शब्द–ब्रह्म
E ISSN 2320 – 0871
भारतीय भाषाओं की अंतर्राष्ट्रीय मासिक शोध पत्रिका
17 अप्रैल 2017
पीअर रीव्यूड रेफ्रीड रिसर्च जर्नल

समकालीन वर्षों में साइबर अपराध

अजित कुमार (शोधार्थी)
राजनीति विज्ञान विभाग
दिल्ली विश्वविद्यालय
दिल्ली, भारत

शोध संक्षेप

बीसवीं सदी में वैज्ञानिक आविष्कारों में इलेक्ट्रानिक और दूरसंचार के क्षेत्र में हुई अभूतपूर्व खोजों ने एक तरफ तो दुनिया को विश्वग्राम में परिवर्तित कर दिया तो दूसरी ओर अनेक प्रकार की चुनौतियां भी उपस्थित हुईं हैं। आज पूरी दुनिया में इलेक्ट्रानिक माध्यम से होने वाले अपराधों में बेतहाशा वृद्धि हुई है। भारत भी इससे अछूता नहीं है। भारत में आठवे दशक में हुए सूचना प्रौद्योगिकी तथा इलेक्ट्रानिक मीडिया के विकास के परिणामस्वरूप अपराधों का एक नया वर्ग अस्तित्व में आया, जिसे साइबर अपराध के नाम से जाना जाता है। विश्व स्तर पर इन अपराधों की निरंतर बढ़ती हुई संख्या के कारण विधि अपराध प्रवर्तन संस्थाओं के समक्ष यह चुनौतियाँ उभर कर सामने आई। साइबर अपराधों की विशेषता यह है कि यह अपराधी की घटना स्थल पर उपस्थित हुए बिना किसी भी स्थान से अपराध को अंजाम दे सकते हैं। अपराधी व अपराध का शिकार हुआ व्यक्ति एक-दूसरे से पूर्णतः अनजान होते हैं। इन अपराधों की अन्य विशेषता यह है कि इसे कारित करने वाला व्यक्ति स्वयं अदृश्य रहते हुए कम्प्यूटर तकनीक के माध्यम से लक्षित व्यक्ति को क्षति पहुंचाता है।1 अतः उसके पकड़े जाने की संभावना नहीं के बराबर रहती है।2 प्रस्तुत शोध पत्र में समकालीन वर्षों में साइबर अपराध का विश्लेषणात्मक अध्ययन और उसके समाधान के बिंदु सुझाये गए हैं। इस शोध आलेख को चार भागों में विभाजित किया गया है। पहले भाग में साइबर अपराध का विवेचन, दुनिया के विभिन्न देशों में साइबर अपराधों का संक्षिप्त विवेचन, दूसरे भाग में विभिन्न प्रकार के साइबर अपराध, भाग तीन में भारत में होने वाले साइबर अपराध और भाग चार में साइबर अपराध को नियंत्रित करने के विभिन्न तरीकों का विवेचन किया गया है।3

भूमिका

इंटरनेट व साइबर अपराध. इंटरनेट (संजाल) हमारी जिंदगी का अहम हिस्सा बन चुका है। चंद सेकेंड में क्लिक करके हम अनगिनित सूचनाओं को प्राप्त कर सकते है। इंटरनेट के तेजी से हो रहे प्रसार के साथ ही साइबर अपराध के आंकड़े भी बढ़ते जा रहे है। इंटरनेट के द्वारा बैंकिंग संबंधी सूचनाएँ और शेयर बाजार को प्रभावित करने के अलावा साइबर अपराधी इन दिनों युवाओं में मशहूर होते जा रहे ऑनलाइन डेटिंग एप्स में सक्रिय हो रहे हैं। साइबर अपराधों से पूरी दुनिया जूझ रही है। इन अपराधों पर अंकुश लगाने की बजाय यह तेजी से बढ़ते चले जा रहे हैं। साइबर अपराध के बारे में देबारती हदर एंड के जयशंकर लिखते हैं, "साइबर अपराध एक ऐसा अपराध है जिसे इंटरनेट के जरिये करने का प्रयास किया जाता है, जैसे ई-मेल, फेसबुक हैक करना, फोन या किसी अन्य तरीके से बैंक एकाउंट की जानकारी लेकर उससे पैसे निकलवाना, एटीएम या सीवीसी कोड जानना इत्यादि। जहां एक ओर इंटरनेट वरदान साबित हुआ वहीं दूसरी ओर अभिशाप बनने में देर नहीं

लगी। जहां पहले सिर्फ हैकिंग या वाइरस का डर होता था वहीं आज मर्फिंग, पोर्नोग्राफ़ी व पीडोफाइल को भी इसके अंतर्गत शामिल किया जाने लगा है।4

मार्को गारको ने अंतरराष्ट्रीय परिप्रेक्ष्य में साइबर अपराध को स्पष्ट करने की कोशिश की और माना कि पूरी दुनिया में साइबर अपराध कम्प्यूटर नेटवर्क के लिए खतरा बना हुआ है। इससे निपटने के लिए अंतरराष्ट्रीय स्तर पर एंटी साइबर क्रिमिनल लॉ लागू किए जाने की आवश्यकता है। इस हेतु टोकियो में सन् 1998 में संयुक्त राष्ट्र संघ द्वारा विशेषज्ञों के एक कार्य दल की बैठक आयोजित की गयी, ताकि साइबर आपराधिकता के निवारण हेतु कारगर कदम उठाया जा सके। विगत दशक में विश्व के प्रायः सभी विकसित एवं विकासशील देशों ने अपनी साइबर विधियां विकसित की हैं जो अधिकांशतः राष्ट्र संघ द्वारा निर्मित मॉडल साइबर ला पर आधारित है।5 इन्टरनेट द्वारा संचालित आपराधिक गतिविधियों की रोकथाम हेतु कनाडा, ब्रिटेन, आस्ट्रेलिया, जापान, फिलीपींस, फ्रांस, चीन, मॉरीशस, श्रीलंका, पाकिस्तान, बांग्लादेश और भारत आदि देशों ने अपनी साइबर विधियों को अद्यतन बनाया है, जबकि ब्राज़ील, चेक गणराज्य, स्पेन, पोलैंड जैसे देशों में साइबर आपराधिकता के ऊपर अलग-अलग तरह के प्रावधान किए गए हैं।

साइबर अपराध हेतु वैश्विक प्रावधान

मार्को गारके ने संयुक्त राज्य अमेरिका की साइबर विधि का विश्लेषण किया और यह स्पष्ट किया कि अमेरिका में सर्वप्रथम कम्प्यूटर क्राइम विधेयक सन् 1986 में पारित हुआ जिसे कंप्यूटर फ्रॉड एंड एब्यूज एक्ट 1986 कहा गया। वर्तमान में अमेरिका के विभिन्न राज्यों तथा संघीय सरकार ने अपनी साइबर विधियाँ पारित की हैं। राज्यों में घटित होने वाले साइबर अपराधों के प्रति केलिफोर्निया की दंड संहिता के उपबंध लागू होते हैं, जिनमें कम्प्यूटर, कम्प्यूटर सिस्टम, या कम्प्यूटर नेटवर्क में अधिकृत अभिगमन के लिए दंड की व्यवस्था है।6 न्यूयार्क कम्प्यूटर क्राइम लॉ में भी इसी तरह के प्रावधान हैं। फेडरल कम्प्यूटर लॉ 1995 अंतर्गत कम्प्यूटर के अधिकृत उपयोग या इसमें संग्रहीत रिकॉर्ड, डाटा आदि को नष्ट करने या अधिकृत तौर से बदलने आदि संबंधी उपबंध दिये गए हैं।7

