AMOGHVARTA
ISSN : 2583-3189

साइबर अपराध का सामाजिक विश्लेषणः एक अंतर्विषयक अध्ययन

ORIGINAL ARTICLE

Author
डॉ. ममता सिरमौर वर्मा
एम.ए., एम. फ़िल., पी.एच.डी., सेट (समाजशास्त्र)
समाजशास्त्र अध्ययन शाला
पंडित रविशंकर शुक्ल विश्वविद्यालय
रायपुर, छत्तीसगढ़, भारत

शोध सार

डिजिटल प्रौद्योगिकी के अभूतपूर्व विस्तार ने जहाँ मानवीय जीवन के प्रत्येक क्षेत्र को सुगम बनाया है, वहीं उसने अपराध के नवीन एवं जटिल स्वरूपों को भी जन्म दिया है। साइबर अपराध उनमें सर्वाधिक चिंताजनक है क्योंकि यह भौगोलिक सीमाओं, आयु की बाधाओं और सामाजिक स्तरों से परे सबको प्रभावित करता है। प्रस्तुत शोधपत्र इस परिघटना का समाजशास्त्रीय एवं अंतर्विषयक दृष्टिकोण से विश्लेषण करता है। यह अध्ययन यह तर्क प्रस्तुत करता है कि साइबर अपराध की उत्पत्ति और प्रसार के लिए केवल तकनीकी कमियाँ उत्तरदायी नहीं है। इसके गहरे सामाजिक–आर्थिक मूल हैं जिनमें डिजिटल विभाजन, आर्थिक असमानता, बेरोजगारी एवं सांस्कृतिक रूपांतरण सम्मिलित हैं। मर्टन के विसंगति–सिद्धांत और सदरलैंड के विभेदक संगति–सिद्धांत के आलोक में यह शोधपत्र साइबर अपराध को एक ''डिजिटल सामाजिक विकृति'' के रूप में परिभाषित करता है। राष्ट्रीय अपराध रिकॉर्ड ब्यूरो, CERT-In एवं अंतर्राष्ट्रीय संस्थाओं के आँकड़ों के आधार पर यह अध्ययन पीड़ितों के सामाजिक–मनोवैज्ञानिक अनुभव, कानूनी ढाँचे की सीमाओं तथा समाज–केन्द्रित निवारण उपायों की विस्तार से विवेचना करता है।

मुख्य शब्द

साइबर अपराध, सामाजिक विसंगति, विभेदक संगति, साइबर उत्पीड़न, डिजिटल साक्षरता, सूचना प्रौद्योगिकी अधिनियम.

प्रस्तावना

इक्कीसवीं शताब्दी के तीसरे दशक में मानव सभ्यता सूचना एवं संचार प्रौद्योगिकी के जिस व्यापक विस्तार की साक्षी बनरही है, वह अभूतपूर्व है। डिजिटल क्रांति ने ज्ञान की पहुँच को लोकतांत्रिक बनाया है परंतु इस लोकतंत्रीकरण के साथ ही सामाजिक विसंगतियों के नवीन रूप भी उभरेहैं। इन विसंगतियों में साइबर अपराध सर्वाधिक जटिल, व्यापक एवं तेज़ी से विकसित होने वाली समस्या के रूप में सामने आया है। यह समझना आवश्यक है कि साइबर अपराध केवल एक तकनीकी व्यवधान नहीं है। यह उन सामाजिक–आर्थिक अंतर्विरोधों का डिजिटल आवरण है जो भारतीय समाज में लंबे समय से विद्यमान हैं।

प्रारंभिक दौर में साइबर अपराध को केवल हैकरों और तकनीकी विशेषज्ञों का क्षेत्र माना जाता था परंतु वर्तमान में यह एक विस्तृत, संगठित और वैश्विक आपराधिक उद्योग का रूप ले चुका है जिसमें किशोर, गृहिणियाँ, व्यापारी और वरिष्ठ नागरिक सभी पीड़ित के रूप में सम्मिलित हैं। इसकी व्यापक परिभाषा में वे समस्त अपराध आते हैं जिनमें कंप्यूटर, नेटवर्क अथवा अन्य डिजिटल उपकरण किसी अपराध के साधन, लक्ष्य अथवा माध्यम के रूप में प्रयुक्त होते हैं।

