PUNE RESEARCH SCHOLAR ISSN 2455-314X
AN INTERNATIONAL MULTIDISCIPLINARY JOURNAL VOL 3, ISSUE 2

साइबर अपराध :
इंटरनेट के बढते प्रसार की एक चुनौती

सरोज बाला
शोध छात्रा शिक्षा विभाग
राजस्थान विश्वविधालय
जयपूर राजस्थान **भारत**

जहां एक और २१वीं सदीं के लिए नई—नई सूचना प्रौधोगिकी एक वरदान सिद्व हो रही है वहीं दूसरी और इसका गलत इस्तेमाल मानव जाति के लिए अफिषाप भी बनता जा रहा है।पिछले कुछ दिनों से समाज के सामने एक बहुपयोगी साधन के रुप में इंटरनेट ने एक चमत्कारी उदाहरण पेष किया है और लोगों के जीवन को काफी सरल भी बना दिया है किन्तु हर एक सिक्के के दो पहलू होते हैं। इसी के साथ एक नये अपराध का जन्म हुआ जिसे साइबर क्राइम के नाम से जाना जाता है। आज तक समाज में दो तरह के अपराध :—एक सिविल एवं दूसरा क्रिमिनिल आदि का फैलाव था किन्तु आधुनिक तकनीकी ने आधुनिक अपराध पैदा कर दिया जिसका नियंत्रण ही असम्भव प्रतीत जान पड़ता हैं। यहां तक कि केन्द्र सरकारए सुप्रीम कोर्ट तक के दखल देने की नोबत आ गई हैं। एक षोध में पाया गया की इंटरनेट पर आने वाले स्पैम मेल और फिषिंग जैसी घटनाएं खूब हो रही हैं। इस तरह के स्पैम इंटरनेट नेटवर्को में से स्पेक्टानेट सबसे ज्यादा बदनाम है। पिछले साल के अंत में भारत समेत दुनिया भर के लाखों कंप्यूटरों में स्टक्सनेट वार्म का संक्रमण पाया गया। पहला साइबर क्राइम १८२० में देखा गया। आधुनिक समय में इसका क्षेत्र अत्यंत व्याप्त हो गया है। अकेले भारत में अब तक ५०० से अधिक मामलें सामने आ चुके हैं तो सम्पूर्ण विष्व क्या हाल होगाघ अत: साइबर अपराध का अर्थ जाने बिना इसका वर्णन अधूरा होगा इसलिए सबसे पहले साइबर अपराध को परिभाशित करते हैं।

क्या हैं साइबर अपराध:—

यह इस प्रकार की एक आपराधिक गतिविधि है जिसमें कंप्यूटर और इससे जुडे नेटवर्को को साधन के तौर पर प्रयोग किया जाता हैं। उदाहरण के लिए आंकडों से छेड़छाडएबिना अनुमति दूसरे की जानकारी हासिल करनाए आंकड़ों को हटानाए बौधिक संपदा की चोरी जैसी घटनाएं षामिल है। इसके अलावा राश्ट्रीय सुरक्षा से जुड़े महत्वपूर्ण सुचनाओं की हैंकिंगए किसी को डराने के इमेल का प्रयोगए किसी दूसरे की पहचान को चुरानाए यौन उत्पीड़नए .मानहानिए स्पैम और फिषिंग करना भी साइबर अपराध की कैटेगरी में आता हैं। साइबर अपराध के मामले में भारत का विष्व में १३ वां स्थान है। साइबर अपराध के बढ़ने की वजह इंटरनेट के इस्तेमाल व ई—कामर्स का बढ़ता बाजार है।