रुससेल जी स्मिथ आस्ट्रेलिया की साइबर विधि को स्पष्ट करते हुए माना कि आस्ट्रेलिया की अपनी प्रारंभिक साइबर विधि सन् 2001 में अधिनियमित की गयी, जिसे साइबर क्राइम एक्ट 2001 कहा गया। यह अधिनियम अप्रैल 2, 2002 से लागू किया गया। इस अधिनियम के अंतर्गत साइबर अपराधों को तीन प्रमुख भागों में रखा गया 1 अधिकृत अधिगमन, 2 डाटा का अधिकृत उपांतरण, 3 इलेक्ट्रोनिक संचार का अधिकृत ह्रास। इसके अतिरिक्त कोई साइबर अपराध कारित करने के आशय से डाटा कब्जे में रखना भी दंडनीय अपराध माना जाएगा, जिसके लिए तीन वर्ष तक का कारावास का दंड होगा।8

इसी तरह तकलो नस्त्सुई ने जापान की साइबर विधि का अध्ययन किया। जापान ने यूरोपियन साइबर क्राइम कन्वेंशन की संधि पर हस्ताक्षर किए गए। अतः यह इसका सदस्य होने के कारण इसने साइबर अपराधों से निपटने के लिए दो कानून पारित किए, जिन्हें अन अथोराइज्ड कम्प्यूटर एसेस लॉ 1999 तथा कम्प्यूटर क्राइम एक्ट कहा गया। इसमें से प्रथम अधिनियम फरवरी 2000 से लागू हुआ, जिसमें अनधिकृत कम्प्यूटर अभिगमन के लिए कठोर दंड की

व्यवस्था है। कम्प्यूटर क्राइम अधिनियम द्वारा जारी जापानी दंड संहिता को संशोधित किया गया ताकि इंटरनेट के माध्यम से कारित होने वाले अपराधों का भी इस संहिता के प्रावधानों के अधीन निस्तारण किया जा सके।9

ऐसा ही विवेचन कलूम जेफफरी ने ब्रिटेन में ब्रिटिश कम्प्यूटर विधि का किया। ब्रिटेन में कम्प्यूटर मिसयुज अधिनियम 1990 पारित किया गया, जिसे सन् 2006 में कम्प्यूटर अधिनियम द्वारा प्रतिस्थापित किया गया। इस अधिनियम के अंतर्गत सेवा के प्रत्याख्यान आक्रामणों को केंद्र बिन्दु बनाया गया ताकि वे कम्प्यूटर का सुचारु रूप से संचालन कर सकें और डाटा इंटरनेट आदि से छेड़छाड़ के अपराध घटित न हो सकें। इस अपराध के लिए दस वर्ष तक के कारावास का दण्ड दिया जा सकता है। किसी अन्य व्यक्ति को कम्प्यूटर प्रोग्राम या डाटा में वैध हस्तक्षेप या उसे नष्ट करने या बीच में रोकने के लिए उत्प्रेरित करना भी साइबर अपराध होगा।10

फ्रांस की साइबर विधि का विवेचन हरप्रीत सिंह एंड दोल्लांद गीता के द्वारा किया गया। फ्रांस का कम्प्यूटर कानून अधिकांशतः यूरोपियन कम्प्यूटर विधि पर आधारित है तथा इसके अधीन बनाए गए नियम प्रायः सभी यूरोपियन देशों पर लागू होते हैं। फ्रांस ने यूरोपियन निदेश तथा इलेक्ट्रोनिक हस्ताक्षर एवं ई-कॉमर्स सेवाओ संबंधी विधिक ढांचा 8 जून 2000 से लागू किया गया। कम्प्यूटर सिस्टम के माध्यम से कारित होने वाले बौद्धिक संपदा अधिकारों के उल्लंघन को नियंत्रण में रखने हेतु फ्रांस में एक नेशनल सुपरवाइजिंग एजेंसी कार्यरत है, जो इनसे संबन्धित अपराधो पर निगरानी रखती है। फ्रांस में (Internet Co-operation for assigned Name and Numbers) जिसे संक्षेप ICANN कहा जाता है के नियमों को अंगीकार किया गया है, ताकि ऑनलाइन व्यापार करने वालों के डोमेन नामों को समुचित सुरक्षा प्रदान की जा सके।11

राज सामनी ने चीन के साइबर कानून का विवेचन करते हुए कहा कि चीन गणराज्य में साम्यवादी सत्ता के दौरान साफ्टवेयर को उचित संरक्षण प्रदान करने हेतु चायनीज़ कापीराइट अधिनियम 1990 के अंतर्गत विनियम पारित किए गए परंतु सूचना प्रौद्योगिकी तथा इंटरनेट में नब्बे के दशक में हुए विकास के फलस्वरूप साइबर अपराधों में निरंतर हो रही वृद्धि को ध्यान में रखते हुए चीन सरकार में सूचना टास्क फोर्स गठित किया गया। चीन के ब्यूरो ऑफ पब्लिक सिक्यूरिटी को यह शक्ति प्राप्त है कि वह साइबर विनियमनों का उल्लंघन करने वालों के विरुद्ध कार्यवाई कर सकता है तथा लाइसेन्स के बगैर इंटरनेट सेवा प्रदान करने वालों को 1500 आरकेबी तक के जुर्माने से दंडित किया जा सकता है।12

अरुण कुमार पाठक ने भारत में साइबर विधि पर अपना ध्यान केन्द्रित करते हुए सूचना प्रद्यौगिकी अधिनियमए 2000 के द्वारा साइबर अपराध को परिभाषित किया गया है। अनेक विद्वानों का मत है कि इसकी परिभाषा अन्य परंपरागत अपराधों की परिभाषा से मूलतः भिन्न नहीं है, क्योंकि अन्य अपराधों की भांति साइबर अपराध भी कोई ऐसा कार्य करना या कार्य लोप जिससे विधि के उल्लंघन होता है। राज्य द्वारा दंडनीय होगा। फिर भी स्वतंत्र परिभाषा की दृष्टि से साइबर अपराध को ऐसा आपराधिक कृत्य कहा जा सकता है जिससे कम्प्यूटर को या तो माध्यम के रूप में प्रयोग किया जाता है या

अपराध कारित करने का साधन या लक्ष्य के रूप में निशाना बनाया जाता है।13

समकालीन वर्षों में साइबर अपराध की स्थिति

देश में वर्ष 2011 कुल 13301, वर्ष 2012 में 22060, वर्ष 2013 में 71780 साइबर अपराध दर्ज किए गए। साल 2014 में साइबर अपराध की करीब डेढ़ लाख वारदात होने की बात अध्ययन में सामने आई जिनके 2015-16 में बढ़कर 2.3 लाख होने की आशंका जताई गयी। यह भी आशंका जताई गयी कि अंजाम देने वाले अधिकतर युवा वर्ग हैं, जिनकी आयु 18 से 30 वर्ष है। वर्तमान में ऑन लाइन वित्तीय लेन-देन का 48 से 60 प्रतिशत हिस्सा मोबाइल के माध्यम से किया जा रहा है।14 बढ़ती ऑनलाइन बैंकिंग सेवाओं के मद्देनजर 2015 के अंत तक 55 से 60 प्रतिशत रहा। बढ़ती ऑनलाइन बैंकिंग सेवाओं के मद्देनजर भारत, अमेरिका और जापान के बाद तीसरे स्थान पर है। हालांकि दुनिया के दूसरे देशों के मुक़ाबले भले ही अपराधी भारत में कम हैं, लेकिन इनके बढ़ते आंकड़े नये सिरे से सोचने को मजबूर कर रहे हैं।15