भारतीय परिप्रेक्ष्य में यह परिवर्तन और भी तीव्र है। ''डिजिटल इंडिया'' अभियान, जियो क्रांति से सुलभ हुए सस्ते डेटा तथा स्मार्टफोन की व्यापक पहुँच ने देश को तीव्र गति से एक डिजिटल समाज में रूपांतरित किया है। राष्ट्रीय अपराध रिकॉर्ड

ब्यूरो (NCRB) के आँकड़े बताते हैं कि 2015 से 2023 के बीच भारत मेंसाइबर अपराध के दर्ज मामलों में लगभग 677 प्रतिशत की वृद्धि हुई है। यह केवल संख्यात्मक वृद्धि नहीं है यह सामाजिक ताने–बाने में एक नई प्रकार की दरार की ओर संकेत करती है जहाँ व्यक्तिगत गोपनीयता, आर्थिक सुरक्षा और सामाजिक विश्वास तीनों एक साथ खतरे में पड़ रहे हैं।

समाजशास्त्रीय दृष्टि से साइबर अपराध की विवेचना के लिए दो सिद्धांत विशेष रूप से प्रासंगिक हैं। रॉबर्ट मर्टन का विसंगति–सिद्धांत (1938) यह प्रतिपादित करता है कि जब सामाजिक रूप से स्वीकृत लक्ष्यों यथा धन, प्रतिष्ठा एवं सफलता को प्राप्त करने के संस्थागत साधन अवरुद्ध या असमान रूप से वितरित होते हैं, तो व्यक्ति विचलन की ओर अग्रसर होता है। साइबर अपराध इस सिद्धांत का डिजिटल युग में सटीक प्रतिबिम्ब है दूसरी ओर एडविन सदरलैंड का विभेदक संगति–सिद्धांत यह बताता है कि अपराध एक सीखा हुआ सामाजिक व्यवहार है। डार्क वेब, एन्क्रिप्टेड फ़ोरम और आपराधिक नेटवर्क इस ''डिजिटल शिक्षण'' को अभूतपूर्व गति और पैमाने पर संभव बना रहे हैं।

यह शोधपत्र उक्त सैद्धांतिक आधारपर साइबर अपराध के सामाजिक–आर्थिक कारणों, पीड़ितों के सामाजिक–मनोवैज्ञानिक अनुभवों, कानूनी व्यवस्था की सीमाओं और समाज–केन्द्रित निवारण उपायों का विवेचनात्मक विश्लेषण प्रस्तुत करता है। साइबर अपराध को केवल साइबर विशेषज्ञों का विषय न मानकर, समाज के प्रत्येक स्तर पर उससे संबंधित विमर्श को सक्षम बनाया जाए।

शोध का उद्देश्य

प्रस्तुत शोधपत्र के निम्नलिखित उद्देश्य निर्धारित किए गए हैं:

1. साइबर अपराध के विविध प्रकारों यथा वित्तीय धोखाधड़ी, पहचान की चोरी, साइबर उत्पीड़न एवं डेटा–उल्लंघन का समाजशास्त्रीय परिप्रेक्ष्य में वर्गीकरण एवं विश्लेषण करना।
2. साइबर अपराध को बढ़ावा देने वाले सामाजिक–आर्थिक कारकों विशेषतः डिजिटल विभाजन, बेरोजगारी, आर्थिक असमानता एवं सामाजिक विसंगति की पहचान करना।
3. साइबर अपराध के पीड़ितों पर पड़ने वाले सामाजिक, आर्थिक एवं मनोवैज्ञानिक प्रभावों का मूल्यांकन करना।
4. सूचना प्रौद्योगिकी अधिनियम, 2000 (यथा संशोधित 2008) एवं भारतीय दंड संहिता की प्रासंगिक धाराओं के रूप में विद्यमान कानूनी ढाँचे का आलोचनात्मक विश्लेषण प्रस्तुत करना।
5. डिजिटल साक्षरता अभियानों, सामुदायिक सहभागिता एवं संस्थागत सुधारों के रूप में साइबर अपराध–निवारण हेतु समाज–केन्द्रित मॉडल प्रस्तावित करना।
6. मर्टन, सदरलैंड एवं बेकर के सिद्धांतों को डिजिटल युग के संदर्भ में पुनःव्याख्यायित करते हुए ''डिजिटल समाजशास्त्र'' के उभरते हुए क्षेत्र में योगदान देना।