साइबर क्राइम का वर्गीकरण:—

तकनीकी दृश्टि से यह दो प्रकार का हो सकता हैए पहले प्रकार में एक कंप्यूटर को लक्ष्य के रुप में प्रयोग करके दूसरे कंप्यूटरों पर आक्रमण करना जैसे—हैंकिगए वायरसए वर्मस तथा डोस आक्रूमण आदि। दूसरे प्रकार में कंप्यूटर का प्रयोग एक षस्त्र के रुप में किया जाता है जैसे—साइबर टेररिज्मए बौद्रिक सम्पदा अधिकारों का उल्लघंनए क्रेडिट कार्ड धोखाधड़ी एब्लैकमेंलिंगए अष्लील सामग्री का वितरण इत्यादि। इसके अलावा कुछ प्रमुख साइबर क्राइम है—हैकिंग़एकंप्यूटर वायरस या वर्मसए इंटरनेट पाइरेसीए टोजन लाजिक बम या ई—मेल बांबिंगए डाटा डिडलिंग तथा इंटरनेट टाइम चोरी आदि जो प्रतिदिन देखे जा सकते हैं।

साइबर हमलें जो करते हैं इंटरनेट बेहाल:—

१.संदेषों की बौछार:—साइबर हमलावर सर्वर पर भारी संदेषों की बौछार कर देते हैं। इससे सर्वर जाम हो जाता है व काम करना बंद कर देता है।

२.फर्जी आवेदन:—इसके तहत हमलावर सर्वर पर हर सेकेंड लाखों फर्जी आवेदन भेजता रहता है व जब सर्वर इन आवेदनों का निस्तारण करने की कोषिष करता है तो वह ठप पड़ जाता हैं।

३.डीएनएस पर निषाना:—डोमेन नेम सिस्टम पर हमला करके लाखों —करोड़ों संस्थाओं से अवांछित जानकारियां मांगते है हमलावर। ज्योंहि ये संस्थाएं जानकारियां भेजती है तो सर्वर जाम हो जाता है व इंटरनेट सेवाएं ठप पड़ जाती है।

डदाहरण के लिए ऐसे ही साइबर हमलें एक ब्रिटिष कंपनी स्पैमहाज पर हुए जो हैकरों के निषानों पर तब आई जब उसने स्पैम पोस्ट करने के लिए साइबर बंकर नाम की होस्टिंग कंपनी को काली सूची में डाल दिया। इस तरह से साइबर ठप हो गया और पूरा जगत प्रभावित हुआ। इसी तरह की घटना मिस्त्र में एलेक्जैडिया के पास समुद्र में अंतराश्ट्रीय सबमैरीन केबल एसएमडब्ल्यू —४ में आई तकनीकी खामी के कारण सर्वर ठप होने पर देखने में आई। अभी हाल ही में हुए सर्वे में आया है कि साइबर अपराधी न केवल इंटरनेट सेवाओं को ही ठप्प करते है बल्कि वो लोगों की निजी जानकारी खोजकर सम्पति की लूट पाट भी करने लगें हैं। जैसे एटीएम से पैसे निकालना आदि।दूसरी और कुछ विकसित देष तो साइबर हथियारों की हौड़ में भी लगे हुए है। अरब बसंत की घटनाएंए जिनकी षुरुआत सामाजिक नेटवर्क के माध्यम से ही हुई थी और ईरान पर सामाजिक हमलें आदि यह स्पश्ट करते है कि भविश्य के युद्व साइबर हथियारों से लड़े जायेगें।

कैसे करते हैं हमला:—साइबर अपराधी साफटवेयर कोड से छेड़छाड़ करतें हैं और इसको मालवेयर के साथ मिला रहें हैं। इसकी मदद से साइबर अपराधी उपभोक्ताओं की निजी और वितीय सूचनाएं चूरा लेते हैं।इसके अलावा मालवेयर की मदद से साइबर अपराधी कंप्यूटर के माइक्रोफोन और वीडिया केमरा का रिमोट से चालू कर देते हैं। इससे साइबर अपराधियों को घर में या कंपनी के बोर्डरुम में घुसपैठ करने में सफलता मिल जाती है। उदाहरण के लिए मम्बई हमलों में भी आतंकवादियों ने **प्रोक्सी इंटरनेट सर्वर्स और वोयस ओवर इंटरनेट** प्रोटोकोल का प्रयोग कर पुलिस को भी चकमा दे दिया था।