संयुक्त राष्ट्र की एक रिपोर्ट की माने तो 18 से 24 साल की महिलाएं व लड़कियाँ खास तौर पर अपराध का निशाना बनती हैं। रिपोर्ट के मुताबित दुनिया भर में इंटरनेट इस्तेमाल करने वाले देशों की 5 में से 1 महिला औसतन ऐसी है जिनके खिलाफ अगर साइबर अपराध होता है तो दोषी को सजा मिलने की आशंका बहुत ही कम हो जाती है। 86 देशों में किए गए अध्ययन में यह भी खुलासा हुआ कि साइबर अपराध कानून लागू करने की जिम्मेदार संस्थाएं ऐसे मामलों में से केवल 24 फीसदी मामलों पर ही पर्याप्त कदम उठती हैं। भारत में महिलाओं द्वारा उन्हें ऑनलाइन परेशान किए जाने संबंधी मामलों की बहुत ही कम शिकायत की जाती है। एसोचैम के अनुसार सबसे बड़ी चिंता की बात यह है कि इन अपराधों का मूल स्थान चीन, पाकिस्तान, बंग्लादेश व अल्जीरिया सहित विदेश स्थित अन्य जगहों पर है।16 अध्ययन के अनुसार ऑनलाइन बैकिंग खातों पर फिशिंग हमले या एटीम या डेबिट कार्ड की क्लोनिंग आम साइबर अपराध है। इनके अलावा ऑनलाइन वित्तीय लेन-देन के लिए मोबाइल फोन, स्मार्टफोन, टेबलेट के बढ़ते इस्तेमाल के कारण भी साइबर अपराधों की आशंका बढ़ी है। साइबर अपराध अन्य अपराधों से इस प्रकार भिन्न है कि इसमें किसी भी चरण में साइबर अंतरिक्ष का प्रयोग किया गया होता है तथा यह कम्प्यूटर या इंटरनेट के माध्यम से कार्यान्वित किया जाता है।17

साइबर अपराध में तीव्र गति से वृद्धि के कारण साइबर अपराध के विभिन्न तरीकों का उल्लेख करने से पूर्व यह जान लेना आवश्यक है कि इन अपराधों में अन्य रूढ़िगत अपराधों की तुलना में शीघ्रता से वृद्धि के क्या कारण हैं तथा साइबर अपराधी सूचना प्रद्यौगिकी का दुरुपयोग करने की ओर क्यों प्रवृत हो रहे हैं।

कम्प्यूटर अपराध बढ़ने के कारण

कम्प्यूटर में थोड़ी-सी जगह में बृहत डाटा संग्रहीत रखने की विलक्षण क्षमता होने के कारण इसमें विविध सूचनाएँ एकत्रित कर रखी जा सकती हैं, जिसका किसी भी समय आवश्यकतानुसार उपयोग किया जा सकता है। इसी प्रकार आवश्यकता न रहने पर जानकारी को सरलता से हटाया जा सकता है।

सुरक्षा उपायों की अनदेखी करते हुए कम्प्यूटर में अधिकृत अभिगमन द्वारा गोपनीय या अवांछित

शब्द–ब्रह्म
E ISSN 2320 – 0871
भारतीय भाषाओं की अंतर्राष्ट्रीय मासिक शोध पत्रिका 17 अप्रैल 2017
पीअर रीव्यूड रेफ्रीड रिसर्च जर्नल

व्यक्तिगत जानकारी हासिल करना अपेक्षाकृत सरल होता है।18

कम्प्यूटर एक जटिल व्यवस्था से चालित होता है, जिसमें हजारों कूट संकेत रहते हैं। साइबर अपराधी मानव मस्तिष्क की विस्मृति का नाजायज फायदा उठाते हुए कम्प्यूटर सिस्टम में अवैध प्रवेशन द्वारा संचयित जानकारी चुरा लेते हैं ताकि उससे व्यक्ति को ब्लैकमेल किया जा सके या इसका नाजायज फायदा उठाया जा सके।19

कम्प्यूटर सिस्टम का मुख्य लक्षण यह है इसमें से सबूत को आसानी से नष्ट किया जा सकता है ताकि अन्वेषण संस्थाओं की पकड़ से बाहर रहे और उसके विरुद्ध अभियोजन का कोई साक्ष्य उपलब्ध न रहे।

कम्प्यूटर प्रयोक्ता द्वारा कम्प्यूटर में एकत्रित करके रखी गयी जानकारी को सुरक्षित रखने में तनिक भी असावधानी उसे घोर क्षति कारित कर सकती है, क्योंकि साइबर अपराधी कम्प्यूटर सिस्टम में अनधिकृत अभिगमन द्वारा जानकारी चुरा कर उसका दुरुपयोग कर सकता है।20

वाइरस (Viruses) - वर्तमान कम्प्यूटर वायरसों के कारण कम्प्यूटर सिस्टम को बहुत क्षति पहुँचती है। यहाँ वाइरस से आशय किसी बीमारी से फैलने वाली चिकित्सकीय बीमारी न होकर ऐसे कम्प्यूटर प्रोग्राम या कूट संकेत जो किसी अन्य प्रोग्रामो में प्रवेश कर उन्हें प्रतिकृत कर देता है और इस प्रकार कम्प्यूटर से संग्रहीत प्रोग्राम दूषित या विनष्ट हो जाता है। इससे डाटा फ़ाइलों को भी नुकसान पहुंचता है।

समान्यतः वाइरस मुख्यतः दो प्रकार के होते है 1 फ़ाइल इन्फेक्टर्स और 2 बूट रेकॉर्ड इन्फेकटर्स। फ़ाइल इन्फेक्टर्स सीधे मारक हो सकते हैं। सीधे मारक या फ़ाइल इन्फेक्टर्स एक ही समय या एक से अधिक प्रोग्रामों को विदूषित करते हैं, जबकि निवासी वाइरस कम्प्यूटर की मेमोरी में छिपा रहता है और जब भी किसी प्रोग्राम का निष्पादन किया जाता है तो वह उसे संक्रमित कर देता है। वही बूट रेकॉर्ड वाइरस इन्फेक्टर्स निष्पादनीय कूट संकेत को संक्रमित कर देता है, जो कि कम्प्यूटर डिस्क के सिस्टम में पाया जाता है। उदाहरण ब्राइन्न, अजूसा, माइकेलंगेलों, सोनदे, आदि बूट रेकॉर्ड वायरस हैं तथापि ऐसे भी कई वाइरस हैं जो दोनों को अर्थात फ़ाइल एवं बूट को संक्रमित कर देते हैं। इसलिए इन्हें बूट एंड फ़ाइल वायरस कहा जाता है।

साइबर अपराध को समान्यत: तीन वर्गों में विभाजित किया जा सकता है पहला व्यक्ति विशेष के विरूद्ध साइबर अपराध. इसमें ईमेल में हेराफेरी करके व्यक्ति को संत्रास पहुंचाना, मानहानि, कम्प्यूटर सिस्टम का प्रोग्राम में अधिकृत अभिगमन, अभद्र या अश्लील अंग प्रदर्शन, छल, वेवसाइट पर अश्लील साहित्य का प्रदर्शन शामिल है। दूसरा संपत्ति के विरूद्ध अपराध. कम्प्यूटर को जानबूझ कर क्षतिग्रस्त करना, उसमें वाइरस संक्रमित करना, सेवा उपलब्धि को रोकना, बौद्धिक सम्पदा अधिकारों का हनन, इंटरनेट टाइम चोरी, प्रतिबंधित वस्तुओं का क्रय-विक्रय का संवेश है। तीसरा समाज या राज्य के विरूद्ध अपराध. इसमें साइबर आतंकवाद, वित्तीय घोटाले, कपातए ऑनलाइन जुआ, अश्लीलता आदि सम्मिलित है।

कम्प्यूटर सिस्टम के माध्यम से अंतरिक्ष में होने वाले साइबर अपराध.