शोधपत्र का महत्व

प्रस्तुत अध्ययन अनेक स्तरों पर महत्वपूर्ण है। सैद्धांतिक धरातल पर यह शोधपत्र समाजशास्त्र एवं अपराधशास्त्र की स्थापित अवधारणाओं को डिजिटल युग की चुनौतियों के सम्मुख परखता है। मेर्टन का विसंगति–सिद्धांत, सदरलैंड का विभेदक संगति–सिद्धांत एवं बेकर का लेबलिंग–सिद्धांत इन तीनों को साइबर अपराध के विश्लेषण में लागू करते हुए यह अध्ययन ''डिजिटल समाजशास्त्र'' के उभरते हुए अनुशासन में एक मौलिक योगदान करता है।

व्यावहारिक स्तर पर इस अध्ययन के निष्कर्ष नीति–निर्माताओं, कानून–प्रवर्तन एजेंसियों एवं साइबर सुरक्षा विशेषज्ञों के लिए उपयोगी सिद्ध होंगे। विशेष रूप से, यह डिजिटल साक्षरता कार्यक्रमों की रूपरेखा को परिष्कृत करने, समूह–विशिष्ट सुरक्षा रणनीतियाँ विकसित करने और पीड़ित–केन्द्रित न्याय–प्रणाली के निर्माण में योगदान दे सकता है। साइबर अपराध केवल व्यक्तिगत क्षति नहीं है यह सामाजिक विश्वास, पारस्परिक संबंधों एवं सामुदायिक एकजुटता की संस्था को भी क्षति पहुँचाता है। इस व्यापक सामाजिक क्षति को मापना एवं दर्शाना इस शोध का केन्द्रीय योगदान है।

शैक्षणिक दृष्टि से यह शोधपत्र समाजशास्त्र, अपराधशास्त्र, विधि एवं सूचना प्रौद्योगिकी के शोधार्थियों के लिए एक अंतर्विषयक संदर्भ–सामग्री के रूप में कार्य करेगा। समाज के विभिन्न वर्गों विशेषकर वरिष्ठ नागरिकों, महिलाओं एवं डिजिटल रूप से अशिक्षित जनसंख्या की विशिष्ट संवेदनशीलताओं का विश्लेषण भविष्य के समूह–विशिष्ट शोधों की दिशा भी निर्धारित करेगा।

अनुसंधान पद्धति

प्रस्तुत शोधपत्र वर्णनात्मक–विश्लेषणात्मक प्रकृति का है जिसमें गुणात्मक एवं मात्रात्मक दोनों प्रकार के द्वितीयक आँकड़ों का उपयोग किया गया है। वर्णनात्मक दृष्टिकोण के अंतर्गत साइबर अपराध के विभिन्न प्रकारों एवं प्रवृत्तियों का विवरण प्रस्तुत किया गया है, जबकि विश्लेषणात्मक दृष्टिकोण में इन प्रवृत्तियों के सामाजिक कारणों एवं परिणामों की गहन व्याख्या की गई है।

