साइबर क्राइम की प्रकृति तथा सुरक्षात्मक उपाय

– डॉ. सुभि धुसिया

आज वास्तविक दुनिया के समानांतर 'साइबर वर्ल्ड' की दुनिया अपना आकार ले रही है और मोबाइल तक इंटरनेट की पहुँच हो गई है, लेकिन दिक्कत यह है कि 'साइबर स्पेस' जहाँ आंकड़ों व सूचनाओं का आदान–प्रदान होता है इसके लिए दुनिया भर में कोई प्रभावी नियामक व्यवस्था नहीं बनाई जा सकी है, तीसरी दुनिया के विकासशील देशों में जहाँ सूचना व संचार प्रौद्योगिकी अपने पाँव पसार ही रही है, वहाँ साइबर क्राइम के कारण हालात और भी चिन्ताजनक बने हुए हैं।

साइबर क्राइम की व्याख्या

अंतर्राष्ट्रीय विशेषज्ञों द्वारा साइबर क्राइम की निम्नलिखित परिभाषाएं दी गई हैं–

(1) पूर्वाग्रह से ग्रसित लोगों द्वारा सूचना व संचार तंत्र, कम्प्यूटर प्रोग्रामों, डाटा तथा आंकड़ों को बाधित करने का प्रयास, (मार्क पॉलिट एफबीआई यू.एस.ए.)।

(2) बाधाएँ उत्पन्न करने के प्रयास एवं कम्प्यूटर के माध्यम से लक्ष्य पर निशाना, (केविन कोलमैन, टेक्नोलाइटिक्स इंस्टीट्यूट, टेक्सास, यू.एस.ए.)

(3) राजनैतिक–सामाजिक–सांस्कृतिक या आर्थिक उद्देश्यों की पूर्ति के लिए देश की सरकार या देश के नागरिकों को डराने–धमकाने, प्रताड़ित करने तथा वित्तीय धोखाधड़ी करने के लिए कम्प्यूटर नेटवर्क तथा उसमें संरक्षित सूचनाओं एवं आंकड़ों को चोट पहुँचाने की कोशिश करना, चाहे वह किसी भी माध्यम से की गई हो (वैरी कोलिन, इंस्टीट्यूट ऑफ सिक्योरिटी एण्ड इंटेलीजेंस, कैलीफोर्निया, यू.एस.ए.)।

(4) कम्प्यूटर नेटवर्क को हैक करके उसमें संग्रहित आंकड़ों को चुराना और फिर अपने सामाजिक–राजनैतिक तथा व्यवसायिक प्रतिद्वन्द्वियों के खिलाफ उनका इस्तेमाल करना।

(5) सूचना तंत्र पर किसी भी प्रकार से चोट पहुंचाने की कोशिश जिसमें वेबसाइट तथा कम्प्यूटर की मदद से की गई कोई भी छेड़छाड़ शामिल है।

(6) साइबर स्पेस में ऐसी कोई भी गतिविधियाँ जो मूलतः मानवीय संवेदनाओं का अपमान कर सकती हैं अथवा सूचना तकनीक के जरिए सामाजिक–आर्थिक–राजनैतिक–सांस्कृतिक अथवा भावात्मक रूप से किसी को नुकसान पहुंचाना अथवा संकट में डालना (संयुक्त राष्ट्र संघ)।

भारत में 'आई टी कानून–2000' लागू होने के बाद सरकार क्राइम को पहली बार व्यवस्थित ढंग से प्रस्तुत किया गया। इस अधिनियम के अनुसार 'कोई भी ऐसा गैर कानूनी कृत्य जिसमें कम्प्यूटर एक औजार के रूप में इस्तेमाल किया गया हो या उसे लक्ष्य बनाया गया हो वह लक्ष्य तथा औजार दोनों हो, साइबर क्राइम कहलाता है।' साइबर टेररिज्म, साइबर–फ्रॉड, साइबर–ब्लैकमेलिंग, साइबर हैकिंग, साइबर वेब जैकिंग, पीसी हैकिंग इत्यादि साइबर क्राइम के ही रूप हैं। जब आतंकवादी गतिविधियों के लिए साइबर स्पेस का इस्तेमाल