साइबर अपराधों का समाज पर प्रभाव:—

भले ही देष टैक्नोलोजी के प्रयोग में आगे निकल गया हो किन्तु आज भी अनेकों समस्याएं समाज पर कुप्रभाव डाल रही हैं। क्या इंटरनेटध क्या फोन ध क्या अखबार और टीवी चैनल सब अषलिलता को प्रोसने में होड़ लगा रहे हैं। इस समय ८० करोड़ मोबाईल उपभोक्ता हैं। किसी महिला का नेकड चित्र फेसबुक पर अपलोड करना।जैसे कुछ दिन पहले नोएडा के स्कूल में छात्रों ने प्रिंसिपल तक को नहीं बकसा। क्या इनसे व्यक्ति के सम्मान को हानि नहीं होती ध क्या किसी आम आदमी से जानकारी लेकर उसके खाते को हैक करना व पैसे निकालना उचित है ध समाज के छोटे से तबके से लेकर बढ़े से बढ़े तक साइबर अपराधों की चपेट में हैं। देष की

सरकारी रक्षा व विज्ञान और षोध संस्थान व राजनयिक दूतावास पर भी साइबर जासूसी का आंतक मंडरा रहा हैं। ब्रिटिष अखबार गार्जियन के अनुसार अमेरिका ने पूरे विष्व में लगभग २०० से ७०० सर्वर लगा रखे हैं जिनमें से एक कहीं भारत में होने की भी सम्भावना हैं।

साइबर अपराधों से निपटने के लिए किये गये प्रावधान:

नेषनल **साइबर सिक्योरिटी पालिसी**:—देष में साइबर नेटवर्क की सुरक्षा के लिए सरकार नेषनल साइबर सिक्योरिटी पालिसी लेकर आई जिसका लक्ष्य नागरिक बिजनेस और सरकार को सुरक्षित साइबर स्पेस मुहैया कराना व साइबर खतरों से होने वाले नुकसान को कम करना है। इसके साथ ही लेनदेन सुरक्षा को और पुख्ता बनाने पर जोर दिया जा रहा है। इसके अलावा उत्पाद व तकनीकी प्रक्रयाओं को सुरक्षित बनाने पर जोर दिया जा रहा है। सूचना एवं संचार नेटवर्क की सुरक्षा करने के लिए चौबीसों घंटे निगरानी की व्यवस्था की जा रही है। इसके लिए नेषनल क्रिटिकल इंफोर्मेषन इंफ्रास्टक्चर प्रोटेक्षन सेंटर बनाया गया है जिससे डिजायन व अधिग्रहण डेवलपमेंट एवं इस्तेमाल के समय सुरक्षा प्रक्रियाओं को अपनाना अनिवार्य कर दिया गया है।