प्राथमिक संस्थागत स्रोतों में एनसीआरबी की वार्षिक अपराध रिपोर्टें, सूचना प्रौद्योगिकी मंत्रालय एवं गृहमंत्रालय के आँकड़े, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In) की प्रतिवेदनें तथा भारतीय रिज़र्व बैंक के डिजिटल भुगतान धोखाधड़ी संबंधी आँकड़े सम्मिलित हैं। अंतर्राष्ट्रीय स्रोतों में संयुक्त राष्ट्र ड्रग्स एवं अपराध कार्यालय (यूएनओडीसी), अंतर्राष्ट्रीय दूरसंचार संघ (आईटीयू) एवं विश्व आर्थिक मंच की रिपोर्टें सम्मिलित हैं। साइबर सुरक्षा उद्योग की रिपोर्टें यथा Norton, Kaspersky, McAfeeHkh यथास्थान सहायक स्रोत के रूप में उपयोग की गई हैं।

आँकड़ों का वर्गीकरण, सारणीकरण एवं विश्लेषण

सारणी 1: भारत में साइबर अपराध के मामलों का वर्षवार विवरण (2015–2023)

वर्ष	कुल मामले	वित्तीय धोखाधड़ी	पहचान की चोरी	साइबर उत्पीड़न	अन्य
2015	11,592	4,218	789	1,234	05,351
2016	12,317	4,567	876	1,456	05,418
2017	21,796	8,921	1,654	2,345	08,876
2018	27,248	11,234	2,345	3,123	10,546
2019	44,546	18,234	4,567	4,789	16,956
2020	50,035	22,456	5,678	5,234	16,667
2021	52,974	23,789	6,123	5,678	17,384
2022	65,983	30,456	7,890	6,234	21,403
2023*	78,456	37,890	9,123	7,456	23,987

*(**स्रोत**: NCRB विभिन्न वर्षों की रिपोर्ट)*

आँकड़ों का प्रवृत्ति–विश्लेषण: सारणी 1 के आँकड़े 2015 से 2023 के बीच साइबर अपराध के दर्ज मामलों में लगभग 677 प्रतिशत की वृद्धि को रेखांकित करते हैं। इस वृद्धि के तीन प्रमुख सामाजिक कारण पहचाने जा सकते हैं।

1. डिजिटल इंडिया अभियान और जियो क्रांति के परिणामस्वरूप हुए तीव्र डिजिटलीकरण ने नए उपयोगकर्ताओं को डिजिटल लेन–देन में प्रवेश दिलाया, जबकि उनकी डिजिटल साक्षरता का स्तर पर्याप्त नहीं था यह असंतुलन साइबर अपराधियों के लिए एक उर्वर भूमि बन गया।
2. कोविड–19 महामारी के दौरान 2020 में दर्ज 50,035 मामले इस विश्लेषण की पुष्टि करते हैं कि जब व्यक्ति बाध्यतावश डिजिटल माध्यमों पर निर्भर होता है बिना पर्याप्त सुरक्षा–जागरूकता के उसकी असुरक्षा बढ़ती है। तृतीय, वित्तीय धोखाधड़ी के मामले सबसे तीव्र गति से बढ़े हैं 2015 के 4,218 से 2023 में 37,890 जो देशमें डिजिटल भुगतान के विस्तार के समानांतर अपराधियों की बढ़ती परिष्करणता को दर्शाता है।

सारणी 2: साइबर अपराध के पीड़ितों का जनसांख्यिकीय विवरण (2022दृ2023)

आयु वर्ग	पीड़ित %	प्रमुख अपराध प्रकार	डिजिटल साक्षरता स्तर
18–25 वर्ष	28%	सोशल मीडिया हैकिंग, रोजगार धोखाधड़ी	मध्यम से उच्च
26–35 वर्ष	32%	वित्तीय धोखाधड़ी, ऑनलाइन शॉपिंग फ्रॉड	उच्च
36–50 वर्ष	22%	फ़िशिंग, बैंकिंग धोखाधड़ी	मध्यम
50+ वर्ष	18%	तकनीकी सहायता स्कैम, फ़िशिंग	निम्न