स्टाकिंग.- इस अपराध में अनिच्छुक प्राप्तकर्ता को लगातार संदेश भेजे जाते हैं ताकि उन्हें मानसिक यातना हो तथा वह क्षुब्ध हो जाए।

शब्द–ब्रह्म
E ISSN 2320 – 0871
भारतीय भाषाओं की अंतर्राष्ट्रीय मासिक शोध पत्रिका 17 अप्रैल 2017
पीअर रीव्यूड रेफ्रीड रिसर्च जर्नल

अनचाहे ई-मेल संदेशों से कम्प्यूटर उपभोक्ता के निजता के अधिकार का हनन होता है जिसे कम्प्यूटर भाषा में स्पेमिंग भी कहा जाता है। ऑनलाइन धमकियों तथा संत्रास के अनेक तरीके हैं जो साइबर अपराधियों द्वारा अपनाए जाते हैं। अधिकांश पुरुष साइबर अपराधी किसी महिला को लक्षित कर उनके ई-मेल पर अनचाहे भद्दे या अश्लील संदेश भेजकर स्टाकिंग करते हैं। वह अपना अपराध कम्प्यूटर के माध्यम से घर बैठकर कर सकते हैं तथा उसे पकड़े जाने का भय नही रहता, क्योंकि भौतिक रूप से उसकी उपस्थिति न होने के कारण उसकी पहचान नही की जा सकती और साइबर स्पेस में अपराध घटित होने के कारण अपराधी दृश्यमान भी नही होता।21

हैकिंग- वर्तमान समय में हैकिंग सर्वाधिक घटित होने के कारण अपराध है। साइबर अपराधियों द्वारा हैकिंग किए जाने के उद्देश्य नाजायज पैसे अर्जित करने से लेकर राजनीतिक हितों की पूर्ति या केवल कौतूहल या उत्सुकता इनमें से कुछ भी हो सकता है। हैकिंग के अनेक प्रकार हैं जैसे स्पूफिंग, ई-मेल, वार्विंग, ट्रोजन हमले, वाइरस हमले, पासवर्ड क्रेकिंग आदि। सरल शब्दों में क्रेकिंग से आशय कम्प्यूटर नेटवर्क के माध्यम से अधिकृत अभिगमन का प्रयास करते हुए संकलित डाटा या प्रोग्राम को नष्ट करना या उसमें अनधिकृत छेड़छाड़ करना।22

वेब जैकिंग- यह भी हैकिंग का एक प्रकार है, जिसमें अपराधी किसी अन्य व्यक्ति या उत्पीड़ित की बेबसाइट को अनधिकृत तरीके से अपने नियंत्रण में ले लेता है ताकि वह अपने अवैध या राजनीतिक उद्देश्य प्राप्त कर सके।23

ई-मेल ववविंग- का अर्थ उत्पीड़न को असंख्य ई-मेल संदेश भेजना ताकि वह भ्रमित होकर परेशान हो जाए और उसे मानसिक क्लेश पहुंचे। ट्रोजन हमला भी एक अनधिकृत प्रोग्राम है जो किसी अन्य के कम्प्यूटर सिस्टम पर स्वतः को अनधिकृत प्रोग्राम दर्शाने हेतु नियंत्रण प्राप्त कर लेता है।24

ई-मेल स्पूफिंग- एक स्पूफिंग किया गया अपराध उसे कहते हैं जो ई-मेल का दुर्व्यसन, गलत बयानी करता है अर्थात उसे मूल पाठ की चालाकी से परिवर्तित कर दिया जाता है। उदाहरण यदि अ किसी धमकी भरा ई-मेल स्वयं के नाम की बजाय ब के नाम से करता है जो कि ई-मेल प्राप्त करता है, मित्र है तो अ द्वारा किया गया ई-मेल स्पूफिंग कहा जाएगा।

कम्प्यूटर वेल्डलिज्म- वेडलिज़्म का अर्थ किसी अन्य की संपत्ति को नष्ट करना। कम्प्यूटर के संदर्भ में यदि कोई व्यक्ति किसी व्यक्ति के कम्प्यूटर को क्षति पहुंचाता है, निरुपयोगी बनाता है तो वह कम्प्यूटर वेंडलिज़्म का दोषी माना जाएगा। किसी कम्प्यूटर की चोरी या उससे जुड़े हुए किसी अन्य भाग को विनष्ट करना स्पूफिंग का अपराध होगा।

मोबाइल फोन और साइबर अपराध

मोबाइल फोन द्वारा साइबर अपराधों की दुनिया में वृद्धि होती जा रही है। अश्लील एसएमएस, ई-मेल भेजना, यह धारा 67 आईटी एक्ट 2000 के तहत दंडनीय अपराध है। तमिलनाडु राज्य बनाम सुहास कुट्टी इममोर मद्रास मे मोबाइल फोन से भेजी गई अश्लील एसएमएस तथा धमकी के मामले में अभियुक्त को धारा 469, 809 भारतीय दंड विधि की धारा 67 आईटी एक्ट के तहत सजा सुनाई गयी। यह अश्लील एसएमएस प्रकरण के तहत भारत में साइबर कानून के तहत पहली बार सजा दी गयी थी। मोबाइल फोन फिकिंग करना भी अपराध माना जाता है। किसी

शब्द–ब्रह्म
E ISSN 2320 – 0871
भारतीय भाषाओं की अंतर्राष्ट्रीय मासिक शोध पत्रिका 17 अप्रैल 2017
पीअर रीव्यूड रेफ्रीड रिसर्च जर्नल

हैकर द्वारा किसी फोन लाइन को अवैध रूप से रोक कर उस नेटवर्क की सुरक्षा को तोड़ कर लंबी कॉल करना तथा फोन टेपिंग करना मोबाइल फोन फ्रीकिंग कहलाता है। यह आईटी एक्ट की धारा 63ए 65 व 66 के तहत अपराध माना जाता है।25

एटीएम और साइबर अपराध

जिस तरह से भारत में एटीएम कार्ड का चलन बढ़ता जा रहा है, उसी तेजी से इस कार्ड का दुरुपयोग भी होना शुरू हो गया है। कार्ड को क्लोन किया जा रहा है। क्लोन का अर्थ किसी चीज़ की हूबहु नकल तैयार करना। इसी तरह से क्लोनिंग वह प्रक्रिया है जिसमें असली बैंक कार्ड की मैग्नेटिक स्ट्रिप को कॉपी कर डुप्लीकेट कार्ड में दर्ज किया जाता है। कार्ड की माइग्नेटिक स्ट्रिप की कॉपी करने की इस प्रक्रिया को समान्य रूप से स्किमिंग कहा जाता है इसमे कार्ड को स्किमिंग उपकरण पर स्वाइप किया जाता है। यह उपकरण सेल्फ ऑफ पॉइंट पर स्वाइप करने हेतु उपलब्ध स्किमिंग उपकरण के समान होता है।26 कार्ड को स्वाइप करने पर कार्ड संबंधी सूचनाएं स्किमिंग उपकरण में दर्ज हो जाती हैं। फिर उसे दूसरे नकल कॉर्ड की मैग्नेटिक स्ट्रिप पर दर्ज कर लिया जाता है। इस प्रकार असली कार्ड की सारी सूचनाएं नकली कार्ड पर आ जाती हैं और यह कार्ड भी असली कार्ड की तरह कार्य करने लगता है।

धोखेबाज कैसे करते है

धोखेबाज़ी.- धोखेबाज तीन तरीके से कार्ड की क्लोनिंग करके पिन हासिल करके धनराशि का आहरण करते हैं। पहले कार्ड स्किमिंग उपकरण को एटीएम कार्ड रीडर पर लगा दिया जाता है, जो एटीएम क्रेडिट कार्ड की सूचनाओं को स्वाइप कर मैग्नेटिक स्ट्रिप पर दर्ज सूचना को कॉपी कर लेता है।27 इस स्कीमिग उपकरण के साथ एक छोटा कैमरा और रिकॉर्डिंग भी होती है, जो एटीएम की पैड पर आपके द्वारा दर्ज की जा रही पिन को रेकॉर्ड कर लेता है। दूसरा होटल, रेस्टोरेन्ट, पंप या अन्य बड़ी दुकानों पर टेलर या वेटर द्वारा स्वाइप के दौरान भी कार्ड की क्लोनिंग कर ली जाती है। तीसरा विश्वसनीय किन्तु चालबाज व्यक्ति कार्ड धारक से कार्ड सत्यापित कराने के नाम पर अन्य किसी बहाने से कार्ड प्राप्त कर कॉर्ड को स्वाइप कर लेता है।28

क्लोनिंग कब-कब होती है - 1 जब कोई व्यक्ति कार्ड धारक के पास आकार कार्ड से संबन्धित कोई जानकारी लेता है, उसके तुरंत बाद ही वह धोखाधड़ी से आहरण करता है, 2 धोखाधड़ी की घटना से पहले कार्ड धारक किसी ऐसे स्टोर में ख़रीदारी करता है, जो क्लोनिंग की गतिविधि में संलिप्त है।