किया जाता है तो वह 'साइबर टेररिज्म' कहलाता है। जब वित्तीय लेन–देन व क्रेडिट कार्ड फ्रॉड, पासवर्ड–बैंक एकाउंट एवं क्रेडिट कार्ड नम्बर चोरी करने के लिए साइबर स्पेस का इस्तेमाल किया जाता है तो यह 'साइबर–फ्रॉड' कहलाता है। इसी तरह अन्य प्रकार की परिभाषाएं भी दी जाती हैं। इसलिए साइबर क्राइम साइबर टेररिज्म, साइबर फ्रॉड इत्यादि में अधिक अन्तर करना सही नहीं है। हैं तो ये साइबर क्राइम के ही रूप, मगर लक्ष्य तथा उद्देश्य अलग–अलग होने के कारण ही इनकी अलग–अलग शब्दावली है, मसलन किसी एक देश द्वारा अपने प्रतिद्वन्द्वी दूसरे देश की सूचना प्रणाली में सेंध लगाने को 'साइबर–वार' की संज्ञा दी गई है। जाहिर है साइबर–क्राइम के अंतर्गत आने वाली इस प्रकार की भिन्न–भिन्न शब्दावली के कारण भ्रमित नहीं होना चाहिए।

साइबर क्राइम के सभी रूप ही व्यक्ति, समाज, देश तथा दुनिया की वैयक्तिकता, गोपनीयता, एकता तथा अखण्डता के लिए नुकसानदेह हैं, लेकिन 'साइबर–टेररिज्म' तथा 'साइबर–वार' ऐसे दो प्रारूप हैं जो सर्वाधिक भयावह साबित हो रहे हैं। भारत में विगत पाँच सालों में हुए आतंकवादी हमलों में सूचना एवं संचार माध्यमों का बड़ी बखूबी तथा चतुराई से उपयोग किया गया है।

साइबर क्राइम का वर्गीकरण

तकनीकी दृष्टि से साइबर क्राइम को दो भागों में वर्गीकृत किया जा सकता है–

(1) पहली श्रेणी के अंतर्गत कम्प्यूटर को एक 'लक्ष्य' के रूप में अन्य 'कम्प्यूटरों' पर आक्रमण करने के लिए प्रयुक्त किया जाता है, जैसे– हैकिंग, वायरस, वर्मस् तथा DOS आक्रमण, इसमें अन्य कम्प्यूटरों को हैक कर या उनमें वावरस डालकर उन्हें बाधित किया जाता है।

(2) दूसरी श्रेणी में अपराध करने के लिए कम्प्यूटर का उपयोग एक शस्त्र या हथियार के रूप में किया जाता है, जैसे– साइबर टेररिज्म, बौद्धिक सम्पदा अधिकारों का उल्लंघन, क्रेडिट कार्ड धोखाधड़ी, ब्लैकमेलिंग, अश्लील सामग्री का वितरण इत्यादि। इसमें साइबर–स्पेस का उपयोग अपने किसी भी प्रकार के कुत्सित स्वार्थों (आतंकी घटनाओं को अंजाम देना, किसी का अकाउंट या क्रेडिट कार्ड नम्बर लेकर वित्तीय फर्जीवाड़ा करना, किसी के डाटा व सूचनाओं में छेड़छाड़ करके उसे बदलना, अपने प्रतिद्वन्द्वी की गोपनीय या वैयक्तिक सूचनाओं को चुराकर उसके खिलाफ रणनीति बनाना, अश्लील–असामाजिक तथा उन्माद फैलाने वाली सामग्री का प्रसारण करना दुष्प्रचार या ब्लैकमेलिंग करना इत्यादि) की पूर्ति के लिए करना।

सैद्धांतिक रूप से विशेषज्ञों ने साइबर–क्राइम को तीन श्रेणियों में वर्गीकृत किया है–

(1) सरकार के विरुद्ध अपराध जैसे– साइबर टेररिज्म, जिसमें इंटरनेट के जरिए राजनैतिक–धार्मिक–सांप्रदायिक और इस तरह की कई विचारधाराओं के माध्यम से लोगों में आतंक एवं उन्माद फैलाना तथा आतंकी घटनाओं को अंजाम देने के लिए सूचना माध्यमों के द्वारा रणनीति बनाना।