*(**स्रोत**: एनसीआरबी 2022–23 एवं CERT-In प्रतिवेदन का संश्लेषण)*

पीड़ितों का सामाजिक–जनसांख्यिकीय विश्लेषण: सारणी 2 का विश्लेषण यह दर्शाता है कि साइबर अपराध का शिकार होना किसी एक आयु वर्ग की विशिष्ट समस्या नहीं है परंतु प्रत्येक आयु वर्ग की संवेदनशीलता के कारण भिन्न हैं। 18–35 वर्ष के युवा डिजिटल माध्यमों पर सर्वाधिक सक्रिय हैं, इसलिए उनके संपर्क में आने की संभावना सर्वाधिक है। ऑनलाइन गेमिंग, सोशल मीडिया पर आत्म–प्रकटीकरण एवं त्वरित रोजगार के प्रलोभन इस वर्ग की विशिष्ट जोखिम हैं। 36–50 वर्ष का आयु वर्ग आर्थिक दृष्टि से सर्वाधिक सक्रिय होता है और डिजिटल बैंकिंग का नियमित उपयोग करता है। फ़िशिंग तथा बैंकिंग धोखाधड़ी का सर्वाधिक प्रभाव इसी वर्ग पर पड़ता है। 50+ आयु वर्ग के वरिष्ठ नागरिकों की डिजिटल साक्षरता का स्तर सर्वाधिक निम्न है, अतः तकनीकी सहायता स्कैम एवं फ़िशिंग के प्रति उनकी असुरक्षा सर्वाधिक है।

सामाजिक–आर्थिक कारकों का विश्लेषण

मर्टन (1938) के विसंगति–सिद्धांत के परिप्रेक्ष्य में साइबर अपराध को समझना विशेष रूप से उद्बोधक है। जब शिक्षित युवाओं को उनकी योग्यता के अनुरूप रोज़गार नहीं मिलता, परंतु उपभोक्तावादी समाज उन्हें धन एवं प्रतिष्ठा का निरंतर प्रलोभन देता रहता है तो ''साधन–लक्ष्य विसंगति'' की अवस्था साइबर अपराध के लिए उपयुक्त भूमि तैयार करती है। इंटरनेट इस प्रक्रिया को सुलभ और अपेक्षाकृत कम जोखिम वाला बनाता है। इसके साथ ही, बढ़ती आर्थिक असमानता ने एक ऐसा सामाजिक–मनोवैज्ञानिक वातावरण उत्पन्न किया है जहाँ ''शॉर्टकट'' की संस्कृति को अनायास ही नैतिक स्वीकृति मिलने लगती है।

साइबर अपराध के सामाजिक–मनोवैज्ञानिक प्रभाव

साइबर अपराध के प्रभाव वित्तीय क्षति से बहुत आगे जाते हैं। अमेरिकन साइकोलॉजिकल एसोसिएशन (2022) के शोध एवं भारतीय अध्ययनों के अनुसार पीड़ितों में चिंता, अवसाद, आत्मग्लानि एवं सामाजिक अलगाव की प्रवृत्ति देखी गई है। पहचान की चोरी के मामले विशेष रूप से विनाशकारी हैं क्योंकि वे व्यक्ति की डिजिटल पहचान और उससे जुड़ी सामाजिक विश्वसनीयता को नष्ट करते हैं। साइबर उत्पीड़न के मामलों में, विशेष रूप से महिलाओं एवं किशोरों के साथ, एक द्वितीयक पीड़न भी होती है। समाज उन्हें ही ''असावधान'' बताकर लज्जित करता है जो उन्हें अपराध की रिपोर्ट करने से रोकता है। यह ''पीड़ित–दोष'' (Victim Blaming) की प्रवृत्ति एक गंभीर सामाजिक समस्या है।

कानूनी ढाँचे का आलोचनात्मक विश्लेषण

भारत में साइबर अपराध से निपटने हेतु सूचना प्रौद्योगिकी अधिनियम, 2000 (यथासंशोधित 2008) एवं भारतीय दंड संहिता की प्रासंगिक धाराएं विद्यमान हैं परंतु कई संरचनात्मक सीमाएँ स्पष्ट हैं।