क्लोनिंग की विशेषताएं - 1 कार्ड के क्लोन होने से थोड़ी ही देर मे धोखाधड़ी करने वाला अधिकतम धनराशि या पूरी धनराशि निकाल लेता है, 2 असली कार्ड धारक के पास रहते हुए क्लोन कार्ड से रकम निकाल ली जाती है। निकाली गयी रकम सामान्य तौर पर ग्राहक द्वारा अपनाए गए तरीके से भिन्न होती है। खरीदार एवं आहरण ऐसे स्थान से किया जाता है जहां ग्राहक कभी नहीं गया हो।

कार्ड धारक के लिए उपाय - कार्ड धारक अपने कार्ड से हुई लेन-देन की सूचना त्वरित बैंक को दे। अपने निजी कम्प्यूटर पर वायरस सुरक्षात्मक सॉफ्टवेयर लगाना, ऑनलाइन ख़रीदारी करते समय विशेष सावधानी रखनी चाहिए। अपना खाता, नए कार्ड समाप्त होने की तारीख तथा संबन्धित कंपनी का फोन नंबर सुरक्षित स्थान

पर रखना चाहिए। कार्डो की क्लोनिंग के कारण बैंको एवं ग्राहकों को हो रहे व्यापक नुकसान से बचाव के लिए विभिन्न देशों ने स्मार्ट कार्ड तैयार किया है। इस पर मैग्नेटिक स्ट्रिप की जगह स्मार्ट चिप लगाई जा रही है। इसके अतिरिक्त कार्डो पर आइरिस कोड, बायोमेट्रिक चिप, फिंगर प्रिंट लगाई जा रही है। इसके अतिरिक्त अलग पिन की भी जरुरत हो सकती है। स्मार्ट कार्ड भी क्लोनिंग से अछूता नही है, पर इसकी क्लोनिंग महंगी और कठिन है।29 भारत में क्लोनिंग कार्ड के अपराध के लिए न तो भारतीय दंड संहिता और न ही आई टी एक्ट 2000 में कोई प्रावधान है। डाटा संरक्षण के लिए कोई भी नियम नही बनाया गया। इसके लिए सरकार को सोचना पड़ेगा और शीघ्र ही प्रभावी सरकार का निर्माण करना पड़ेगा, ताकि कार्ड क्लोनिंग और धोखाधड़ी को कानून के दायरे मे लाकर उस पर प्रभावी अंकुश लगाया जा सके तभी तेजी से बढ़ते अपराधों को रोका जा सकता है।30

अरुण कुमार पाठक का मानना है कि सूचना तकनीकी कानून के तहत उल्लिखित आरोपों की सूची निम्नवत है - कम्प्यूटर संसाधनों से छेड़छाड़ की कोशिश, कम्प्यूटर में संग्रहीत डाटा के साथ छेड़छाड़ कर उसे हैक करना धारा 66, संचार सेवाओं के माध्यम से प्रतिबंधित सूचना भेजने के लिए दंड का प्रावधान करना 66 अ कम्प्यूटर या अन्य किसी ईलेक्ट्रोनिक गैजेट से चोरी की गयी सूचनाओं को गलत 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।31

सूचना प्रौद्योगिकी अधिनियम की परिधि में आने आले अपराध.

परांजपे के अनुसार अनधिकृत अधिनियम (Unauthorized access) अधिनियम की धारा 43 के अंतर्गत कोई भी व्यक्ति कम्प्यूटर सिस्टम या कम्प्यूटर नेटवर्क के स्वामी या इंचार्ज की अनुमति के बिना अनधिकृत अभिगमन करता है तो इससे प्रभावित व्यक्ति को प्रतिकर देगा जो एक करोड़ रुपए से अधिक राशि हो सकेगी। धारा 43 के प्रयोजनों के लिए निम्नलिखित को कम्प्यूटर या कम्प्यूटर नेटवर्क में अनधिकृत पहुँच (अधिगमन) माना जाता है। किसी कम्प्यूटर को अवैध रूप से स्विच ऑन करना किसी कम्प्यूटर में संस्थापित साफ्टवेयर प्रोग्राम का अनाधिकृत उपयोग करना। फ़्लापी डिस्क की अंतर्वस्तु को अवैध रूप से देखना, किसी कम्प्यूटर को अवैध रूप से बंद कर देना, अवैध रूप से कम्प्यूटर प्रिंट आउट निकालना, इंटरनेट को अवैध तरीके से लॉग ऑन करना, कम्प्यूटर से तीव्र घंटीनुमा ध्वनि उत्सर्जित करना।32 मूल रूप से सन 2008 में संशोधन द्वारा एक नई धारा 43 जोड़ दी गई है, जिसके अंतर्गत किसी व्यक्ति के कम्प्यूटर संसाधन में वैयक्तिक डाटा या जानकारी संरक्षित रखने में विफलता की स्थिति में प्रतिकर प्राप्त करने का अधिकार प्राप्त होगा। रिटर्न या जानकारी प्रस्तुत करने में विफल रखने का अपराध. धारा 44 के अनुसार यदि कोई व्यक्ति इस अधिनियम निर्मित के अधीन कोई दस्तावेज रिटर्न कंट्रोल या प्रामाणिक प्राधिकारी को प्रेषित करने के लिए आबद्ध है, परंतु वह इसमें व्यतिक्रम करता है या विफल रहता है तो उसे प्रत्येक विफलता के लिए जुर्माना डेढ़ लाख रुपए तक हो सकता है। अधिनियम के अंतर्गत बनाए गए नियमों का उल्लंघन सूचना प्रद्यौगिकी अधिनियम की धारा 45 के अधीन अधियम के अंतर्गत नियमों के

उल्लंघन को अपराध माना जाएगा। यद्यपि इसके लिए निश्चित जुर्माना (Penalty) विहीनित नहीं की गयी। अधिनियम की धारा 46 में उल्लंघन करने पर व्यक्ति को देय दंड या शास्तियों के न्याय निर्णय संबंधी प्रावधान है परंतु जुर्माना आधिरोपित करने से पूर्ण उसे अपना पक्ष प्रस्तुत करने का पूरा अवसर दिया जाना आवश्यक है।33

कम्प्यूटर जनित दस्तावेजों में हेरफेर करने को अधिनियम की धारा 65 के अनुसार कम्प्यूटर जनित दस्तावेजों का हेरा-फेरी को दंडनीय अपराध माना गया है। ऐसे दस्तावेज़ या कूट संकेतो को नष्ट करना, बदलना, छिपाना, दूसरों के साथ विनिष्ट करना, दूसरों के साथ कूट संकेत साधन को बदलना, इस अपराध के विभिन्न रूप हैं। इस अपराध के लिए तीन वर्षों का कारावास तथा दो लाख रुपए जुर्माने का दंड देय है।34 कंट्रोलर के निर्देश का पालन नही किया जाना. धारा 68 कंट्रोलर को अधिकृत करती है वह प्रमाणीकरण प्राधिकारी के किसी कर्मचारी को यह शक्ति प्रदान कर सकता है।

