साइबर अपराध र वर्तमान चुनौतिहरू

महेश सिंह कठायत*

कम्प्यूटर, सञ्चार तथा इन्टरनेट प्रविधिलाई प्रयोग गरी गरिने अपराधलाई कम्प्यूटर अपराध अर्थात् साइबर अपराध (Cyber Crime) भनिन्छ। साइबर अपराध व्यक्ति विशेष, सम्पत्ति विशेष र सरकार विशेष गरी मुख्यतः तीन प्रकारका हुन्छन्।

१. व्यक्ति विशेष साइबर अपराध

ई-मेलको माध्यमबाट व्यक्तिहरूलाई मानसिक तनाव सिर्जना गर्नु वा बाल यौन सम्बन्धी सामग्रीको अनाधिकृत रूपमा वितरण गर्नुलाई व्यक्ति विशेष साइबर अपराध भन्ने बुझिन्छ। यसका साथै पीडित व्यक्तिलाई ई-मेलको माध्यमबाट धम्क्याएर प्रताडित गर्ने जस्ता कार्यहरू (Cyber Stalking) समेत यस अपराधभित्र पर्दछन्।

२. सम्पत्ति विशेष साईबर अपराध

बिना अनुमति अनाधिकृत रूपमा कम्प्यूटरहरूमा साइबर अङ्ग मार्फत् छिर्नु, (Computer Vandalism) अर्थात् कम्प्यूटरमा रहेका सूचनाहरूको स्वामित्व प्राप्त गर्नु वा गर्न खोज्नु जस्ता अपराधहरू सम्पत्ति विशेष साईबर अपराध अन्तर्गत पर्दछन्। यसका साथै Hacking/Cracking जस्ता साइबर अपराधहरू गर्ने गराउने कार्य समेत यस अपराध अन्तर्गत पर्दछन्। यस्तै खतरापूर्ण प्रोग्रामहरू तथा कम्प्यूटर भाइरसहरूलाई वितरण गर्नु पनि सम्पत्ति विशेष साइबर अपराधहरू हुन्।

३. सरकार विशेष साइबर अपराध

सञ्चार तथा सूचना प्रविधिद्वारा गरिने आतङ्ककारी क्रियाकलापहरू (Cyber Terrorism) सरकार विशेष साइबर अपराध अन्तर्गत पर्दछन्। जसमा कुनै पनि व्यक्ति वा समूहले कम्प्यूटर र इन्टरनेट मार्फत् कुनै पनि देशको सरकार तथा जनताहरूलाई धम्क्याउन सक्दछन्। उदाहरणको लागि, कुनै व्यक्ति विशेषले कुनै पनि देशको सरकारी तथा सैनिक वेबसाईटहरूमा प्रवेश गरी वेबसाईट निस्क्रिय पार्ने, सामग्रीहरू मेटाउने तथा सूचनाहरूमा थपघट पनि गर्न सक्दछन्।

इन्टरनेट र साईबर अपराध

मानव समाजले विश्वमा आजसम्म आविष्कार गरेका सबै प्रकारका प्रविधिहरूमध्ये ज्यादै ठूलो उपलब्धीको रूपमा इन्टरनेटलाई लिइएको छ। वर्तमान युगमा सूचना प्रविधि, बैकिङ्ग प्रणाली अन्तर्गत ई-बैकिङ्ग तथा आम जनतासँग प्रत्यक्ष सरोकार विभिन्न कार्यहरू / सेवाहरू तथा आपत्कालिन सेवाहरू सबै इन्टरनेट मार्फत् कम्प्यूटर सञ्जाल (Computer Network) द्वारा सञ्चालन गरिन्छ। तर समाजमा यस्ता व्यक्तिहरू पनि छन् जसले यस प्रविधिको उपयोग गरी अरुलाई हानी-नोक्सानी पुऱ्याउने कार्यमा लगाउँछन्। यस्ता कार्यहरू गर्नेहरूको उद्देश्य बुझ्न ज्यादै कठिन हुन्छ। उद्देश्य बुझ्न नसकिए पनि यसको परिणामबाट जनमानसलाई यस प्रविधिप्रति आत्मविश्वास बढाउने कार्यमा भने आघात पुग्दछ। यस्तो नियति इन्टरनेटले आफ्नो जन्म भएको धेरै छोटो अवधिमा नै भोग्नु परिरहेको छ।