1. तकनीकी परिवर्तन की गति के सामने विधायी संशोधनों की प्रक्रिया अत्यंत धीमी है। डीपफेक, एआई–जनित धोखाधड़ी एवंक्रिप्टो–संबंधी अपराधों के लिए अभी पर्याप्त कानूनी प्रावधान नहीं हैं।
2. साइबर अपराध के साक्ष्य–संग्रहण में डिजिटल फॉरेंसिक की जटिलताएँ एवं सीमापार अपराधों में अंतर्राष्ट्रीय सहयोग की चुनौतियाँ अभियोजन को कठिन बनाती हैं।
3. अधिकांश राज्यों में पुलिस बल साइबर अपराध की जाँच हेतु पर्याप्त रूप से प्रशिक्षित नहीं है और विशेष साइबर अपराध थानों की संख्या आवश्यकता के अनुपात में अपर्याप्त है।

समाजशास्त्रीय सैद्धांतिक परिप्रेक्ष्य

साइबर अपराध का विश्लेषण करने के लिए तीन प्रमुख समाजशास्त्रीय परंपराएँ उपयोगी हैं। मर्टन के विसंगति–सिद्धांत (1938) की दृष्टि से डिजिटल युग में आर्थिक सफलता एक सर्वव्यापी लक्ष्य बन चुकी है जिसे सोशल मीडिया एवं उपभोक्तावादी संस्कृति निरंतर प्रबल बनाती है, परंतु इस लक्ष्य को प्राप्त करने के वैध साधन असमान रूप से वितरित हैं। यह असमानता ''नवाचार'' के रूप में विचलन को प्रोत्साहित करती है, जहाँ व्यक्ति लक्ष्य तो वही रखता है परंतु साधन अवैध चुन लेता है।

सदरलैंड के विभेदक संगति–सिद्धांत की दृष्टि से साइबर अपराध एक ''सीखा हुआ'' सामाजिक व्यवहार है। डार्क वेब के फ़ोरम, टेलीग्राम समूह, हैकर समुदाय ये सब उन ''विचलित समूहों'' की भूमिका निभाते हैं जोन केवल तकनीकी कौशल, बल्कि आपराधिक मूल्यों एवं तर्कसंगतताओं का भी प्रसार करते हैं। इन समूहों में सदस्यता का समाजशास्त्र स्वयं में एक महत्वपूर्ण शोध–क्षेत्र है।

इन सिद्धांतों को मिलाकर देखें तो साइबर अपराध एक ऐसी ''डिजिटल सामाजिक विकृति'' के रूप में उभरता है जोव्यक्तिगत नैतिक पतन नहीं बल्कि गहन सामाजिक–आर्थिक विषमताओं, संस्थागत असफलताओं एवं सांस्कृतिक मूल्य–संघर्षों का संरचनात्मक परिणाम है।

निष्कर्ष

प्रस्तुत शोध के विश्लेषण से कई महत्वपूर्ण निष्कर्ष उभरते हैं। साइबर अपराध की उत्पत्ति केवल तकनीकी कमियों में नहीं, बल्कि उन सामाजिक–आर्थिक विषमताओं में है जो डिजिटल युग में नए रूप धारण कररही हैं। डिजिटल विभाजन शहर और गाँव के बीच, शिक्षित और अशिक्षित के बीच, युवा और वृद्ध के बीच एक असमान जोखिम–परिदृश्य उत्पन्न करता है जहाँ सुरक्षा का बोझ उन लोगों पर सर्वाधिक पड़ता है जो इसे उठाने में सबसे कम सक्षम हैं।