(2) किसी खास व्यक्ति के विरुद्ध अपराध, जिसमें उस व्यक्ति की साइबर स्पेस में की गई हर प्रकार की छोटी से छोटी गतिविधियों पर नजर रखना तथा उसके बारे में ली गई सूचनाओं के द्वारा उसे हानि पहुंचाने का प्रयास करना।

(3) सम्पत्ति से जुड़े अपराध जिसमें किसी व्यक्ति की सम्पत्ति से संबंधित गोपनीय सूचनाएं, वित्तीय लेन–देन, बैंक एकाउंट, पासवर्ड या कार्ड से जुड़ी महत्वपूर्ण जानकारियों को हासिल किया जाता है।

कुछ प्रमुख साइबर अपराध

(1) हैकिंग– 'हैकिंग' शब्द का इस्तेमाल सर्वप्रथम 'मेसाच्युसेट्स इंस्टीट्यूट आफ टेक्नोलॉजी' (एम.आई.टी.) में किया गया था, उस समय इसका अर्थ था– ''कोई भी काम चालाकी से या विचारोत्तेजक नई शैली में करना'', मगर आज हैकिंग शब्द का इस्तेमाल सूचना व संचार प्रौद्योगिकी को नुकसान पहुंचाने के रूप में किया जाा रहा है। हैकिंग का शुरुआती मामला अगस्त 1986 में तब पकड़ा गया, जब कैलिफोर्निया यूनिवर्सिटी के ऑडिट में गड़बड़ी पाई गई। जाँच के बाद पता चला कि यह काम कुछ हैकर्स ने किया था। हैकिंग के द्वारा हैकर्स एक तरह से आपकी कम्प्यूटर प्रणाली पर कब्जा जमा लेते हैं और जब तक आपको पता चलता है तब तक वे आपके नेटवर्क का गलत उद्देश्यों के लिए इस्तेमाल कर चुके होते हैं। हैकर्स आपकी ई–मेल ट्रेस कर सकता है। आपकी ई–मेल आईडी, पासवर्ड या वेबसाइट का उपयोग अवांछित गतिविधियों में कर सकता है अथवा साइबर स्पेस में आपकी गतिविधियों पर नजर रखकर आपको नुकसान पहुंचा सकता है। इसके अलावा किसी कम्प्यूटर प्रणाली, कम्प्यूटर नेटवर्क, ई–मेल, साफ्टवेयर प्रोग्रामिंग, डाटा, मशीन कोड तथा मशीन कोड में बदलवाकर उसे ऑरिजनल फॉर्म से अलग करके हैकर सिस्टम को खत्म कर सकते हैं अथवा महत्वपूर्ण जानकारियाँ चुरा सकते हैं। मुम्बई, अहमदाबाद तथा बेंगलुरू में घटित आतंकी घटनाओं से पूर्व आतंकवादियों ने हैकिंग का तरीका अपनाकर ही अपनी रणनीतियों को अंजाम दिया। वेबसाइटों को हैक करने के लिए हैकर कई तरह के तरीके अपनाते हैं। वे ऐसे सॉफ्टवेयर का प्रयोग करते हैं जो मोडम का प्रयोग कर हजारों फोन नम्बर डायल कर कम्प्यूटर से जुड़े किसी अन्य मोडेम को ढूंढ़ता है। इसके अलावा कम्प्यूटर की प्रोग्रामिंग मशीन लैंग्वेज में लिखी होती है, जिसको कम्प्यूटर समझता है तथा जिसके आधार पर आपका बनाया गया प्रोग्राम काम करता है। हैकर इसी प्रोग्राम के बीच में दी गई कंडीशनल स्टेटमेंट जैसे– जंप, इफ को विभिन्न कंडीशन के द्वारा संतुष्ट कराकर हैकिंग करते हैं, वह इन स्टेटमेंट को किसी साफ्टवेयर के आधार पर पता करते हैं। साथ ही ऑपरेटिंग सिस्टम में कौन सी खामी है जिसके लिए पैच इंस्टाल नहीं किया गया है को जानने के बाद हैकर उसे हैक कर लेते हैं। इसके अलावा स्कैनर प्रोग्राम के द्वारा, नेटवर्क से जुड़े कम्प्यूटर्स के 'आईपी एड्रेस' को स्कैन कर ऐसा सिस्टम ढूंढ़ता है जो फिलहाल काम कर रहा हो।