साइबर अपराधों से निपटने के लिए किये आईटी एक्ट २०००:—

मोजूदा आईटी एक्ट में किये गये प्रावधान वर्तमान परिपेक्ष्य में इतने सक्षम सिद्व नहीं हो पाये जितना इन्हें होना चाहिए। इंटरनेट के बढ़ते इस्तेमाल को देखते हुए इसमें २००८ में संषोधन किया गया किन्तु अब मोबाईल के बढ़ते प्रसार को देखते हुए इसमें कोई खास प्रावधान नहीं किया गया। जबकि २०१३ में विधानसभा एवं २०१४ में लोकसभा चुनावों में मतदाताओं को लुभाने के लिए मोबाईल का भरपूर प्रयोग किया गया। इसी एक्ट के सेक्षन ६६ए में २०१२ में संषोधन किया गया जिसमें केस दर्ज करने से पहले सरकार की अनुमति लेना जरुरी किया गया है। वहीं दूसरी और सोषल मीडिया के दायरे में भी अब चौतरफा विकास देखने को मिला है। हालांकि इस दौरान आईटी एक्ट २००० सोषल मीडिया से जुड़े कानूनी व नीतिगत और नियंत्रण से जुड़े मुदे को प्रभावी तौर पर हल करने में उतना सक्षम नहीं बन पाया है। **उदाहरण** के लिए भारत में साइबर क्राइम से जुड़े मसलों में स्कूल और षैक्षणिक संस्थाओं में डराने—धमकाने के मामले भी षामिल हैं।माइक्रोसोफट के पिछले साल २५ देषों में साइबर बुलिंग को लेकर किये एक सर्वे के मुताबिक इंटरनेट इस्तेमाल करने वाले छात्रों में आधे से अधिक इसके षिकार हैं।यहीं नहीं आनलाइन अफवाह फैलाने

के भी कई मामलें आ चुके हैं।इन सभी को देखते हुये सुप्रीम कोर्ट तक को कहना पड़ा की आधार कार्ड बनाना अनिवार्य नहीं है क्योंकि इसमें प्रयुक्त निजी जानकारी भी सुरक्षित नहीं है। ऐसा ही एक बयान अभी हाल ही में आरटीआई कार्यकरता अरुणा राय ने भी दिया है कि आधार कार्ड की अनिवार्यता को हटाया जाये।हालांकि सरकार लोगों की निजता का ध्यान रखते हुए प्राइवेसी से जुड़े एक विधेयक पर काम कर रही है परन्तु फिलहाल वर्तमान एक्ट में पोर्न साईटों को रोकने के लिए कोई प्रावधान नहीं है।

राश्टीय **साइबर सुरक्षा नीति—२०१३:—**

साइबर स्पेस पर खतरों को देखते हुए केन्द्रीय संचार एवं सूचना प्रौधोगिकी मंत्रालय ने राश्टीय साइबर सुरक्षा नीति २ जुलाई २०१३ को जारी की जिसमें निम्नलिखित प्रावधान किये गये:

१.साइबर स्पेस में सूचना —संरचना को संरक्षित रखना २.साइबर खतरों को रोकने और उनके जवाब की क्षमता निर्मित करना।३.संस्थागत संरचनाओं दृलोगों प्रक्रियाओं. तकनीकी एवं सहयोग के समन्वय से साइबर दुर्घटनाओं के कारण होने वाली क्षति एवं प्रभाव को कम करना ४.देष में सुरक्षित साइबर पारिस्थितिकी का सृजन करना।५. राश्टीय एवं क्षेत्रीय स्तर पर २४ घंटे संकट प्रबंधन के प्रति सचेतनता की व्यवस्था करना।६.नेषनल क्रिटिकल इंफोर्मेषन इंफ्रास्टक्चर प्रोटेक्षन सेंटर के संचालन हेतु व्यवस्था करना।७.कौषल विकास एवं प्रषिक्षण के माध्यम को समर्पित ५ लाख विषेशज्ञों का कार्यबल गठित करना।८.साइबर सुरक्षा के लिए अंतराश्टीय सहयोग एवं समन्वय को बढ़ावा देना।९.राश्टीय स्तर पर कंप्यूटर इमर्जेंसी टीम की स्थापना करना।

अंतराश्ट्रीय स्तर पर साइबर क्राइम से निपटने के प्रावधान:—

पिछले दिनों दिल्ली में अंतराश्ट्रीय स्तर पर एक साइबर क्राइम से संबंधित सम्मेलन का आयोजन हुआ जिसमें मोजूदा परिस्थितियों को ध्यान में रखकर साइबर सुरंक्षा नीति बनाने की बात कही गई। इसी तरह अंतराश्टीय स्तर पर साइबर कानून में हो रहे बदलावों का न्याय क्षेत्र पर पडने वाले प्रभाव का मामला भी चर्चा में है। यह उन सभी संबंधित पक्षों पर प्रभाव डालेगा जिनका संबंध डिजिटल एवं मोबाइल इकोसिस्टम से है। ऐसे समय में जरुरत इस बात की है कि अंतराश्टीय स्तर पर एक

