन स्टडी, ऑनलाइन जॉब इत्यादि। आज के समय में इंटरनेट का उपयोग लगभग हर क्षेत्र में किया जाता है। इंटरनेट के विकास और इसके संबंधित लाभों के साथ साइबर अपराधों की अवधारणा भी विकसित हुई है। वर्तमान में भारत की बढ़ी आबादी सोशल नेटवर्किंग साइट्स का उपयोग करती है। भारत में सोशल नेटवर्किंग साइट्स के उपयोग के प्रति लोगों में जानकारी का अभाव है। इसके साथ ही अधिकतर मो साइट के सर्वर विदेश में हैं जिससे भारत में साइबर अपराध घटित होने की स्थिति में इनकी जड़ तक पहुँच पाना कठिन होता है।

हमले में साइबर अपराध उसके प्रकार के उपाय और सरकार के द्वारा किये प्रावधान पर विमर्श किया जाएगा। इसके साथ ही साइबर अपराध में सोशल नेटवर्किंग में इसकी भूमिका भी मूल्यांकन किया जाएगा।

साइबर अपराध क्या है?

साइबर अपराध विभिन्न रूपों में किये जाते हैं। कुछ साल पहले, इंटरनेट के माध्यम से होने वाले अपराधों के बारे में जागरूकता का अभाव था। साइबर अपराधों के मामलों में भारत भी उन देशों के पीछे नहीं है, जहाँ साइबर अपराधों की घटनाओं की दर भी दिन-प्रतिदिन बढ़ती जा रही है। साइबर अपराध के मामलों में एक साइबर अपराधी, किसी उपकरण का उपयोग, उपयोगकर्ता की व्यक्तिगत जानकारी, गोपनीय व्यावसायिक जानकारी, सरकारी जानकारी या किसी डिवाइस को अक्षम करने के निये कर सकता है। उपरोक्त सूचनाओं को ऑनलाइन वेचना या खरीदना भी एक साइबर अपराध है।

इसमें कोई संशय नहीं है कि यह एक आपराधिक गतिविधि है, जिसे कंप्यूटर और इंटरनेट के उपयोग द्वारा अंजाम दिया जाता है। साइबर अपराध, जिसे 'इलेक्ट्रॉनिक अपराध' के रूप में भी जाना जाता है एक ऐसा अपराध है जिसमें किसी भी अपराध को करने के लिये कंप्यूटर, नेटवर्क डिवाइस या नेटर्स का उपयोग, एक वस्तु या उपकरण के रूप में किया जाता है। जहाँ इनके (कंप्यूटर, नेटवर्क डिवाइस वा नेटवर्क) ज़रिये ऐसे अपराधों को अंजाम दिया जाता है वहीं इन्हें लक्ष्य बनाते हुए इनके विरुद्ध उपयोग भी किया जाता है।

ऐसे अपराध में साइबर जबरन वसूली, पहचान की चोरी, क्रेडिट कार्ड धोखाधड़ी, कंप्यूटर से व्यतिरत डेटा हैक करना, फिशिंग, अवैध डाउनलोडिंग, साइबर स्टॉकिंग, वायरस प्रसार, सहित कई प्रकार की गतिविधियाँ शामिल हैं। गौरतलब

है कि सॉफ्टवेयर चोरी भी साइबर अपराध का ही एक रूप है, जिसमें यह जरूरी नहीं है कि साइबर अपराधी, ऑनलाइन पोर्टल के माध्यम से ही अपराध करे।

साइबर अपराध का वर्गीकरण

साइबर विशेषज्ञों के अनुसार, अपराध की श्रेणी को दो वर्गों में विभाजित किया जा सकता है-

वे अपराध जिनमें कंप्यूटर पर हमला किया जाता है। इस तरह के अपराधों के उदाहरण हैकिंग, वायरल हमले आदि हैं। [19]

वे अपराध जिनमें कंप्यूटर को एक हथियार/उपकरण/ के रूप में उपयोग किया जाता है। इस प्रकार के अपराधों में साइबर आतंकवाद, आईपीआर उल्लंघन, क्रेडिट कार्ड धोखाधड़ी, पोर्नोग्राफी आदि।

साइबर अपराध की श्रेणियाँ

साइबर अपराध के अंतर्गत 3 प्रमुख श्रेणियाँ आती हैं जिसमें व्यक्ति: विशेष, संपत्ति और सरकार के