इन्टरनेटबाट हुन सक्ने दुर्व्यवहारहरू

- लगातार नचाहिँदा पत्रहरू कुनै व्यक्ति विशेषलाई पठाइरहने प्रक्रियालाई मेल बमिङ् भनिन्छ। जसले गर्दा ई-मेल प्राप्त गर्ने व्यक्तिको मेल बक्समा अनावश्यक पत्रहरू सदैव भरिएर रहन्छन्। जसले गर्दा आवश्यक पत्रहरू समयमा प्राप्त नहुन पनि सक्दछन्।
- स्पामिङ् एकैपटक सबै पत्र पठाउने प्रविधि हो। यसको वास्तविक प्रयोग व्यापार प्रबर्द्धन आदि कार्यका लागि गरिन्छ। तर कहिलेकाहीं यसको पनि दुरूपयोग हुन गई केही व्यक्तिहरूको मेल बक्समा अनावश्यक पत्रहरूको बाढी आएर दुःख दिने गर्दछ।
- लिस्ट लिङ्किङ् मार्फत् अर्काको मेल ठेगाना आदान-प्रदान गर्न सकिन्छ। तर यसैको दुरूपयोग गरी कहिलेकाहीँ मेल ठेगानामा लाखौंको सङ्ख्यामा रहेका 'मेल ठेगानाहरू'को लिस्ट नै पठाएर अनावश्यक हैरानी दिने गरिएको पाइन्छ।
- स्पुफिङ् (Spoofing) अर्थात् झुट्टा व्यक्तिले अन्य वास्तविक व्यक्तिको ई-मेल ठेगानामा मेल पठाएर झुक्याउने अथवा भाइरस आदि

* *महेश सिंह कठायत नेपाल प्रहरीमा कम्प्यूटर महाशाखा प्रमुख हुनुहुन्छ।*

पठाएर दुःख दिने गर्दछन् ।

- लिङ्किङ्/फ्रेमिङ् (Linking/Framing) मार्फत् कुनै आधिकारिक वेबसाईटलाई अर्काको ठेगानामा लगेर जोडी दिने गर्दछन् ।
- वास्तविक ग्राहकलाई उसको आधिकारिक सेवाबाट वञ्चित गरिदिने गर्दछन् ।
- क्रेकिङ् (Cracking) भन्नाले अनाधिकृत रूपमा कुनै पनि कम्प्यूटर प्रणालीमा पहुँच प्राप्त गर्ने र अन्तोगत्वा सो प्रणाली बिगारी दिने कार्यलाई बुझिन्छ । प्रयोगकर्ताले कहिलेकाहीँ यो दुर्व्यवहार समेत झेल्नुपर्ने हुन्छ ।

साइबर अपराधका चुनौतिहरू

वास्तवमा साइबर स्पेसमा हुने अपराधहरूले कुनै पनि राष्ट्रको कानुनलाई मान्दैनन् । यसले गर्दा साइबर अपराधको रोकथाम तथा अपराधीलाई सजाय नहुने हो भने ई-कमर्शले समयानुकूल विकास गर्न सक्दैन । त्यसबाहेक, हाल आएर बालयौन अपराध, झुट्टा अपराध, जालसाजी, आई.पी.आर. चोरी, सूचना तथा पैसाको चोरी तथा गम्भीर प्रकृतिका धम्की आदि अपराधहरू अब इन्टरनेटमा सरिरहेका छन् ।

हाल साइबर अपराधले मानव सम्भयताका अगाडि प्राविधिक, कानुनी र साधन-स्रोत सम्बन्धी गरी मुख्य तीन प्रकारका चुनौतिहरू ल्याएको छ । जसलाई निम्नानुसार वर्णन गर्न सकिन्छ :-

(क) प्राविधिक चुनौतिहरू - साइबर अपराध कसले, कसरी, कहाँबाट किन गऱ्यो आदि कुराहरू पत्ता लगाउन त्यति सजिलो छैन । किनकि, यस अपराधको प्रकृति एवम् प्रयोग हुने प्रविधि ज्यादै जटिल एवम् सम्वेदनशील हुने गर्दछ । कहिलेकाहीँ त अपराधीसम्म पुग्न ठूलो धनराशीको खर्च गर्नुपर्ने मात्र होइन, प्राविधिक हिसाबले असम्भव नै हुने गर्दछ ।

(ख) कानुनी चुनौतिहरू - यस प्रविधिमा हुने द्रुततर गतिको विकास एवम् परिवर्तनले गर्दा विद्यमान कानुन तथा कानुनी पद्धति एवम् औजारहरूले समेत सबै अपराधलाई समेट्न गाह्रो महसुस हुन थालेको छ ।

(ग) साधनस्रोत सम्बन्धी चुनौतिहरू - वास्तवमा साइबर अपराधसँग जुध्नको लागि आवश्यक पर्ने प्राविधिक दक्षता, तालिम तथा बजेटको सदैव अभाव हुने गर्दछ । जसबाट वर्तमान २१ औं शताब्दीमा यसप्रकार द्रुततर गतिमा भइरहेको सूचना प्रविधिको परिवर्तनका लागि आवश्यक पर्ने साधनस्रोत बाधा बन्दछ ।