ऐसा नेटवर्क बनाया जाए जिसमें साइबर क्राइम और साइबर लीगल ला से जुड़े प्रोफेषनल षामिल हों।

भारत के संबंध में एक और तथ्य ध्यान देने योग्य है कि अब भी हमारे देष में ज्यादातर कंप्यूटर और मोबाइल उपकरण विदेषों से मंगाए जाते हैं। इनमें प्रयुक्त सेमीकंडक्टर चिप्स विदेषों में बनती हैं और ज्यादा साफटवेयर के कोड्स का स्वामित्व भी विदेषी ही हैं। यही नहींए निजी और सरकारी दोनों तरह की साइबर सेवाओं के लिए गूगलए माइक्रोसोफटए याहू फेसबुकए यू—टयूबए स्काइपए एंपलए एओएलए पैलटाक आदि जिन अमेरिकी इंटरनेट कंपनियों की सेवाएं ली जाती हैं.वे सारी कंपनियां फोरेन इंटेलिजेंस सर्विलांस एक्ट फीसा जैसे अमेरिकी कानूनों के तहत अपने सर्वरों पर रखा डाटा एनएसए यानि अमेरिका की राश्टीय सुरक्षा एजेंसी को देने के लिए बाध्य हैं। ऐसे में हमारी साइबर सुरक्षा का क्या होगा क्योंकि विदेषों में बैठे साइबर जासूस जब चाहे हमारी गोपनीय सूचनाओं को हैक कर सकता है।

बेषक हमारा देष राश्टीय साइबर सुरक्षा नीति लागू कर इन समस्याओं को सुलझाने की कोषिष कर रहा है.पर यहां यह ध्यान में रखना होगा कि साइबरस्पेस सीमाविहीन है और उसका स्वरुप अंतराश्ट्रीय है। ब्रिटेन जैसे देष साइबर आर्मी बनाने जा रहे हैं ऐसे में हमें भी इस दिषा में आगे सोचना होगा। इसलिए जरुरी है कि देष के संवेदनषील ठिकानों की सुरक्षा के प्रति सेना और सरकार के प्रतिश्ठानों के साथ—साथ उन लोगों को भी जागरुक किया जाए जो ईमेल.फेसबुक.टिवट्र से जुड़े हैं। और जिनकी अपनी कोई वेबसाइट है। इसी तरह देष की हवाई प्रतिरक्षा.यहां के परमाणु संयंत्र.वाणिज्य जगत से जुड़ी जानकारियां या दूरसंचार —प्रणाली—ये सभी साइबर खतरे से बचे रहें.इसके लिए राश्टीय नीति की घोशणा तो हुई है मगर उसे लागू करने का सही रोडमैप नहीं बन पाया है। अत: जितना जल्दी हो सकें सरकार को इस दिषा में सटीक कदम उठाने चाहिए अन्यथा साइबर जासूसी देष की सुरक्षा के लिए कभी भी बड़ा खतरा पैदा कर सकते हैं। मेरे विचार से विषेशज्ञों की एक टीम का गठन कर लोगों में इंटरनेट के सुरक्षित प्रयोग के प्रति जागरुकता अभियान चलाया जाना चाहिए।

संदर्भ सूचि :

कानून के स्त्रोत (रोडने डी रायडर)

कानून की शक्ति एवं राष्टीय सुरक्षा (लोरी पोलर)

आधुनिक समय में साईबर कानूनों की आवश्यकता (डेविड अस वैल)

शौध ग्रंथ (मिना कुमारी राजस्थान विश्वविधालय)

लगु शौध ग्रंथ (विकास कुमार महलोत्रा)