विरुद्ध अपराध शामिल हैं।

व्यक्ति विशेष के विरुद्ध साइबर अपराध ऐसे अपराध, यद्यपि ऑनलाइन होते हैं, परंतु वे वास्तविक लोगों के जीवन को प्रभावित करते हैं। इनमें से कुछ अपराधों में साइबर उत्पीड़न और साइबर स्टॉकिंग, चाइल्ड पोर्नोग्राफी का वितरण, विभिन्न प्रकार के स्पूर्फिम, क्रेडिट कार्ड धोखाधड़ी, मानव तस्करी, पहचान की चोरी और ऑनलाइन बदनाम किया जाना शामिल हैं। साइबर अपराध की इस श्रेणी में किसी व्यक्ति या समूह के खिलाफ दुर्भावनापूर्ण या अवैध जानकारी को ऑनलाइन लीक कर दिया जाता है।

संपत्ति विशेष के विरुद्ध साइबर अपराध- कुछ ऑनलाइन अपराध संपत्ति के खिलाफ होते हैं, जैसे कि कंप्यूटर या सर्वर के खिलाफ या उसे ज़रिया बनाकर किये जाते हैं। इन अपराधों में हैकिंग, वायरस ट्रांसमिशन, साइबर और टाइपो स्क्वाटिंग, कॉपीराइट उल्लंघन, आईपीआर उल्लंघन आदि शामिल हैं। उदाहरण- कोई आपको एक वेब-लैंक भेजे, जिस पर क्लिक करने के पश्चात एक वेब पेज खुले जहाँ आपसे आपके बैंक खाते/गोपनीय दस्तावेज़ संबंधित सारी जानकारी मांगी जाए और ऐसा कहा जाए कि यह जानकारी रिज़र्व बैंक ऑफ़ इंडिया या सरकार की ओर से मांगी जा रही है, आप वहाँ सारी जानकारी दे दें और फिर उस जानकारी के इस्तेमाल से आपके दस्तावेज़ एवं बैंक खाते के साथ छेड़छाड़ की जाए, तो यह संपत्ति के विरुद्ध साइबर हमला कहा जायेगा।

सरकार विशेष के विरुद्ध साइबर अपराध: यह सबसे गंभीर साइबर अपराध माना जाता है। सरकार के खिलाफ किये गए ऐसे अपराध की साइबर आतंकवाद के रूप में भी जाना जाता है। सरकारी साइबर अपराध में सरकारी वेबसाइट

या सैन्य बेवसाइट को हैक किया जाना शामिल हैं। गौरतलब है कि जब सरकार के खिलाफ एक साइबर अपराध किया जाता है, तो इसे उस राष्ट्र की संप्रभुता पर हमला और युद्ध की कार्रवाई माना जाता है। ये अपराधी आमतौर पर आतंकवादी या अन्य शत्रु देशों की सरकारें होती हैं। इस प्रकार के साइबर अपराधों पर नियंत्रण के लिये प्रत्येक देश की सरकार द्वारा कठोर साइबर कानून बनाए गए हैं।

सोशल मीडिया की भूमिका

बड़े पैमाने पर सोशल नेटवर्किंग साइट्स का उपयोग करने वाली जनसंख्या साइबर अपराध के खतरों से अनजान है। विभिन्न सोशल नेटवर्किंग साइट्स के सर्वर अन्य देशों में केंद्रित हैं, जिससे यह डर रहता है कि कहीं ये देश लोगों की व्यक्तिगत जानकारी का दुरुपयोग न करें। विभिन्न सोशल नेटवर्किंग साइट्स पर लोग अपनी व्यक्तिगत जानकारी सांझा करते हैं जिससे प इन नेटवर्किंग एकाउंट को आसानी से बैंक कर लेते हैं और फिर प्राप्त सूचना का दुरुपयोग

लोगों को सोशल नेटवर्किंग साइट्स पर हैकर्स ऑनलाइन ठगी का शिकार बनाते हैं।

सरा एजेंसियों द्वारा यह भी पता लगाया गया है कि ऑनलाइन मुद्रा स्थानांतरित करने वाले वि.एफ.एफ.के. के माध्यम से आतंकवादियों और देशविरोधी तत्वों को फंडिंग की जाती है।

