आखर हिंदी पत्रिका ; e-ISSN-2583-0597 खंड 3/अंक 3/जून 2023
Received: 09/06/2023; Accepted: 14/06/2023; Published: 24/06/2023

साइबर अपराध: मुद्दे और चुनौतियाँ

अखिल एम जैन
द्वितीय सेमेस्टर, बी.सी.ए. 'ए'
सुराना कॉलेज, बेंगलुरु, कर्नाटक

अखिल एम जैन, **साइबर अपराध: मुद्दे और चुनौतियाँ**, आखर हिंदी पत्रिका, खंड 3/अंक 3/जून 2023, पृष्ट(270-276)

I. सारांश

कंप्यूटर प्रौद्योगिकी की सुविधाएं बिना कमियों के सामने नहीं आई हैं। हालांकि यह जीवन को तेज बनाता है लेकिन 'साइबर क्राइम' कहे जाने वाले सबसे घातक प्रकार के अपराध से खतरे के ग्रहण में आ गया है। कंप्यूटर के बिना, पूरे व्यवसाय और सरकारी संचालन कार्य करना लगभग बंद कर देंगे। सस्ते, शक्तिशाली, उपयोगकर्ता के अनुकूल कंप्यूटरों के इस प्रसार ने अधिक से अधिक लोगों को उनका उपयोग करने में सक्षम बनाया है और इससे भी महत्वपूर्ण बात यह है कि वे अपने सामान्य जीवन के हिस्से के रूप में उन पर भरोसा करते हैं। जैसे-जैसे व्यवसाय, सरकारी एजेंसियां और व्यक्ति उन पर अधिक से अधिक भरोसा करना जारी रखते हैं, वैसे-वैसे अपराधी भी करते जाते हैं। साइबर अपराधों पर प्रतिबंध उनके व्यवहार के उचित विश्लेषण और समाज के विभिन्न स्तरों पर उनके प्रभावों की समझ पर निर्भर है। इसलिए, इस शोध पत्र में, साइबर अपराधों की भविष्य की प्रवृत्तियों के साथ सामाजिक-पारिस्थितिक-राजनीतिक, उपभोक्ता विश्वास आदि जैसे विभिन्न क्षेत्रों पर साइबर अपराधों और उनके प्रभावों की एक व्यवस्थित समझ को समझाया गया है।

II. परिचय

साइबर क्राइम एक ऐसा शब्द है जिसका उपयोग व्यापक रूप से आपराधिक गतिविधि का वर्णन करने के लिए किया जाता है जिसमें कंप्यूटर या कंप्यूटर नेटवर्क एक उपकरण, एक लक्ष्य या आपराधिक गतिविधि का स्थान है और इसमें इलेक्ट्रॉनिक क्रैकिंग से लेकर डेनियल-ऑफ-सर्विस (डीओएस) हमलों तक सब कुछ शामिल है।

इसका उपयोग पारंपरिक अपराधों को शामिल करने के लिए भी किया जाता है जिसमें अवैध गतिविधि को सक्षम करने के लिए कंप्यूटर या नेटवर्क का उपयोग किया जाता है। साइबर क्राइम किसी भी रेलवे को जहां है वहीं रोक सकता है, यह विमानों को उनकी उड़ान पर गलत संकेतों के साथ गुमराह कर सकता है, इससे कोई भी महत्वपूर्ण सैन्य डेटा विदेशों के हाथों में जा सकता है, यह ई-मीडिया को रोक सकता है और हर सिस्टम एक पल में ध्वस्त हो सकता है।

साइबर क्राइम के रूप में इंटरनेट स्पेस या साइबरस्पेस बहुत तेजी से बढ़ रहा है। कुछ प्रकार के साइबर-अपराधियों का उल्लेख नीचे किया गया है।