(2) कम्प्यूटर वायरस/वर्मस्– यह एक खास तरह का प्रोग्राम होता है जिसे इस तरह विकसित किया जाता है ताकि वह कम्प्यूटर के डाटा को नुकसान पहुंचा सके। दूसरे शब्दों में कहें तो कम्प्यूटर वायरस संक्रामक बीमारी के वायरस की तरह स्वयं अपनी प्रतिलिपियों

को कम्प्यूटर के अन्य प्रोग्रामों से जोड़कर उन्हें संक्रमित कर लेता है, जिसके कारण मूल प्रोग्राम सुचारू रूप से काम नहीं करता और कम्प्यूटर की कार्य प्रणाली एवं क्षमता को पूरी तरह विघटित कर देता है। वायरस के अन्य विध्वंसक कार्य हैं– डाटा को डिलीट या खराब करना अथवा उसमें परिवर्तन करना, ड्राइव को पढ़ने योग्य न रहने देना, संचार व सूचना में बाधा डालना तथा कम्प्यूटर के सुरक्षा कॉरडॉन को तोड़ देना। वर्ष 1950 में 'जॉन वान न्यमेन' ने सर्वप्रथम कम्प्यूटर वायरस की कल्पना की थी। वर्ष 1987 में कमांड डॉट कॉम फाइलों को इफेक्ट करने वाले पहले वायरस का नाम 'लाइह' रखा गया। इसके बाद अस्तित्व में आए कुछ कुख्यात वायरस थे– सी–ब्रेन या पाकिस्तानी वायरस, लब–बग, लैटलिंग, ब्लडी, 8290 (पहला भारतीय वायरस) रेडलोफ, लवलेटर, लवगेट, सिरकेम इत्यादि। वर्ष 2000 में अस्तित्व में आए अकेले लव–बग वायरस ने अमरीका को 200 बिलियन डॉलर का चूना लगाया था। वायरस की खतरनाक विशेषता यह है कि वह अपने सम्पर्क में आने वाले अन्य कम्प्यूटर्स की हार्ड–हिस्क तथा फ्लॉपी को भी संक्रमित करता है और इस प्रकार नेटवर्क से जुड़े अन्य कम्प्यूटर्स में इसका क्रमशः प्रसार होता जाता है। यह ऑडियो, वीडियो, बर्ड या किसी अन्य शक्ल में हो सकता है। यह ई–मेल, पेन–ड्राइव व सीडी से डाटा ट्रांसफर करते समय या इंटरनेट से कोई फाइल डाउनलोड करते समय कम्प्यूटर में समा जाते हैं। इसी तरह वर्मस् जब किसी कम्प्यूटर में घुसते हैं तो तब तक अपनी प्रतिलिपियाँ बनाते जाते हैं जब तक उसकी मेमोरी का पूरा स्पेस खत्म न कर लें।

(3) इंटरनेट पाइरेसी– इंटरनेट पाइरेसी के बारे में आम यूजर्स को अधिक पता नहीं होता है, जबकि जाने–अनजाने वे भी इस काम को अंजाम दे चुके होते हैं अथवा इसका शिकार हो चुके होते हैं। इंटरनेट पाइरेसी भी साइबर क्राइम की श्रेणी में आता है। इंटरनेट पाइरेसी यानी किसी कॉपीराइट डिजिटल को गैरकानूनी तरीके से इंटरनेट पर चुराना। कई तरह की फाइल जैसे– फिल्में, संगीत फाइलें, ई–बुक्स, सॉफ्टवेयर तथा अन्य सामग्री की चोरी इंटरनेट पाइरेसी के अंतर्गत आती है, इंटरनेट पाइरेसी में शामिल लोग अपने विज्ञापन तथा सेल जैसे कार्य भी नेट के जरिए ही करते हैं। पाइरेसी आज वैश्विक समस्या के रूप में उभर रही है। सॉफ्टवेयर के मामले में पाइरेसी आम है, लोग अक्सर बिना जानकारी के चुराए गए सॉफ्टवेयर खरीद लेते हैं। इंटरनेट पायरेट अपने चोरी के सामान को बेचने के लिए नकली वेबपेज भी बना लेते हैं जिस पर वह अपना विज्ञापन करते हैं, दरअसल इंटरनेट पर प्रत्येक व्यक्ति को बिना अपनी जानकारी दिए सौदे करने का हक होता है। अन्य भौतिक उत्पादों से इतर वहाँ खाते की डिजिटल फाइल बनाने की जरूरत भी नहीं होती जिसके चलते पाइरेसी काफी अधिक होती है। शक के दायरे में आने पर ऐसे कथित विक्रेता गायब भी हो जाते हैं और खरीददार हाथ मलते रह जाते हैं। इसलिए पाइरेटेड सॉफ्टवेयर को न खरीदें और वहीं से खरीदारी करें जो वेबसाइट रजिस्टर्ड हो तथा जिसके बारे में अधिकांश लोग जानते हों, बिना आज्ञा किसी की कॉपीराइट फाइल या सॉफ्टवेयर के गुपचुप इस्तेमाल को लेकर पूरी दुनिया में बहस चल रही है और कुछ देशों ने इस संबंध में कानून भी बना लिये हैं, मगर प्रत्येक देश के कानून इस मामले में अलग–अलग हैं। कनाडा में म्यूजिक