साइबर अपराधी विभिन्न ऑनलाइन के माध्यम से बच्चों को अपराध करने के लिये प्रोत्साहित करते हैं।

साइबर अपराधों से निपटने की दिशा में सरकार के प्रयास

भारत में सूचना प्रौद्योगिकी अधिनियम, 2000 पारित किया गया जिसके प्रावधानों के साथ-साथ भारतीय दंड संहिता के प्रावधान सम्मिलित रूप से साइबर अपराधों से निपटने के लिये पर्याप्त है।

सूचना प्रौद्योगिकी अधिनियम 2000 की धाराएँ 45, 43ए, 66, 66बी, 66ती, 66डी, 66ई, 66एफ 67, 67ए, 67वी, 70, 72, 72ए और 74 हैकिंग और साइबर अपराधों से संबंधित हैं।

सरकार द्वारा राष्ट्रीय साइबर सुरक्षा नीति, 2013 जारी की गई जिसके तहत सरकार ने अति-संवेदनशील सूचनाओं के संरक्षण के लिये 'राष्ट्रीय अति-संवेदनशील सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure protection centre-NCIIPC) का गठन किया।

इसके अंतर्गत 2 वर्ष से लेकर उम्रकैद तथा दंड अथवा जुर्माने का भी प्रावधान है।

विभिन्न स्तरों पर सूचना सुरक्षा के क्षेत्र में मानव संसाधन विकसित करने के उद्देश्य से सरकार ने 'सूचना सुरक्षा शिक्षा और जागरूकता' (Information Security Education and Awareness: ISEA) परियोजना प्रारंभ की है।

सरकार द्वारा 'कंप्यूटर इमरजेंसी रिस्पॉन्स टीम (CERT-In)' की स्थापना की गई जो कंप्यूटर सुरक्षा के लिये राष्ट्रीय स्तर की मॉडल एजेंसी है।

देश में साइबर अपराधों से समन्वित और प्रभावी तरीके से निपटने के लिए 'साइबर स्वच्छता केंद्र' भी स्थापित किया गया है। यह इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय (Ministry of Electronics and Information Technology-Meit Y) के तहत भारत सरकार की डिजिटल इंडिया मुहिम का एक हिस्सा है।

भारत सूचना साझा करने और साइबर सुरक्षा के संदर्भ में सर्वोत्तम कार्य प्रणाली अपनाने के लिये अमेरिका, ब्रिटेन और चीन जैसे देशों के साथ समन्वय कर रहा है। [18,19,20]

अंतर-एजेंसी समन्वय के लिये 'भारतीय साइबर अपराध समन्वय केंद्र (Indian Cyber Crime Co-ordination Centre-14C) की स्थापना की गई है।

भारतीय साइबर अपराध समन्वय केंद्र

जनवरी 2020 में गृह मंत्रालय द्वारा साइबर क्राइम में निपटने के लिये 'भारतीय साइबर अपराध समन्वय केंद्र' (Indian Cyber Crime Coordination Centre-14C) का उद्घाटन किया गया है।

इस योजना को संपूर्ण भारत में लागू किया गया है। साइबर क्राइम से बेहतर तरीके से निपटने के लिये तथा 14C को समन्वित और प्रभावी तरीके से लागू करने हेतु इस योजना के निम्नलिखित सात प्रमुख घटक हैं-

नेशनल साइबरक्राइम थ्रेट एनालिटिक्स यूनिट (National Cybercrime Threat Analytics Unit)

नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल (National Cyber Crime Reporting Portal)

संयुक्त साइबर अपराध जाँच दल के लिये मंच (Platform for Joint Cyber Crime Investigation Team)

राष्ट्रीय साइबर अपराध फॉरेंसिक प्रयोगशाला पारिस्थितिकी तंत्र (National Cyber Crime Forensic Laboratory Ecosystem)

राष्ट्रीय साइबर क्राइम प्रशिक्षण केंद्र (National Cyber Crime Training Centre)

साइबर क्राइम इकोसिस्टम मैनेजमेंट यूनिट (Cyber Crime Ecosystem Management Unit)

राष्ट्रीय साइबर अनुसंधान और नवाचार केंद्र (National Cyber Research and Innovation Centre)

बुडापेस्ट कन्वेंशन क्या है?

