वैश्वीकरण और बढता साइबर क्राइम

डॉ. अशोक कुमार – सहायक आचार्य, सैन्य विज्ञान विभाग, जयनारायण व्यास वि.वि., जोधपुर।

सूर्यप्रकाश व्यास – अतिथि सहायक आचार्य, सैन्य विज्ञान विभाग, जयनारायण व्यास वि.वि., जोधपुर।

सरांश :
वैज्ञानिक और तकनीकी प्रगति के कारण संसार बहुत छोटा होता जा रहा है। आज संसार के सभी देश आपस में बहुत निकट आ गए हैं तथा एक देश की घटनाओं का प्रभाव दूसरे देश पर पड़ता है। यातायात के साधनों का विकास और सूचना प्रौद्योगिकी के विकास के कारण संसार के दूरस्थ देशों में यात्राएँ करना तथा वहां से वस्तुओं का आयात और निर्यात करना बहुत आसान हो गया है। टेलीविजन, इन्टरनेट कम्प्यूटर और टेलिफोन से दुनिया के दूर देशें की घटनाओं की जानकारी प्राप्त करना तथा संवाद स्थापित करना बहुत ही आसान और सस्ता हो गया है। संसार के एक भाग में कुछ भी अच्छा बुरा होता है उसका प्रभाव पूरे विश्व पर भी पड़ता है। सूचना प्रौद्योगिकी के कारण फैशन, रहन–सहन, खान पान सभी का वैश्वीकरण हो गया है। इससे स्थानीय विविधताओं के समाप्त होने का खतरा (आशंका) उत्पन्न हो गयी है। चिकित्सा के तरीकों और सभी औषधियों का भी वैश्वीकरण हुआ है। सामुहिक विनाश के रासायनिक और जैविक हथियार सभी विश्वव्यापी हो गए हैं। सभी सौन्दर्य व खेल प्रतियोगिताओं पर वैश्वीकरण का प्रभाव दिखाई देता है। विश्व के आर्थिक जीवन, सूचना और प्रौद्योगिकी के क्षेत्र में इस वैश्वीकरण के बहुत घातक परिणाम हुए हैं।[1]

प्रस्तावना :

कम्प्यूटर, वर्ल्ड वाइड वेब (www) तथा उपग्रह प्रणाली विज्ञान के वे आधुनिक आविष्कार हैं जिन्होंने सूचना तथा संचार प्रौद्योगिकी की गतिसीमा तथा उपयोगिता को आश्चर्यजनक रूप से बढ़ा दिया है। इनके चलते सूचना प्रौद्योगिकी का एक नवीन एवं क्रान्तिकारी प्रारूप दुनिया के सामने आया।

विशेषज्ञों की मानें तो अभी सूचना प्रौद्योगिकी अपने शैशवकाल में है और इसमें अभी विकास की इतनी अधिक सम्भावनाएं छुपी हैं। समय के साथ–साथ यह आशंका भी बलवती होती जा रही है कि कहीं साइबर क्राइम सूचना प्रौद्योगिकी की सम्भावनाओं पर ग्रहण ना लगा दे। आज वास्तविक दुनिया के समान्तर साइबर वर्ल्ड की दुनिया अपना आकार ले रही है और मोबाइल तक इन्टरनेट की पहुँच हो गई है। लेकिन कठिनाई यह है कि 'साइबर स्पेस' जहाँ आँकड़ों व सूचनाओं का आदान–प्रदान होता है। इसके लिए विश्वभर में कोई प्रभावी नियम व्यवस्था नहीं बनाई जा सकी है। तीसरी दुनिया के विकासशील देशों में जहाँ सूचना व संचार प्रौद्योगिकी अपने पाँव पसार रही रही है वहाँ साइबर क्राइम के कारण परिस्थितियाँ और भी चिन्ताजनक बनी हुई है।

साइबर क्राइम की व्याख्या :

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

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

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

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 पहुंचाने की कोशिश करना, चाहे वह किसी भी माध्यम से की गई हो (वैरीकोलिन इंस्टीट्यूट ऑफ सिक्योरिटी एण्ड इंटेलीजेंस, कैलिफोर्निया USA)।