- **कंप्यूटर-क्रैकर्स:** ये व्यक्ति कुछ असामाजिक उद्देश्यों को पूरा करने के लिए या केवल मनोरंजन के लिए नुकसान पहुंचाने पर आमादा हैं। कई कंप्यूटर वायरस निर्माता और वितरक इस श्रेणी में आते हैं।
- **हैकर्स**: ये व्यक्ति शिक्षा के लिए, जिज्ञासा से बाहर, या अपने साथियों के साथ प्रतिस्पर्धा करने के लिए दूसरों के कंप्यूटर सिस्टम का पता लगाते हैं। वे अधिक शक्तिशाली कंप्यूटर का उपयोग करने, साथी हैकर्स से सम्मान प्राप्त करने, प्रतिष्ठा बनाने, या औपचारिक शिक्षा के बिना एक विशेषज्ञ के रूप में स्वीकृति प्राप्त करने का प्रयास कर सकते हैं।
- **प्रैंकस्टर्स:** ये व्यक्ति दूसरों पर टोटके करते हैं। वे आम तौर पर किसी विशेष या लंबे समय तक चलने वाले नुकसान का इरादा नहीं रखते हैं।
- **कैरियर अपराधी:** ये व्यक्ति अपराध से अपनी आय का हिस्सा या पूरी आय अर्जित करते हैं, हालांकि वे असंतुलित, नशेड़ी और तर्कहीन और अक्षम लोग हैं।
- **साइबर आतंकवादी:** साइबर आतंकवाद के कई रूप हैं। कभी-कभी यह एक सरकारी वेबसाइट में सेंध लगाने वाला एक स्मार्ट हैकर होता है, अन्य समय में यह समान विचारधारा वाले इंटरनेट उपयोगकर्ताओं का एक समूह होता है जो किसी वेबसाइट को ट्रैफ़िक से भरकर क्रैश कर देता है। इससे कोई फर्क नहीं पड़ता कि यह कितना हानिरहित लग सकता है, फिर भी यह उन लोगों के लिए अवैध है जो ड्रग्स, शराब, प्रतिस्पर्धा, या दूसरों से ध्यान, आपराधिक लापरवाही के लिए।
- **साइबर बुल्स:** साइबरबुलिंग कोई भी उत्पीड़न है जो इंटरनेट के माध्यम से होता है। भद्दे फ़ोरम पोस्ट, चैट रूम में नाम-पुकार, वेबसाइटों पर नकली प्रोफ़ाइल पोस्ट करना, और मतलबी या क्रूर ईमेल संदेश साइबर बुलिंग के सभी तरीके हैं।
- **सलामी हमलावर:** उन हमलों का उपयोग वित्तीय अपराध करने के लिए किया जाता है। यहाँ बात यह है कि परिवर्तन को इतना महत्वहीन बना दिया जाए कि एक ही मामले में, यह पूरी तरह से किसी का

ध्यान नहीं जाएगा। उदाहरण के लिए, एक बैंक कर्मचारी बैंक के सर्वर में एक प्रोग्राम डालता है, जो प्रत्येक ग्राहक के खाते से एक छोटी राशि काट लेता है।

III. साइबर अपराध के प्रकार

1. डेटा अपराध

i. डेटा अवरोधन

एक हमलावर सूचना एकत्र करने के लिए लक्ष्य से डेटा प्रवाह की निगरानी करता है। यह हमला बाद के हमले का समर्थन करने के लिए जानकारी इकट्ठा करने के लिए किया जा सकता है या एकत्र किया गया डेटा हमले का अंतिम लक्ष्य हो सकता है। इस हमले में आम तौर पर स्नीफिंग-नेटवर्क ट्रैफ़िक शामिल होता है, लेकिन इसमें अन्य प्रकार की डेटा स्ट्रीम, जैसे रेडियो का अवलोकन करना शामिल हो सकता है। इस हमले की अधिकांश किस्मों में, हमलावर निष्क्रिय होता है और केवल नियमित संचार का निरीक्षण करता है, हालांकि कुछ रूपों में हमलावर डेटा स्ट्रीम की स्थापना शुरू करने या प्रेषित डेटा की प्रकृति को प्रभावित करने का प्रयास कर सकता है।

ii. डेटा संशोधन

संचार की गोपनीयता यह सुनिश्चित करने के लिए आवश्यक है कि डेटा को ट्रांज़िट में संशोधित या देखा नहीं जा सकता है। वितरित वातावरण अपने साथ यह संभावना लेकर आते हैं कि एक दुर्भावनापूर्ण तृतीय पक्ष डेटा के साथ छेड़छाड़ करके एक कंप्यूटर अपराध को अंजाम दे सकता है क्योंकि यह साइटों के बीच चलता है।