साइबर अपराध के संबंध में बुडापेस्ट कन्वेंशन (Budapest Convention on cyber crime) पर हस्ताक्षर करने के लिये गृह मंत्रालय द्वारा साइबर अपराध और डेटा सुरक्षा को बढ़ावा देने के लिये अंतर्राष्ट्रीय सहयोग की आवश्यकता पर बल दिया जा रहा है।

बुडापेस्ट कन्वेंशन साइबर क्राइम पर एक कन्वेंशन है, जिसे साइबर अपराध पर बुडापेस्ट कन्वेंशन के

नाम से जाना जाता है।

यह अपनी तरह की पहली ऐसी अंतर्राष्ट्रीय संधि है जिसके अंतर्गत राष्ट्रीय कानूनों को सुव्यवस्थित करके, जाँच-पड़ताल की तकनीकों में सुधार करके तथा इस संबंध में विश्व के अन्य देशों के बीच सहयोग को बहाने हेतु इंटरनेट और कंप्यूटर अपराधों पर रोक लगाने संबंधी मांग की गई है।

कानडेटा तक पहुंच की अनमति देता है और इस प्रकार यह राष्ट्रीयता उत्त्वंचन करता है, इसलिये भारत ने अभी तक इस पर हस्ताक्षर नहीं किये हैं।

निष्कर्ष

गए हैं। साइबर सुरक्षा उपलब्ध कराने के लिये सरकार की ओर से कई कदम उठाए गए हैं। ले भारत इंटरनेट का तीसरा सबसे बड़ा उपयोगकर्ता है और हाल के वर्षों में साइबर अपराध । अर्थव्यवस्था को अपनाने की दिशा में बढ़ने के कारण भारत में साइबर सुरक्षा सुनिश्चित करना आवश्यक है। डिजिटल भारत कार्यक्रम की सफलता काफी हद तक साइबर सुरक्षा पर निर्भर करेगी अतः भारत की इस क्षेत्र में तीव्र गति से कार्य करना होगा। वहीं दूसरी ओर सोशल मीडिया ने अभिव्यक्ति की स्वतंत्रता के अधिकार को नया आयाम दिया है, आज प्रत्येक व्यक्ति बिना किसी हर के सोशल मीडिया के माध्यम से अपने विचार रख सकता है और उसे हज़ारों लोगों तक पहुँचा सकता। परंतु सोशल मीडिया का सावधानीपूर्वक उपयोग ही हमें ऑनलाइन ठगी तथा साइबर अपराध के गंभीर खतरों से बचा सकता है। [20]

संदर्भ

1) सुखाई, नतालिया बी. (8 अक्टूबर 2004)। "हैकिंग और साइबर अपराध। सूचना सुरक्षा पाठ्यकर विकास पर प्रथम वार्षिक सम्मेलन की कार्यवाही। न्यूयॉर्क, एनवाई, यूएसए: एसीएम। पीपी. 123-152. doi: 10.1145/1059524-10595551 आईएसबीएन। 1-59595-018-5. मूल से 18 जुलाई 2010 को पुरालेखित । 10 दिसंबर 2020 को पुनःप्राप्त ।

2) "बफेट: यह 'मानव जाति की सबसे बड़ी समस्या है'". विजनेस इनसाइडर। मूल से 9 जून १०४० को

संग्रहीत । 17 मई 2021 को लिया गया।

3) "वॉरेन बफेट: 'साइबर मानवता के लिए वास्तविक खतरा है'", finance.yahoo.com. 30 अप्रैल 2019 12 जून 2010 को मूल से संग्रहीत। 17 मई 2021 को लिया गया।

4) "ग्लोबल रिस्क रिपोर्ट 2020" (पीडीएफ)। विश्व आर्थिक मंच 15वां संस्करण: 102. 15 जनवरी 2020 127 सितंबर 2020 को मूल से संग्रहीत (पीडीएफ) । 17 मई 2021 को लिया गया।

5) हेडिंग, सोफी, जाहिदी, सादिया (जनवरी 2020)। "ग्लोबल रिस्क रिपोर्ट 2020, 18वां संस्करण" (पीडीएफ)। विश्व आर्थिक मंच। 5 फरवरी 2020 को मूल से संग्रहीत (पीडीएफ)। फरवरी 2000 को लिया गया।