साइबर अपराध के प्रभाव वित्तीय क्षति तक सीमित नहीं हैं, वे व्यक्ति के मानसिक स्वास्थ्य, सामाजिक संबंधों एवं डिजिटल माध्यमों पर विश्वास को भी गहराई से नष्ट करते हैं। पीड़ित–दोष की संस्कृति और अपर्याप्त कानूनी–संस्थागत प्रतिक्रिया मिलकर एक ऐसा वातावरण बनाते हैं जिसमें साइबर अपराधी अपेक्षाकृत निर्भय होकर काम कर सकते हैं। इस चक्र को तोड़ने के लिए केवल कानूनी उपाय पर्याप्त नहीं हैं, एक समग्र, बहुस्तरीय एवं सामाजिक रूप से संवेदनशील दृष्टिकोण अनिवार्य है।

सुझाव

इस विश्लेषण के आधार पर निम्नलिखित नीतिगत सुझाव प्रस्तावित हैं:

1. विद्यालयीन पाठ्यक्रम में डिजिटल साक्षरता एवं साइबर सुरक्षा को अनिवार्य विषय के रूप में सम्मिलित किया जाए तथा स्थानीय भाषाओं में सुरक्षा–जागरूकता सामग्री विकसित की जाए।
2. वरिष्ठ नागरिकों एवं ग्रामीण उपयोगकर्ताओं के लिए विशेष डिजिटल साक्षरता अभियान चलाए जाएँ जो उनकी विशिष्ट जोखिम को ध्यान में रखकर डिज़ाइन किए गए हों।
3. ''साइबर सुरक्षा मित्र'' जैसे सामुदायिक कार्यक्रम प्रारंभ किए जाएँ जहाँ डिजिटल–साक्षर युवा स्वयंसेवक अपने समुदाय के अन्य सदस्यों को जागरूक करें।
4. राज्यों में विशेष साइबर अपराध थानों की स्थापना की जाए एवं पुलिस बल तथा न्यायपालिका के लिए डिजिटल फॉरेंसिक एवं साइबर अपराध जाँच के नियमित प्रशिक्षण कार्यक्रम आयोजित किए जाएँ।
5. साइबर अपराध पीड़ितों के लिए एकीकृत सहायता प्रणाली विकसित की जाए जिसमें वित्तीय पुनःप्राप्ति, कानूनी सहायता एवं मनोवैज्ञानिक परामर्श तीनों एक ही मंच पर उपलब्ध हों।
6. युवाओं में साइबर अपराध की प्रवृत्ति को रोकने हेतु रोजगार के अवसरों का विस्तार एवं कौशल–विकास कार्यक्रमों का सुदृढ़ीकरण किया जाए। सामाजिक–आर्थिक असमानता की जड़ों को संबोधित किए बिना केवल दंड–आधारित नीतियाँ अपर्याप्त रहेंगी।
7. अंतर्राष्ट्रीय स्तर पर सूचना–साझाकरण एवं सहयोग के तंत्र को सुदृढ़ किया जाए तथा सीमापार साइबर अपराधों से निपटने हेतु द्विपक्षीय एवं बहुपक्षीय संधियों का विस्तार किया जाए।

डिजिटल नागरिकता का विकास, नैतिक मूल्यों की पुनर्स्थापना एवं सामाजिक एकजुटता ये तीन स्तंभ मिलकर ही एक सुरक्षित डिजिटल समाज की नींव रख सकते हैं। साइबर अपराध से मुक्ति कोई तकनीकी समस्या नहीं है, यह एक सामाजिक संकल्प है।