साइबर अपराध र विकासशील मुलुकहरू

हाल धेरै विकासशील एवम् विकासोन्मुख मुलुकहरूमा यस अपराधको सामना गर्नका लागि कानुन तर्जुमा गरिसकिएको छ । फिलिपिन्समा ई-कमर्स एक्टको व्यवस्था गरी साइबर अपराधीहरूको लागि पनि कानुनी व्यवस्था गरिएको छ । मलेसियाले सन् १९९७ मा नै कम्प्यूटर अपराध सम्बन्धी कानुन तर्जुमा गरी लागू गरिसकेको छ । त्यसैगरी, सिङ्गापुरमा सिङ्गापुर साइबर मिसयुज एक्टद्वारा यस अपराधको रोकथाम एवम् अनुसन्धान गरिरहेको छ । त्यसैगरी हाम्रो छिमेकी मुलुक भारतमा पनि इन्टरनेशनल टेक्नोलोजी एक्ट-२००० लागू भइसकेको छ तथा नेपालमा पनि इलेक्ट्रोनिक ट्रान्जेक्सन एक्ट-२००४ द्वारा साइबर अपराधको नियन्त्रण एवम् अनुसन्धानको व्यवस्था गरिएको छ ।

साइबर अपराध नियन्त्रणका विद्यमान उपायहरू

हालसम्म पनि साइबर अपराधको आक्रमणबाट बच्ने मुख्य उपाय नै त्यसको आक्रमण हुन नदिनु नै हो । अर्थात्, यस सम्बन्धी सचेतता नै हो । हाल साइबर आक्रमणबाट कम्प्यूटर प्रणालीलाई सुरक्षित राख्ने धेरै साधनहरू उपलब्ध छन् । उदाहरणको लागि, फयरवाल्स्, इनक्रिप्सन प्रविधिहरू तथा पब्लिक की प्रणाली आदिहरूको प्रयोग गर्न सकिन्छ ।

साइबर कानुन सहित साइबर अपराध अनुसन्धानकर्ताहरूलाई आवश्यक मात्रामा साधनस्रोत तथा बजेटको व्यवस्था गरिनु पर्दछ । जसको माध्यमबाट उनीहरूले साइबर आक्रमणकारीहरूबाट कम्प्युटर नेटवर्क (सञ्जाल) लाई सुरक्षित राख्नको लागि आवश्यक संयन्त्र (Hardware, Software तथा अन्य साधनस्रोतहरू) र तालिमको व्यवस्था गर्न सक्दछन् । साइबर अपराधलाई नियन्त्रण गर्न कानुन तबसम्म सुषुप्त हुन्छ, जबसम्म यस क्षेत्रमा कार्य गर्ने प्रहरी, अधिवक्ता, न्यायाधीश तथा अन्य व्यक्तिहरूमा यसको ज्ञान, शिक्षा तथा आवश्यक तालिमको व्यवस्था गरिँदैन । यसबाहेक सरकार र निजी क्षेत्रहरूबीच समन्वय र आपस सहयोगको आदान प्रदान हुनु ज्यादै जरुरी छ । यसको माध्यमबाट साइबर अपराधसँग जुध्न तथा अनुसन्धान समेत गर्न ठूलो सहयोग हुन जान्छ । यसैगरी, साइबर अपराध सम्बन्धी विद्यमान कानुनलाई राष्ट्रिय, क्षेत्रीय तथा अन्तर्राष्ट्रिय स्तरमा समेत सामञ्जस्यता कायम गरिएमा यो सीमारहित अपराधलाई नियन्त्रण गर्न समेत ठूलो टेवा पुग्न सक्दछ ।

उपसंहार

साइबर सुरक्षा तथा सूचनाको गोपनियता सरकारको मात्र जिम्मेवारी होइन, निजी क्षेत्रहरूले सरल तथा स्वःअनुशासित प्रणालीको विकास गर्न जरुरी हुन्छ । त्यसै गरेर सरकारले सूचना प्रविधि उद्योग तथा अन्य साइबर अपराध सम्बन्धी गैरसरकारी संस्थाहरूसँग सहकार्य गरी साइबर अपराध सम्बन्धी नियन्त्रणमा लाग्न जरुरी छ ।

वास्तवमा, सबैभन्दा ठूलो कार्य भनेको सरकारका विभिन्न तहमा कार्य गर्ने व्यक्तिहरू, निजी क्षेत्र, सामाजिक संघ-संस्थाहरू, गैरसरकारी संस्थाहरूका व्यक्तिहरूको संलग्नतामा साइबर अपराध, व्यक्तिगत डाटा गोपनीयता, साइबर सुरक्षा, साइबर अपराध रोकथाम र नियन्त्रणको विषयमा प्रचार प्रसार एवम् जानकारी गराउन ज्यादै जरुरी हुन्छ । साथै साइबर क्षेत्रहरूमा हुने अपराध तथा तिनीहरूको रोकथाम, नियन्त्रण सम्बन्धी विषयहरूमा समेत सचेत गराउनु पर्दछ । र, अन्तमा सबैभन्दा महत्वपूर्ण एवम् जरुरी कुरा भनेको सामाजिक सर्वसहमतिद्वारा सही तरिका अर्थात् नैतिकतामा आधारित सूचना सञ्चार प्रविधि (Ethical and Trustworthy Computing) को प्रयोग हो ।

■