कम्प्यूटरजनित बौद्धिक सम्पदा अपराध. वर्तमान समय में इन्टरनेट तथा अंकीकरण के फलस्वरूप बौद्धिक सम्पदा अधिकार के उल्लंघकारियों को व्यापारिक गोपनीय तथ्यों, ट्रेडमार्क, लोगो आदि का अवैध रूप से डाउन लोड करके उन्हें अवांछित उद्देश्यों के लिए वितरित करना आसान हो गया है। इसी प्रकार कम्प्यूटर सोर्स कोड की चोरी करके भी उन्हें अपने लक्षित पीड़ित की गोपनीय व्यापारिक सूचना या संदेश हासिल करके उनका दुरुपयोग कर सकते हैं। ट्रेडमार्क भी बौद्धिक संपदा का अधिकार है जो व्यापरियों को साख और प्रतिष्ठा को संरक्षण प्रदान करता है। इससे व्यापारी की व्यापार जगत में इनके माल को लेकर एक पहचान बन जाती है। ट्रेड मार्क अधिनियम की धारा 2 (1), (2), को ट्रेडमार्क को परिभाषित किया गया है।35 पार्सिंग ऑफ भी ट्रेडमार्क अधिनियम के अधीन दंडनीय है। पार्सिंग ऑफ से आशय अपने घटिया माल को किसी प्रतिष्ठित व्यापारी का गुणवत्ता वाला माल बताते हुए खपा देना तथा इस प्रकार ग्राहकों को धोखा देकर या भ्रमित कर अनुचित लाभ कमाना। यदि ये गतिविधियाँ इंटरनेट के माध्यम से संचालित की जाती हैं तो यह एक दंडनीय अपराध होगा। इस संदर्भ में रेडिफ़ कम्यूलिमिटेड बनाम साइबर बूथ एंड रमेश नाहटा के बाद मे बंबई उच्च न्यायालया ने विनिर्दिष्ट किया कि किसी व्यावसायिक या व्यापारिक प्रतिष्ठान का डोमेन नाम उसका केवल इंटरनेट पता मात्र नही होता बल्कि यह उस प्रतिष्ठान के व्यापार चिह्न या सेवा चिन्ह यथास्थिति की भाँति होता है, जिसका उल्लंघन किया जाना साइबर अपराध कहलाता है। सत्यम इन्फोवे लिमिटेड बनाम मेसर्स बनाम सीफ़िनेट साल्यूशन्स प्राइवेट लिमिटेड के वाद में उच्चतम न्यायालय ने विनिश्चित किया कि इंटरनेट के माध्यम से वाणिज्य गतिविधियों के संचालन के बढ़ते हुए चलन के अब व्यापारिक या व्यावसायिक प्रतिष्ठानो का डोमेन नाम भी व्यापार का चिह्न माना जाना लगा।36

साइबर अपराधों के निवारण हेतु विधिक सहायता

विधि का मुख्य प्रयोजन समाज की आवश्यकताओ की पूर्ति करना तथा शांति व्यवस्था बनाए रखना है। सामाजिक परिवर्तन के साथ विधि में भी परिवर्तन करना आवश्यक होता है। वर्तमान में 21वी सदी में कंप्यूटर युग में अनेक ऐसे नए अपराध अस्तित्व में आए जिनके

बारे में पहले कभी कल्पना भी नही की जा सकती थी और अब साइबर अपराध एक दूसरे से दूरस्थ देशों में विभिन्न जगहों पर भारित होना संभव हो गया है, जबकि अपराधी का अपराध के स्थान पर उपस्थित रहना आवश्यक नहीं। इसमें कम्प्यूटर नेटवर्क के माध्यम से डाटा की चोरी, अश्लील सामग्री का प्रसारण, अनधिकृत अधिगमन, वाणिज्यक बैंको में धोखाधड़ी, गबन आदि के साइबर अपराध बहुत जटिलता से घटित हो रहे हैं। इसलिए विधि परिवर्तनकारियों के लिए साइबर स्पेस में घटित होने वाले अपराधों पर नियंत्रण रखना कठिन होता है। यद्यपि व्यावहारिक दृष्टि से इंटरनेट का उपयोग करने वाला व्यक्ति ऑनलाइन गतिविधियों के लिए अपने देश के विधि द्वारा प्रसारित होता है परंतु जब दूरसंचार देश के बाहर पारेषित किया जाता है और उसके संबंध में कोई विवाद की स्थित उत्पन्न होती है तो उन्हे हल करने हेतु कोई अंतरराष्ट्रीय साइबर कानून अस्तित्व में नहीं होने के कारण समस्या उत्पन्न हो जाना स्वाभाविक है।

भारतीय दंड संहिता में साइबर अपराधो से संबन्धित निम्नलिखित प्रावधान हैं -

ई मेल के माध्यम से ऐसे संदेश भेजना जिससे मानहानि होती हो जो आई पी सी की धारा 499 है

फर्जी इलेक्ट्रोनिक रेकॉर्ड्स का इस्तेमाल आई पी सी की धारा463

फर्जी बेबसाइट या साइबर फ्रॉड आई पी सी की धारा 420

चोरी छिपे किसी के मेल पर नजर रखना आई पी सी की धारा 463

वेब हैकिंग आई पी सी की धारा 383

ई-मेल का गलत इस्तेमाल आई पी सी की धारा 500

दवाओं को ऑनलाइन बेचना एनडीपीएस एक्ट

हथियारों की ऑनलाइन खरीद-बिक्री आर्म्स एक्ट 37

साइबर अपराधों पर अंकुश लगाने के लिए पीपीसी परियोजना.

इन अपराधों को पीपीसी के तहत रोकने का प्रयास किया जा रहा है। सिक्यूरिटी सेवा से जुड़ी कंपनी के कार्यकारी निदेशक ने कहा डेटा सुरक्षा के महत्व को नकारा नही जा सकता चाहे वह सरकारी क्षेत्र हो या निजी क्षेत्र। बड़ी कंपनियों के चोरी रूकने के उपाय हैं, लेकिन मझोली और छोटी कंपनियों में ऐसी सुविधा का अभाव है। उन्होंने कहा कि इसके अलावा सरकारी विभागों का डाटा सुरक्षा तंत्र को मजबूत बनाने की आवश्कता है। इसका एक बेहतर तरीका यह है कि साइबर अपराधों पर अंकुश के प्रयासों के निजी क्षेत्र को शामिल किया जाय। एक अन्य साइबर सुरक्षा विशेषज्ञ ने डेटा लीकेज और चोरी के बारे मे जागरूकता बढ़ाने पर जोर दिया। उन्होंने कहा कि निजी क्षेत्र में डाटा लीकेज के मामले आते हैं। सरकारी वेबसाईटों को भी हैक किए जाने के प्रयास हुए। बहुत से लोग इन अपराधों की सूचना नहीं देते। उन पर अंकुश एक बेहतरीन सूचना प्रणाली है। राष्ट्रीय अपराध रेकॉर्ड ब्यूरो ने भी माना कि पिछले कुछ वर्षों में साइबर अपराधो में बढ़ोतरी हुई है।38

साइबर अपराध को करने में सुदरलैंड का मानना था कि इस अपराध को करने वाले भी प्रतिष्ठित व संभ्रांत वेशभूषा वाले ऐसे उच्च वर्ग के लोग हैं, जो शिक्षा, बुद्धि, आवेश स्थिति को प्राप्त कर नियोजित ढंग से अपराध जैसे कार्यों के लिए प्रेरित हो जाते हैं। प्रसिद्ध समाजशास्त्री रोबर्ट