4. कम्प्यूटर नेटवर्क को हैक करके उसमें संग्रहीत आंकड़ों को चुराना और फिर अपने सामाजिक–राजनैतिक तथा व्यावसायिक प्रतिद्वन्द्वियों के खिलाफ उनका उपयोग करना।

5. सूचनातंत्र पर किसी भी प्रकार से चोट पंहुचाने का प्रयत्न 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 माध्यम से सामाजिक आर्थिक राजनैतिक सांस्कृतिक अथवा भावात्मक रूप से किसी को हानि पहुँचाना या संकट में डालना (संयुक्त राष्ट्रसंघ)

भारत में आई.टी. कानून 2000 लागू होने के पश्चात् साइबर 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 उपयोग किया गया हो या उसे लक्ष्य बनाया गया हो या वह लक्ष्य तथा औजार दोनों हो, साइबर क्राइम कहलाता है। साइबर टेररिज्म, साइबर फ्रॉड, साइबर ब्लैकमेलिंग, साइबर हैकिंग, साइबर वेब जेकिंग, पीसी हैकिंग इत्यादि साइबर क्राइम के ही रूप हैं। जब आतंकवादी गतिविधियों के लिए साइबर स्पेस का उपयोग किया जाता है तो यह 'साइबर टेररिज्म' कहलाता है। जब वित्तीय लेन–देन क्रेडिट कार्ड फ्रॉड, पासवर्ड बैंक अकाउंट एवं क्रेडिट कार्ड नम्बर चोरी करने के लिए साइबर स्पेस का उपयोग किया जाता है तो यह 'साइबर फ्रॉड' कहलाता है। इसलिए साइबर टेररिज्म, साइबर फ्रॉड, साइबर हैकिंग आदि साइबर क्राइम के ही विभिन्न रूप हैं। जिनके लक्ष्य व उद्देश्य अलग–अलग हैं। किसी एक देश द्वारा अपने प्रतिद्वन्द्वी दूसरे देश की सूचना प्रणाली में सेंध लगाने को 'साइबर–वार' कहा जाता है।

साइबर क्राइम के सभी रूप में व्यक्ति, समाज, देश तथा दुनिया की वैयक्तिकता, गोपनीयता, एकता तथा अखण्डता के लिए हानिकारक है। लेकिन 'साइबर टेररिज्म' तथा 'साइबर–वार' ऐसे दो प्रारूप हैं जो सर्वाधिक गंभीर चोट पहुंचा रहे हैं। भारत में विगत कुछ वर्षों में हुए आतंकवादी हमलों में सूचना एवं संचार माध्यमों का बहुत ही व्यापक और चतुराई से उपयोग किया गया है। इसक अतिरिक्त चीन तथा पाकिस्तान द्वारा भारतीय विदेश तथा रक्षा मंत्रालय के साथ–साथ प्रधानमंत्री कार्यालय के कुछ दस्तावेजों में भी सेंध लगाने से समस्या और गंभीर बन गई है। मलाल तो इस बात का है कि इस क्षेत्र में भारत द्वारा किए गए सुरक्षात्मक उपाय कारगर सिद्ध नहीं हो रहे हैं। निरन्तर बढ़ती वैश्विक प्रतिस्पर्धा तथा आतंकवाद के कारण भावी युद्धों में 'साइबर स्पेस' निर्णायक भूमिका में होगा और आने वाले समय में आतंकवादी किसी भी देश की सुरक्षा प्रणाली, हवाई सेवाओं, रेलसेवाओं तथा अन्य संचार व परिवहन सेवाओं और कम्पनियों व सरकार के कामकाजों को भी ठप्प कर सकते हैं। साइबर वार के द्वारा किसी भी देश की सूचना व संचार आधारित उपग्रह प्रणाली और प्रकार की रक्षा–प्रतिरक्षा प्रणाली को भी ठप्प किया जा सकता है। यहाँ तक कि जमीन पर बैठे–बैठे किसी भी देश के हवाई जहाज, उपग्रह, लड़ाकू विमानों तथा प्रक्षेपास्त्रों को गिराया जा सकता है, उनका अपहरण किया जा सकता है अथवा उनकी दिशा बदली जा सकती है। भावी घटनाओं से बचने के लिए अभी से सुरक्षात्मक उपाय करने होंगे।