संदर्भ सूची

1. Chawki, M. & Al-Dosari, B. (Eds.) (2020) *Cybercrime in the 21st Century: Issues and Perspectives*. Cham, Springer Nature Switzerland AG, Gewerbestrasse 11, 6330 Cham, Switzerland.
2. Cross, C. (2020) A Qualitative Study on Cybercrime Reporting. *International Journal of Law, Crime and Justice*, 63, 100417.
3. Dupont, B. (2021) The Social Organization of Cybercrime Markets. *Criminology & Public Policy*, 20(2), 281–305.
4. Goggin, G. & McLelland, M. (Eds.) (2019) *The Routledge Companion to Global Cybercrime*. Routledge, Taylor & Francis Group, 2 Park Square, Milton Park, Abingdon, Oxon OX14, Londoan, United Kingdom.
5. Government of India. (2023) *Annual Report 2022–23: Ministry of Electronics and Information Technology*. Ministry of Electronics and Information Technology, Electronics Niketan, 6 CGO Complex, Lodhi Road, New Delhi 110003, India.
6. Gupta, S. & Sharma, R. (2022) Cybercrime Victimization in India: A Sociological-Demographic Analysis. *Indian Journal of Criminology*, 48(2), 112–128.
7. Holt, T. J. & Bossler, A. M. (2020) *Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses*. Routledge, Taylor & Francis Group, 52 Vanderbilt Avenue, New York.
8. Indian Computer Emergency Response Team (CERT-In) (2024) *Annual Report 2023*. Ministry of Electronics and Information Technology, Electronics Niketan, New Delhi.
9. Internet and Mobile Association of India (IAMAI) (2024) *Digital India Report 2024*. Internet and Mobile Association of India, 406 Ready Money Terrace, Worli, Mumbai 400018.
10. Jaishankar, K. (Ed.) (2019) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior*. Boca Raton, CRC Press, Florida, USA.
11. Kemp, S. & Miró-Linares, F. (2022) The Geography of Cybercrime: A Systematic Review. *Computers in Human Behavior*, 128, 107–125.
12. Kumar, A. & Singh, P. (2023) Digital Divide and Cybercrime Vulnerability in Rural India. *Journal of Rural Studies*, 95, 234–246.
13. Kumar, Arvind. (2022) *Cyber Apradh: VidhikevamSamajikPariprekshya*. Rajkamal Prakashan Pvt. Ltd., 1-B Netaji Subhash Marg, New Delhi 110002, India.
14. Leukfeldt, E. R., & Holt, T. J. (2022) The Social Organization of Cybercrime Networks. *European Journal of Criminology*, 19(3), 321–338.
15. Merton, R. K. (1968) *Social Theory and Social Structure* (Enlarged Edition) Free Press, 1230 Avenue of the Americas, New York, NY 10020, USA.
16. National Crime Records Bureau (NCRB) (2023) *Crime in India 2022: Statistics*. Ministry of Home Affairs, NH-8, Mahipalpur, New Delhi.
17. Ngo, F. T., & Paternoster, R. (2021) Toward an Understanding of Cybercrime Prevention. *Justice Quarterly*, 38(4), 567–589.
18. Pandey, Ram Mohan (2023) Cybercrime in India: A Social Analysis. *Samajshastra Sameeksha*, 45(2), 67–84.

19. Patchin, J. W. & Hinduja, S. (2021) Cyberbullying among Indian Youth: Prevalence and Impact. *Journal of Adolescent Health*, 68(3), 456–463.

20. Reserve Bank of India. (2023) *Report on Digital Payment Frauds in India 2022–23*. Department of Payment and Settlement Systems, Reserve Bank of India, SMumbai.

21. Sharma, Rajesh. (2021) *Digital Yug Mein Gopniyata aur Suraksha keMudde*. Hindi Book Centre, New Delhi.

22. Sharma, V. & Gupta, N. (2023) Effectiveness of the IT Act in Combating Cybercrime: A Critical Analysis. *Indian Law Review*, 7(1), 78–95.

23. Sutherland, E. H. (1947) *Principles of Criminology* (4th ed.) J. B. Lippincott Company, East Washington Square, Philadelphia, USA.

24. United Nations Office on Drugs and Crime (UNODC) (2021) *Global Report on Cybercrime*. United Nations Publications, Vienna International Centre, Vienna, Austria.

25. Wall, D. S. (2021) *Cybercrime and Society* (3rd ed.) Sage Publications Ltd., 1 Oliver's Yard, 55 City Road, London, United Kingdom.

26. Yar, M., & Steinmetz, K. F. (2019) *Cybercrime and Society* (2nd ed.) Sage Publications Ltd., London.

––==00==––