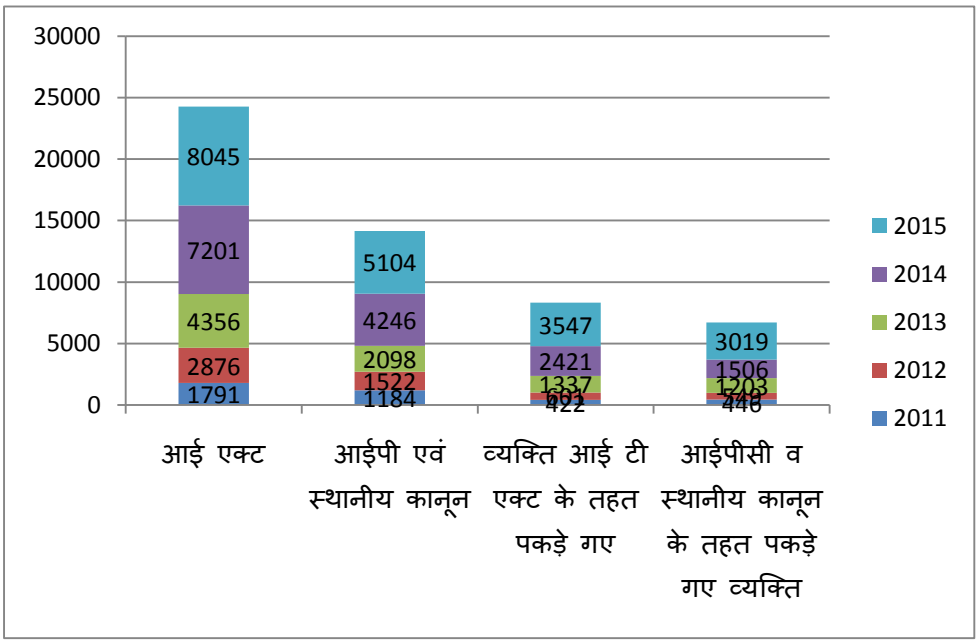
मार्टन के अनुसार मानव संरचनात्मक प्रकार्यवाद के सिद्धांत के अनुसार प्राथमिक हित व लाभ को लक्ष्य बनाता है और परिस्थितियो के अनुसार आपराधिक प्रेरणा को तजब्बो देता है। ऐसे अपराधो को निरूपित करते हुए मैक्स बेबर ने सुझाव दिया कि असीमित इच्छा पूर्ति की चाहत से लोगों में विचलन की स्थिति निर्मित होती है, जिससे व्यक्ति के सामाजिक सम्बन्धों में तीव्र परिवर्तन आता है, जो सामाजिक मूल्यों और नियंत्रण को कम कर देता है। इस स्थिति में सामान्य व्यक्ति में पारम्परिक विश्वास व मूल्यों में कमी तथा निराशा में बढ़ोत्तरी होने के कारण समाज में अपराध जैसी बुराईयाँ पनपती हैं। इसी तारतम्य में पारसंस द्वारा सुझाए गए संरचना और मूल्यों के सिद्धांत की महत्ता सामने आती है, जिससे यह निर्दिष्ट किया गया है। मानव व्यवहार के नियंत्रण एवं उसे व्यवस्थित करने के लिए विघटन उत्पन्न करने वाली प्रवृतियों पर नियंत्रण जरूरी हो जाता है। इसके साथ ही अपराध के खिलाफ अभिमति भी आवश्यक हो जाती है, जिसके अभाव में अपराधों के प्रति सामाजिक भेद्यता भी बढ़ जाती है। हर्बर्ट स्पेन्सर द्वारा सुझाए गए सिद्धांत अतित्व के लिए संघर्ष की महत्ता भी साइबर अपराध को बढ़ावा देती है। उन्होंने यह भी बताया कि उपयुक्त योग्यता वाले व्यक्ति अपनी सफलता के लिए शीघ्र ही अनुकूल या समझौते कि स्थिति भी प्राप्त कर लेता है। इलिएट, मेरिल तथा सेठना ने सुझाव दिया कि सामाजिक नियंत्रण के अभाव में सफेदपोश लोग व्यक्तिवादी धारणाओं के कायल हो जाते हैं और अपने लाभ के लिए दूसरे को हानि पहुंचाते हैं।39

भारत में वर्ष 2015 में साइबर अपराधों की कुल संख्या 11592 थी, जिसमें 8121 व्यक्ति पकड़े गए जिसके तहत सूचना तकनीकी अधिनियम, भारतीय दंड संहिता, स्थानीय व विशेष कानून के ये अपराध घटित हुए, जबकि 2014 में कुल अपराधों की संख्या 9623 थी। इस वर्ष का आंकडा पिछले वर्ष के आंकड़े से 20 प्रतिशत अधिक है। 2015 में सबसे अधिक साइबर अपराध उत्तर प्रदेश में सामने आये जो कुल अपराधों का 19 प्रतिशत था। उसके बाद महाराष्ट्र और कर्नाटक जैसे राज्य शामिल थे।

अपराध	**2013**	**2014**	**2015**	**2013 (पकड़े गए व्यक्ति)**	**2014 (पकड़े गए व्यक्ति)**	**2015 (पकड़े गए व्यक्ति)**
सरकारी अधिकारी	11	06	00	2	0	0
ईलेक्रोनिक रेकॉर्ड	12	01	04	11	02	02
धोखाधड़ी		1115	2255		355	754
Forgery	747	63	45	626	58	72
डाटा चोरी	55	84	52		11	72
फ्राड	518	54	42	471	39	135
काउंटर फिटिंग	59	10	12	93	8	1292
अन्य	974	980	8.6		772	598
कुल	1337	2272	3422	1203	1224	2867

Source (NCRB- 2015)

शब्द–ब्रह्म
E ISSN 2320 – 0871
भारतीय भाषाओं की अंतर्राष्ट्रीय मासिक शोध पत्रिका
17 अप्रैल 2017
पीअर रीव्यूड रेफ्रीड रिसर्च जर्नल



Source (NCRB- 2015)

भारत में साइबर अपराध रोकने के विविध तरीके अपनाए जा सकते है जो इस प्रकार है

- संचार जाल की सुरक्षा की जाय
- तकनीकी का इस्तेमाल सही ढंग से किया जाय
- प्रबंधात्मक तरीके से कार्य हो
- गलत सूचना देने वालों को अपराध के दायरे में रखा जाय
- नेट कार्यकर्त्ता खुद अपना सुरक्षा भी करे
- समबन्धित क़ानूनों को उदार बनाया जाय
- कम्प्यूटर या लैपटाप में इस तरह के सॉफ्ट वेयर का प्रयोग किया जाय कि जब कोई अवैध साइट खुले तो उसमें से आवाज निकले जिसके माध्यम से ऑपरेटर को पता चल जाय की यह अवैध साइट है
- साइबर फोरेंसिक और बाओमेट्रिक तकनीक का इस्तेमाल हो
- कम्प्यूटर अपराध से जुड़े विकास सेंटर को स्थापित किया जाय
- सार्वभौमिक कननूनी प्रबंधात्मक नियम को स्थापित किया जाय
- वैश्विक स्तर पर डिजिटल कननून बनाया जाय
- सार्वभौमिक स्तर पर साइबर कानून को आवश्यक बनाया जाय
- कम्प्यूटर टीम के माध्यम से इंटरपोल और आपात कालीन सेवा उपलब्ध कराया जाय
- विशेष साइबर अपराध को ढूढ़ा जाय
- ई ज्यूसियरी व वीडियो कन्फ्रेंसिंग के जरिये न्याय उपलब्ध कराया जाय 40

निष्कर्ष

साइबर अपराध ऐसा अपराध माना जाता है जिसमें अपराधी प्रत्यक्ष तौर पर नजर नही आता बल्कि छिप कर वार करता है और फिर कही गुम हो जाता है। हालांकि इस तरह के अपराध में अपराध में अपराधी को पकड़ना अन्य अपराधो की तुलना में और भी गंभीर हो जाता हैए

कई बार ऐसा भी मामला सामने आता है कि अपराधी अपना पता बार.बार बदलता रहता हैए इसके लिए पुलिस प्रशासन और अन्य एजेंसियों को अपने कार्यों में बदलाव करना पड़ता है । हालांकि सर्वाधिक मात्रा में अपराध आई टी सेक्टर में सामने आता है उसके बाद आई पीए व्यक्तिगत और सबसे कम स्थानीय स्तर पर देखा जाता है। परंतु यदि हम राष्ट्रीय अपराध रिकॉर्ड ब्यौरों पर नजर डाले तो पाते है की इसकी तदात हर वर्ष बढ़ती जा रही हैएचाहे वह क्लोनिंग की समस्या हो या फिर अन्य समस्या हर तरीके से इसे निपटने के लिए आवश्यक कदम उठाने की जरूरत है तभी इस साइबर अपराध को रोका जा सकते है।

सन्दर्भ ग्रन्थ

1 ना.वि.परांजपे, अपराधशास्त्र, दंड प्रशासन एवं प्रपीड़न शास्त्र, इलाहाबाद सेंट्रल ला, 2012, पृ 130-135

2 सुखविन्दर सिंह धारी, साइबर क्राइम एंड इट्स प्रोटेक्शन इन इंडिया, इंडियन पुलिस जर्नल, जनवरी मार्च.2014, वॉल्यूम 51, पृ 85-102

3 इन्द्रेश कुमार मिश्र, साइबर अपराध कानून एवं पुलिस, पुलिस विज्ञान, जनवरी-मार्च 2016, अंक 134, पृ. 45-49