6) फ्रीज, डि (12 अक्टूबर 2020)। "2020 में साइबर अपराध से दुनिया को सालाना 9.5 ट्रिलियन अमेरिकी डॉलर का नुकसान होगा"। साइबर अपराध पत्रिका। मूल से। फरवरी 2020 को संग्रहीत । 3 फरवरी 2020 को लिया गया।

7) गॉर्डन, सारा (25 जुलाई 2006)। "साइबर अपराध की परिभाषा और वर्गीकरण पर। जर्नल इन कंप्यूटर वायरोलॉजी । 2:15-20. doi: 10.1007/s11516-006-0015-z, S2CID 3334277

8) रिचेट, जीन-तूप (1 जनवरी 20:20)। "साइबर अपराधी समुदाय कैसे बढ़ते और बदलते हैं: विज्ञापन-धोखाधड़ी समुदायों की जांच। तकनीकी पूर्वानुमान और सामाजिक परिवर्तन। 79121282) 121282.doi: 10.1016/j.techfore.2021.181282 11SSN0040-1025151CID9300695401

9) लेहमैन, जेफरी; फेलप्स, शिरेल (2005). बेस्ट इनसाइनलोपीडिया ऑफ अमेरिकन लो, खंड 3 (दूसरा संस्करण), बेट्राइट: थॉमसन/गेल. पृष्ठ 137. आईएसबीएन 9780787065742.

10) "कंप्यूटर और इंटरनेट धोखाधड़ी"। LII/ कानूनी सूचना संस्थान। मूल से 10 अगस्त 2000 को संग्रहीत ।। नवंबर 2020 को लिया गया।

11) पार्कर डी (1983) फाइटिंग कंप्यूटर काइम, यू.एस.: चार्ल्स रिक्वर्न्स संस

12) "बॉटनेट, साइबर अपराध और साइबर आतंकवाद: कांग्रेस के लिए कमजोरियाँ और नीतिगत मुद्दे". www.everycrsreport.com. मूल से 29 सितंबर 2000 को संग्रहीत। 5 सितंबर 2001 को लिया गया 1

- 15) मॉर्गन, स्टीव (13 नवंबर 2020)। "2020 तक साइबर अपराध से दुनिया को सालाना 10.5 ट्रिलियन डॉलर का नुकसान होगा"। साइबर अपराध पत्रिका। 19 जुलाई 2020 को लिया गया।
- 14) लेपोप्रस्की, रॉन. "डेनियल-ऑफ़-सर्विस अटैक द्वारा साइबर जबरन वसूली" (पीडीएफ)। मूल (पीडीएफ) से 6 जुलाई 2011 को संग्रहीत ।
- 15) मोहन्ता, अभिजीत (6 दिसंबर 2014)। "नवीनतम सोनी पिक्चर्स द्वाीच: एक घातक साइबर जबरन बसूली"। मूल से 25 सितंबर 2015 को संग्रहीत। 20 सितंबर 2015 को लिया गया।
- 16) "बढ़ता रैनसमवेयर खतरा: । रुझान और अंतर्दृष्टि"। पालो बऑल्टो नेटवर्क। 25 मार्च 2020। मूल से 18 जुलाई 2020 को संग्रहीत। 11 मई 2020 को लिया गया।
- 17) "2020 और उसके बाद के लिए 100+ रैनसमवेयर ऑकड़े नॉर्टन"। us.norton.com। मूल से 16 जुलाई 2020 को संग्रहीत। 11 मई 2020 को लिया गया।
- 18) कारबैंक, जोशुआ टी. (2018). "साइबरसेक्स तस्करी: अधिक प्रभावी अभियोजन प्रतिक्रिया की ओर क्रिमिनल लॉ बुलेटिन 54 (1): 64-183. पृष्ठ 64.
- 19) "आईजेएम बच्चों की साइबरसेक्स तस्करी को समाप्त करना चाहता है और इस साइबर सोमवार और मंगलवार को रीस्टार्टफ्रीडम करना चाहता है"। पीआर न्यूजबाबर। 28 नवंबर 2016। मूल से 17 अप्रैल 2017 को संग्रहीत। 9 मई 2020 को लिया गया।
- 20) 'साइबरसेक्स ट्रेफिकिंग' । आईजेएम। 2020. मूल से 21 मई 2020 को संग्रहीत। 9 मई 2020 को लिया गया।