डेटा संशोधन हमले में, नेटवर्क पर एक अनधिकृत पार्टी ट्रांज़िट में डेटा को इंटरसेप्ट करती है और उस डेटा के कुछ हिस्सों को फिर से भेजने से पहले बदल देती है।

iii. डेटा चोरी

जब किसी व्यवसाय या अन्य व्यक्ति से अवैध रूप से कॉपी की गई या ली गई जानकारी का वर्णन करने के लिए उपयोग किया जाने वाला शब्द। आम तौर पर, यह जानकारी उपयोगकर्ता की जानकारी होती है जैसे पासवर्ड, सामाजिक सुरक्षा नंबर, क्रेडिट कार्ड की जानकारी, अन्य व्यक्तिगत जानकारी, या अन्य गोपनीय कॉर्पोरेट जानकारी। क्योंकि यह जानकारी अवैध रूप से प्राप्त की जाती है, जब इस जानकारी को चुराने वाले व्यक्ति को पकड़ा जाता है, तो संभावना है कि उस पर कानून की पूरी सीमा तक मुकदमा चलाया जाएगा।

2. नेटवर्क अपराध

i. नेटवर्क हस्तक्षेप

नेटवर्क डेटा को इनपुट, ट्रांसमिट, डैमेज, डिलीट, खराब, बदलना या दबा कर कंप्यूटर नेटवर्क के कामकाज में हस्तक्षेप करना।

ii. **नेटवर्क तोड़फोड़**

'नेटवर्क तोड़फोड़' या अक्षम प्रबंधक उन लोगों का काम करने की कोशिश कर रहे हैं जिनके वे आमतौर पर प्रभारी होते हैं? यह अकेले उपरोक्त या चीजों का संयोजन हो सकता है।

3. **पहुंच-अपराध**

i. **अनधिकृत पहुंच**

एक व्यक्ति किसी नेटवर्क, सिस्टम, एप्लिकेशन, डेटा या अन्य संसाधन की अनुमति के बिना तार्किक या भौतिक पहुंच प्राप्त करता है।

ii. **वायरस प्रसार**

दुर्भावनापूर्ण सॉफ़्टवेयर जो स्वयं को अन्य सॉफ़्टवेयर से जोड़ता है। (वायरस, वर्म्स, ट्रोजन हॉर्स, टाइम बम, लॉजिक बम, रैबिट और बैक्टीरिया दुर्भावनापूर्ण सॉफ़्टवेयर के उदाहरण हैं जो पीड़ित के सिस्टम को नष्ट कर देते हैं।

4. **संबंधित अपराध**

i. **साइबर अपराध में सहायता और प्रोत्साहन**

एक व्यक्ति जो किसी अपराध के होने से पहले उसके बारे में जानता है, और जो अपराध करने वालों को किसी प्रकार की सहायता देता है, कानूनी शब्दों में "तथ्य से पहले सहायक" के रूप में जाना जाता है। वह सलाह, कार्यों या मौद्रिक सहायता के माध्यम से सहायता कर सकता/सकती है। एक व्यक्ति जो अपराध होने से पहले अनजान है, लेकिन जो अपराध के बाद में मदद करता है, उसे "तथ्य के बाद सहायक" कहा जाता है।

ii. **कंप्यूटर से संबंधित जालसाजी और धोखाधड़ी**

कंप्यूटर जालसाजी और कंप्यूटर से संबंधित धोखाधड़ी कंप्यूटर से संबंधित अपराध हैं।

iii. **कंटेन्ट-संबंधित अपराध**

कंटेन्ट संबंधी अपराधों के तहत साइबरसेक्स, अवांछित वाणिज्यिक संचार, साइबर मानहानि और साइबर खतरे शामिल हैं।

IV. साइबर अपराध का प्रभाव

- **साइबर क्राइम का बच्चों पर प्रभाव**

  आजकल बच्चों की आंखों में सबसे बड़ा डर साइबर बुलिंग का है। यह पिछले पांच वर्षों में आम हो गया है, और आमतौर पर निरीक्षण के अनुसार अठारह वर्ष से कम उम्र के लोग साइबर बुलिंग के प्रति अधिक संवेदनशील और भयभीत होते हैं। यह हमारे समाज में एक खतरनाक प्रवृत्ति बनती जा रही है। आंकड़ों के निरीक्षण के अनुसार, साइबर क्राइम का सबसे ज्यादा डर किशोर महिलाओं में है। साइबर बुलिंग एक डर है जब किसी व्यक्ति को किसी अन्य व्यक्ति से धमकियां, नकारात्मक टिप्पणियां, या नकारात्मक तस्वीरें या टिप्पणियां मिलती हैं।