4 देबारती हदर एंड के जयशंकर साइबर क्राइम एंड द विक्टिमाइजेशन ऑफ वुमेन लॉ राइट एंड रेग्युलेशन, यू एस ए. इंटेरनेशनल साइन्स एंड रेफरेन्स, 2012, पृ. 14

5 मार्को गारके, अण्डरस्टैंडिंग साइबर क्राइम, फेनोमीना, चेलेन्जेस एंड लीगल रेस्पोंसेस, न्यूयार्क डेवलपमेंट सेक्टर, 2012, पृ. 97

6 वही

7 मार्को गारके, अण्डरस्टैंडिंग साइबर क्राइम फिनामिना चेलेजेंस एंड लीगल रेस्पोंसेस, न्यूयार्क, डेवलपमेंट सेक्टर 2012, पृ. 97

8 रुससेल जी स्मिथ, साइबर क्राइम रिसर्च (आस्ट्रेलियन इंस्टीट्यूट ऑफ क्रिमिनोलोजी, 2014) पृ 1-20

9 तकलो नस्त्सुई, साइबर क्राइम इन जापान, रिसेंट केसेस लेजीस्लेसनए प्रॉबलम एंड पेरस्पेक्टिव, मैजी, यूनिवरसिटि 2012 पृ 1.22

10 कलूम जेफफरी द थ्रेत ऑफ साइबर क्राइम टू द यू के, (रूसी थ्रेयत असाइनमेंट, जून, 2014) पृ 1-10

11 हरप्रीत सिंह एंड दोल्लांद गीता साइबर क्राइम ए थ्रेट टु पर्सन, प्रॉपर्टी गवर्नमेंट एंड सोसाइटी इंटेरनेशनल जर्नल ऑफ इंजीन्यरिंग साइन्स एंड इनर्जी टेक्नोलोजी, वॉल्यूम 31, 5 मई 2013 पृ.2-7

12 राज सामनी, साइबर क्राइम एक्स्पोज्ड (फरान्सिस्को इंटेल, 2014) पृ. 1-18

13 अरुण कुमार पाठक, क्रेडिट डेबिट कार्ड से बढ़ती धोखाधड़ी समस्या एवं समाधान, पुलिस विज्ञान, अप्रैल-जून, 2014, पृ. 20-23

14 हरप्रीत सिंह एंड दोल्लांद गीता साइबर क्राइम ए थ्रेट टु पर्सन, प्रॉपर्टी गवर्नमेंट एंड सोसाइटी इंटेरनेशनल जर्नल ऑफ इंजीन्यरिंग साइन्स एंड इनर्जी टेक्नोलोजी, वॉल्यूम 31, 5 मई 2013, पृ.2-7

15 इन्द्रेश कुमार मिश्र, साइबर अपराध कानून एवं पुलिस, पुलिस विज्ञान, जनवरी-मार्च, 2016, अंक 134, पृ. 45-49

16 अरुण कुमार पाठक, क्रेडिट, डेबिट कार्ड से बढ़ती धोखाधड़ी समस्या एवं समाधान, अंक 127, अप्रैल-जून 2014, पृ.33-38

17 निधि एंड प्रीति सक्सेना, डिजितलाइजेशन टेरोरिज़्म दी टेक्नोलोजिकल एडवानसेस ऑफ क्राइम इंडियन पुलिस जर्नल जनवरी-मार्च, 2014, वॉल्यूम 51 न. 85-102

18 अरुण कुमार पाठक, क्रेडिट, डेबिट कार्ड से बढ़ती धोखाधड़ी समस्या एवं समाधान, अंक 127, अप्रैल-जून 2014, पृ.33-38

19 ना.वि. परांजपे, अपराधशास्त्र, दंड प्रशासन एवं प्रपीड़न शास्त्र, (इलाहाबाद, सेंट्रल ला, 2012) पृ. 130-135

20 वही

21 रवि कुमार पटेल एवं धवन कटारिया, इवेलुएशन ऑफ साइबर क्राइम इन इंडिया, इंटरनेशनल जर्नल ऑफ ट्रेड एंड टेकनोलोजी इन कम्प्यूटर साइंस, वॉल्यूम 2, इश्यु 4 जुलाई-अगस्त, 2013 पृ 1-20

22 सुमंजीतदास एंड तपस्वीनी नायक, साइबर क्राइम इन इंडिया, इंटरनेशनल जर्नल ऑफ इजीनियरिंग साइंस एंड एनर्जी टेक्नोलोजी, अक्टूबर 2013, वॉल्यूम 6, इश्यू पृ 142-153

23 ना.वि. परांजपे, अपराधशास्त्र, दंड प्रशासन एवं प्रपीड़न शास्त्र (इलाहाबाद सेंट्रल ला, 2012 पृ. 130-135

24 ना.वि.परांजपे, अपराधशास्त्र, दंड प्रशासन एवं प्रपीड़न शास्त्र, (इलाहाबाद सेंट्रल ला 2012, पृ. 130-135

25 अरुण कुमार पाठक, मोबाइल फोन एवं साइबर क्राइम, पुलिस विज्ञान, अंक 123, अप्रैल-जून 2013, पृ.14-16

26 रवि कुमार एस पटेल और धावक कथिरिया, इवेल्युएशन ऑफ साइबर क्राइम इन इंडिया, इंटेरनेशनल जर्नल ऑफ एमेर्जिंग ट्रेंड्स एंड टेक्नोलोजी इन कम्प्यूटर साइंस, वॉल्यूम 2 इश्यू 4 जुलाई-अगस्त 2013 पृ 1-4

27 अरुण कुमार पाठक, क्रेडिट, डेबिट कार्ड से बढ़ती धोखाधड़ी समस्या एवं समाधान, अंक 127, अप्रैल-जून 2014, पृ.33-38

28 वही

29 अरुण कुमार पाठक, मोबाइल फोन एवं साइबर क्राइम, पुलिस विज्ञान, अंक,123, अप्रैल-जून 2013 पृ.14-16

30 रवि कुमार एस पटेल और धावक कथिरिया, इवेल्युएशन ऑफ साइबर क्राइम इन इंडिया, इंटेरनेशनल जर्नल ऑफ एमेर्जिंग ट्रेंड्स एंड टेक्नोलोजी इन कम्प्यूटर साइंस, वॉल्यूम 2 इश्यू 4, जुलाई-अगस्त 2013 पृ .1-4

31 वही

32 ना.वि. परांजपे, अपराधशास्त्र, दंड प्रशासन एवं प्रपीड़न शास्त्र, (इलाहाबाद सेंट्रल ला 2012) पृ. 130-135

33 श्रीमती बृजवाला ठाकुर, दस्तावेज/ अंगुलचिन्हों और मौका ए वारदात के दृश्यों का फोटोग्राफी, पुलिस विज्ञान, अंक 134, जनवरी-मार्च 2016, पृ. 36

34 ना.वि. परांजपे, अपराधशास्त्र, दंड प्रशासन एवं प्रपीड़न शास्त्र, (इलाहाबाद सेंट्रल ला 2012) पृ. 130-135

35 वही

36 श्रीमती बृजवाला ठाकुर, दस्तावेज, अंगुलचिन्हों और मौका ए वारदात के दृश्यों का फोटोग्राफी पुलिस विज्ञान, अंक 134, जनवरी-मार्च 2016, पृ. 36

37 अरुण कुमार पाठक, क्रेडिट-डेबिट कार्ड से क्लोनिंग से बढ़ती समस्या एवं समाधान अंक 127, अप्रैल-जून 2014 पृ 20

38 वही

39 अरुण कुमार पाठक, क्रेडिट-डेबिट कार्ड से क्लोनिंग से बढ़ती समस्या एवं समाधान अंक 127, अप्रैल-जून 2014 पृ 20

40 श्रीमती बृजवाला ठाकुर, दस्तावे, अंगुलचिन्हों और मौका ए वारदात के दृश्यों का फोटोग्राफी पुलिस विज्ञान, अंक 134, जनवरी-मार्च 2016, पृ. 36