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

1. प्रथम भाग में कम्प्यूटर को एक 'लक्ष्य' के रूप में अन्य 'कम्प्यूटरों' पर आक्रमण करने के लिए प्रयुक्त करना है। जैसे–हैकिंग, वायरस, वर्मस तथा DOS आक्रमण।

2. द्वितीय भाग में आपराधिक कार्यों के लिए कम्प्यूटर का उपयोग एक शस्त्र के रूप में किया जाना। जैसे–साइबर टेररिज्म, बौद्धिक संपदा अधिकारों का उल्लंघन, क्रेडिट कार्ड धोखाधड़ी, ब्लैकमेलिंग, अश्लील सामग्री का वितरण इत्यादि, इसमें साइबर स्पेस का उपयोग करना।

सैद्धान्तिक रूप से विशेषज्ञों ने साइबर क्राइम को तीन श्रेणियों में बाँटा है।

1. सरकार के विरुद्ध अपराध जेसे–साइबर टेररिज्म
2. किसी व्यक्ति विशेष के विरुद्ध अपराध।
3. सम्पत्ति से जुड़े अपराध।

कुछ प्रमुख साइबर अपराध :

1. हैकिंग – 'हैकिंग' शब्द का सर्वप्रथम प्रयोग ''मैसाच्युसेट्स इंस्टीट्यूट ऑफ टेक्नोलॉजी (MIT)'' में किया गया था। उस समय इसका अर्थ था – ''कोई भी काम चालाकी से या विचारोत्तेजक नई शैली में करना'', परन्तु आज हैकिंग शब्द का उपयोग सूचना व संचार प्रौद्योगिकी को हानि पहुंचाने के लिए किया जाता है।

2. कम्प्यूटर वाइरस/वर्मस – यह एक विशेष प्रकार का प्रोग्राम होता है जिसे इस प्रकार विकसित किया जाता है ताकि वह कम्प्यूटर के डाटा को हानि पहुंचा सके। वायरस की खतरनाक विशेषता यह है कि यह अपने सम्पर्क में आने वाले अन्य कम्प्यूटर्स की हार्ड–डिस्क 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 रूप में हो सकता है। यह ई–मेल, पेन–ड्राइव व सी.डी. से डाटा ट्रांसफर करते समय कम्प्यूटर में समा जाते हैं। इसी तरह वर्मस 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 में वे भी इस काम को अंजाम दे चुके होते हैं या इसका शिकार हो चुके होते हैं। यह भी साइबर क्राइम है। इंटरनेट पाइरेसी यानि किसी कॉपीराइट डिजीटल फाइल को गैरकानूनी तरीके से इंटरनेट पर चुराना। कई प्रकार की फाइल जैसे फिल्में, संगीत फाइलें, ई–बुक्स, सॉफ्टवेयर तथा अन्य सामग्री की चोरी आदि।

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 होती और अन्य प्रोग्राम्स के साथ यह भी आसानी से क्रियान्वित होता रहता है। किसी के नेटवर्क कम्प्यूटर को हैक करके और ट्रोजन के जरिए ई–मेल का आदान प्रदान करके आतंकी आतंकवादी घटनाओं से पूर्व इसका बहुत उपयोग कर रहे हैं। इसी तरह वेब जैकिंग के अन्तर्गत यदि एक बाइर 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 कों खत्म कर सकता है या उन्हें बदल सकता है।

5. लॉजिक बम या ई–मेल बॉबिंग/डिनायल ऑफ सर्विसेज अटैक – लॉजिक बम ऐसा क्रोड प्रोग्राम है जो किसी विशेष दिन या सुनिश्चित समय पर सक्रिय होकर न केवल 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 अकांउट को नष्ट करना 'ई–मेल बॉबिंग' कहलाता है। इसी प्रकार इंटरनेट यूजर्स की लगातार बढ़ती संख्या से 'वेब सर्वर' पर अत्यधिक दबाव पड़ता 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 प्रभाव पड़ता है। जैसे बिजली तथा पानी की आपूर्ति जैसी सुविधाएँ भी इससे कुछ समय के लिए ठप्प पड़ जाती है। 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 प्रकार इंटरनेट पासवर्ड प्राप्त कर किसी अन्य द्वारा खरीदे गए टाइम का उपयोग करना 'इंटरनेट टाइम थेप्ट' कहलाता है।