- **वित्तीय क्षेत्र**

  वित्तीय संस्थानों पर साइबर हमले के परिणामस्वरूप पर्याप्त वित्तीय नुकसान हो सकता है और संवेदनशील ग्राहक डेटा से समझौता हो सकता है। उल्लंघनों से पहचान की चोरी, अनधिकृत लेनदेन और वित्तीय धोखाधड़ी हो सकती है। इस तरह की घटनाएं वित्तीय प्रणालियों में जनता के विश्वास को कम करती हैं और अर्थव्यवस्था पर लंबे समय तक चलने वाले प्रभाव पड़ सकते हैं।

- **स्वास्थ्य सेवा**

  स्वास्थ्य सेवा क्षेत्र मूल्यवान रोगी डेटा रखता है, जिससे यह साइबर अपराधियों के लिए एक आकर्षक लक्ष्य बन जाता है। स्वास्थ्य सेवा में डेटा का उल्लंघन रोगी की गोपनीयता से समझौता कर सकता है, चिकित्सा पहचान की चोरी का कारण बन सकता है और स्वास्थ्य सेवाओं को बाधित कर सकता है। इसके अतिरिक्त, चिकित्सा उपकरणों और बुनियादी ढांचे पर हमले रोगी की सुरक्षा को खतरे में डाल सकते हैं।

- **खुदरा और ई-कॉमर्स**

  खुदरा व्यवसायों और ई-कॉमर्स प्लेटफॉर्म पर साइबर हमले के परिणामस्वरूप डेटा उल्लंघन, ग्राहक भुगतान जानकारी और व्यक्तिगत डेटा उजागर हो सकते हैं। इससे प्रभावित कंपनियों में वित्तीय नुकसान, प्रतिष्ठा की क्षति और उपभोक्ता विश्वास का क्षरण हो सकता है।

- **ऊर्जा और उपयोगिताएँ**

  बिजली ग्रिड और उपयोगिताओं जैसे महत्वपूर्ण बुनियादी ढाँचे पर साइबर हमले के गंभीर परिणाम हो सकते हैं। वे आवश्यक सेवाओं को बाधित कर सकते हैं, बिजली कटौती का कारण बन सकते हैं और सार्वजनिक सुरक्षा को संभावित रूप से प्रभावित कर सकते हैं। राष्ट्र-राज्य अभिनेता या संगठित साइबर अपराधी समूह इन प्रणालियों को राजनीतिक या वित्तीय प्रेरणाओं के लिए लक्षित कर सकते हैं।