फाइलों को अपने निजी इस्तेमाल के लिए डाउनलोड करने की आज्ञा है, जबकि अमरीका में यह गैरकानूनी है। फिल्में डाउनलोड करना अधिकांश जगह गैरकानूनी है।

(4) ट्रोजन अटैक/वेब जैकिंग– ट्रोजन एक ऐसा प्रोग्राम है जो किसी बड़े प्रोग्राम के बीच में ऐसे डाल दिया जाता है कि किसी को खबर भी नहीं लगती और अन्य प्रोग्राम के साथ यह भी आसानी से क्रियान्वित होता रहता है। किसी के कम्प्यूटर नेटवर्क को हैक करके और ट्रोजन के जरिए ई–मेल का आदान–प्रदान करके आतंकी आतंकवादी घटनाओं से पूर्व इसका खूब इस्तेमाल कर रहे हैं। इसी तरह वेब जैकिंग के अंतर्गत यदि एक बार किसी वेबसाइट को जैक किया जाता है तो वेबसाइट का मालिक उस पर अपना नियंत्रण खो देता है। इसके बाद जैकर वेबसाइट को अवांछित कार्यों के लिए प्रयुक्त कर सकता है। साइट की सूचनाओं को खत्म कर सकता है या उन्हें बदल सकता है।

(5) लॉजिक बम या ई मेल बांबिंग/डिनायल ऑफ अटैक– लॉजिक बम ऐसा क्रोड प्रोग्राम है जो किसी विशेष दिन या सुनिश्चित समय पर सक्रिय होकर न सिर्फ कम्प्यूटर के मुख्य प्रोग्राम में बाधा डालता है बल्कि उसे गुमराह भी कर देता है। इसी प्रकार अत्यधिक संख्या में ई–मेल भेजकर किसी के सर्वर या ई–मेल अकाउंट को नष्ट करना– 'ई–मेल बॉबिंग' कहलाता है। इसी तरह इंटरनेट यूजर्स की लगातार बढ़ती संख्या से 'वेब सर्वर' पर अत्यधिक दबाव पड़ जाता है जिससे कभी–कभी उसकी क्षमता कम हो जाती है। इस प्रकार सर्वर की ओवरलोडिंग के कारण सरकारी व निजी संस्थानों के दैनिक कामकाजों पर बुरा असर पड़ता है। मसलन बिजली तथा पानी की आपूर्ति जैसी सुविधायें भी इससे कुछ समय के लिए ठप्प पड़ जाती हैं। इसे 'डिनायल ऑफ सर्विसेज अटैक' का नाम दिया गया है।

(6) डाटा डिडलिंग तथा इंटरनेट टाइम चोरी– कम्प्यूटर पर प्रोसेस होने से पूर्व डाटा में परिवर्तन कर देना तथा प्रोसेस के बाद फिर उसे वास्तविक रूप में बदल देना 'डाटा डिडलिंग' कहलाता है। इसी तरह इंटरनेट पासवर्ड प्राप्त कर किसी अन्य द्वारा खरीदे गए टाइम का इस्तेमाल करना 'इंटरनेट टाइम थेप्ट' कहलाता है।