साइबर सिक्योरिटी में 'फायरवॉल' की भूमिका :

कम्प्यूटर नेटवर्किंग की आवश्यकता मुख्यतः विभिनन कार्यों जैसे ऑनलाइन बैंकिंग, ई–टिकटिंग, ई–कॉमर्स, ई–गवर्नेंस आदि में होती है। जिनकी सुरक्षा में 'फायरवॉल' महत्त्वपूर्ण भूमिका निभाता है। अधिकांश सरकारी तथा निजी संस्थाओं का अपना पर्सनल कम्प्यूटर नेटवर्क होता है। जिसे 'इंट्रानेट' कहा जाता है। इसमें से किसी महत्त्वपूर्ण तथा गोपनीय सूचना या डाटा का लीक हो जाना उस संस्थन के लिए अत्यधिक हानिकारक हो सकता है। ऐसे में कम्प्यूटर नेटवर्क की सुरक्षा बहुत ही महत्त्वपूर्ण हो जाती है। ताकि बाहरी यूजर्स किसी भी प्रकार से आन्तरिक नेटवर्क की सूचनाओं को एक्सेस न कर पाएं और फायरवॉल नेटवर्क को सुरक्षा प्रदान करने में सहायक सिद्ध होता है। फायरवॉल को 'हार्डवेयर' तथा 'सॉफ्टवेयर' दोनों ही रूपों में उपयोग किया जा सकता है। यह एक ऐसी तकनीक है जो हमारे निजी नेटवर्क तथा इंटरनेट के मध्य सुरक्षा प्रहरी की भूमिका निभाता है और निजी नेटवर्क को अनचाहे यूजर्स के प्रयत्नों से बचाता है।[1]

अपराधों की रोकथाम और इलेक्ट्रॉनिक सर्विलांस :

चीन द्वारा निर्मित कुछ मोबाइल हैंडसेटों में आई.एम.ई.आई नम्बर नहीं होता है जिसकारण ऐसे सेटों को सर्विलांस पर ट्रेस नहीं किया जा सकता। इसलिए सुरक्षा कारणों से दूरसंचार विभाग ने ऐसे सभी मोबाइल हैंडसेटों पर मोबाइल सेवा बंद करने का आदेश (6 जनवरी 2009) जारी किया है।[2]

साइबर अपराधों पर अंकुश हेतु विधेयक संसद के दोनों सदनों में पारित :

साइबद अपराधों पर अंकुश के लिए सूचना प्रौद्योगिकी (संशोधन) विधेयक संसद के दोनों सदनों में गत दिसम्बर माह में पारित किया गया है। लोकसभा में पहले पारित इस विधेयक को राज्यसभा में 23 दिसम्बर को पारित किया गया है। आपराधिक उद्देश्यों के लिए कम्प्यूटरों एवं संचार उपकरणों के दुरुपयोग के लिए कड़े दण्ड का प्रावधान इसमें किया गया है। इलेक्ट्रॉनिक रूप में अश्लील सामग्री के प्रकाशन एवं सम्प्रेषण के मामलों में जहाँ 5 वर्ष तक के कारावास का प्रावधान है वहीं साइबर टेररिज्म के मामलों में आजीवन कारावास तक की सजा इसके तहत दी जा सकेगी। महत्त्वपूर्ण 'डाटा' की चोरी व ई–कॉमर्स धोखाधड़ी आदि के मामलों के लिए भी सजाओं के प्रावधान इस विधेयक में है। ऐसे मामलों की सुनवाई के लिए एक साइबर एप्पीलेट ट्रिब्युनल के गठन का प्रस्ताव इस विधेयक में किया गया है।[3]

सन्दर्भ :

1. माध्यमिक शिक्षा बोर्ड, कक्षा – 11, इतिहास

2. प्रतियोगिता दर्पण, मार्च 2012

3.अपराधा और प्रौद्योगिकी – डॉ. निशांत सिंह

4. प्रतियोगिता दर्पण फरवरी, 2009