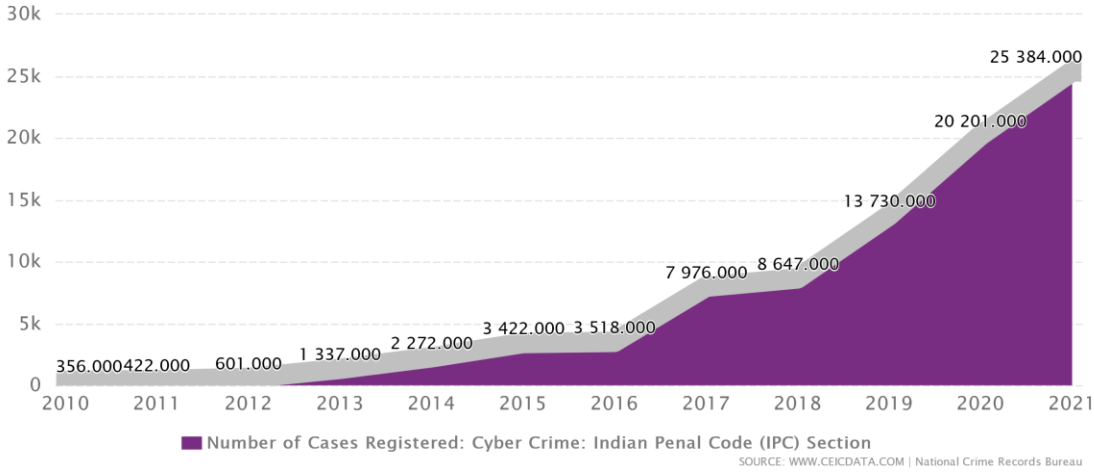
- **विनिर्माण और औद्योगिक प्रणालियां**

- विनिर्माण और औद्योगिक प्रणालियों पर हमले से उत्पादन में व्यवधान, बौद्धिक संपदा की चोरी और संवेदनशील औद्योगिक नियंत्रण प्रणालियों (आईसीएस) से समझौता हो सकता है। इसके परिणामस्वरूप वित्तीय नुकसान, प्रतिष्ठा की क्षति और सुरक्षा जोखिम हो सकते हैं।
- **सरकार और रक्षा**
  सरकारी संस्थाओं को लक्षित करने वाले साइबर हमलों के व्यापक प्रभाव हो सकते हैं। उल्लंघन राष्ट्रीय सुरक्षा से समझौता कर सकते हैं, वर्गीकृत जानकारी चुरा सकते हैं, सरकारी कार्यों को बाधित कर सकते हैं और महत्वपूर्ण बुनियादी ढांचे से समझौता कर सकते हैं। इन हमलों को राज्य-प्रायोजित समूहों या अन्य दुर्भावनापूर्ण अभिनेताओं द्वारा राजनीतिक प्रेरणा से अंजाम दिया जा सकता है।
- **शिक्षा**
  शैक्षिक संस्थानों में छात्र और कर्मचारी रिकॉर्ड सहित मूल्यवान व्यक्तिगत डेटा होता है। साइबर हमले के परिणामस्वरूप डेटा उल्लंघन, पहचान की चोरी और शैक्षणिक संसाधनों तक अनधिकृत पहुंच हो सकती है। वे शैक्षिक सेवाओं को बाधित कर सकते हैं और छात्रों और कर्मचारियों की गोपनीयता से समझौता कर सकते हैं।
- **परिवहन**
  एयरलाइंस, रेलवे और सार्वजनिक परिवहन नेटवर्क सहित परिवहन प्रणालियों पर हमले, सेवाओं को बाधित कर सकते हैं, यात्री सुरक्षा से समझौता कर सकते हैं और वित्तीय नुकसान का कारण बन सकते हैं। साइबर अपराधी इन प्रणालियों को टिकट प्रणाली, संचार नेटवर्क, या परिवहन बुनियादी ढांचे में कमजोरियों का फायदा उठाने के लिए लक्षित कर सकते हैं।
- **मीडिया और मनोरंजन**
  मीडिया और मनोरंजन उद्योग में साइबर अपराध में अक्सर बौद्धिक संपदा की चोरी, पायरेसी और कॉपीराइट की गई सामग्री का अनधिकृत वितरण शामिल होता है। यह वित्तीय नुकसान, प्रतिष्ठा की क्षति का कारण बन सकता है और रचनात्मक उद्योग की राजस्व धाराओं को प्रभावित कर सकता है।
- **व्यक्ति और व्यक्तिगत गोपनीयता**
  पहचान की चोरी, ऑनलाइन घोटाले, रैनसमवेयर हमले और फ़िशिंग जैसे विभिन्न माध्यमों से साइबर अपराध का व्यक्तियों पर सीधा प्रभाव पड़ सकता है। व्यक्तिगत जानकारी चोरी हो सकती है, जिससे वित्तीय नुकसान, प्रतिष्ठा की क्षति और भावनात्मक संकट हो सकता है।

V. एक संक्षिप्त सर्वेक्षण

- भारत साइबर अपराध: IPC अनुभाग: पंजीकृत मामलों की संख्या 2021 में 25,384.000 यूनिट दर्ज की गई थी।

- यह 2020 के लिए 20,201.000 यूनिट की पिछली संख्या से वृद्धि दर्ज करता है।
- 20 अवलोकनों के साथ दिसंबर 2002 से 2021 तक औसत 669.500 यूनिट।
- डेटा 2021 में 25,384.000 यूनिट के सर्वकालिक उच्च स्तर पर और 2008 में 176.000 यूनिट के रिकॉर्ड निचले स्तर पर पहुंच गया।



VI. संदर्भ

1. https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/cybercrime-that-compromises-privacy.html,
2. IMDb (2012), Unauthorized Attacks, Available at: http://www.imdb.com/title/tt0373414/,
3. Computer Hope (2012), Data Theft, Available at: https://www.computerhope.com/jargon/d/datathef.htm, Visited: 07/06/2023.
4. Nidhi Narnolia. https://www.legalserviceindia.com/legal/article-4998-cyber-crime-in-india-an-overview.html National Crime Records Bureau: https://www.ceicdata.com/en/india/crime-statistics/cyber-crime-ipc-section-number-of-cases-registered

****