Naveen Shodh Sansar (An International Refereed / Peer Review Multidisciplinary Research Journal)
RNI No.- MPHIN/2013/60638, ISSN 2320-8767, E- ISSN 2394-3793, Scientific Journal Impact Factor (SJIF)- 8.054,
April to June 2026, E-Journal, Vol. I, Issue LIV (54), ISO 9001:2015 - E2024049304 (QMS)

भारत में साइबर अपराध और साइबर सुरक्षा : उभरते खतरे और चुनौतियां

डॉ. आभा सैनी*

* प्रोफेसर एवं अध्यक्ष (राजनीति विज्ञान) जैन कन्या स्नातकोत्तर महाविद्यालय, मुजफ्फरनगर (उ.प्र.) भारत

प्रस्तावना – आत्मनिर्भर भारत और भारतीय अर्थव्यवस्था, भारत की एक विशिष्ट पहचान अंतरराष्ट्रीय स्तर पर बना रहे हैं आत्मनिर्भर भारत आत्मविश्वास से भरे भारतीय लोगों की अवधारणा का प्रतिनिधित्व करता है और देश की अर्थव्यवस्था को मजबूत करता है। यह भारतीय अर्थव्यवस्था के सभी क्षेत्रों की गुणवत्ता और क्षमता तय करता है। मेक इन इंडिया, मेड इन इंडिया, मेड फॉर द वर्ल्ड इससे संबंधित 3एम हैं। आजकल, डिजिटल इंडिया कार्यक्रम भी भारतीय अर्थव्यवस्था को मजबूत बनाने में अपना योगदान देता है वैश्वीकरण के युग में, बढ़ते इंटरनेट उपयोगकर्ताओं के कारण साइबर अपराध बढ़ गए हैं और इसीलिए साइबर सुरक्षा एक आवश्यकता बन गई है। साइबर सुरक्षा में, डेटा को अनधिकृत स्रोतों से सिस्टम और नेटवर्क में सुरक्षित किया जाता है। साइबर खतरों के बदलते पैटर्न, कुशल साइबर सुरक्षा पेशेवरों की कमी, साइबर सुरक्षा के लिए इंटरनेट उपयोगकर्ताओं की जागरूकता की कमी आदि भारत में बहुत सारे मुद्दे और चुनौतियां हैं। साइबर अपराध अब राष्ट्रीय सुरक्षा, आर्थिक स्थिरता और व्यक्तिगत निजता के लिए गंभीर खतरा बन गया है।

साहित्य पुनरावलोकन

डॉक्टर एस. मार्सेलिन पुष्पा (2024) इंडियन गवर्नेंस के लगातार बदलते नजरिए को खासकर वैश्विक दुनिया के संदर्भ में वर्णन करती है। उन्होंने प्रशासन और डिजिटल सुरक्षा डिजिटल ट्रांसफॉर्मेशन, नागरिकों की भागीदारी और डिजिटल गवर्नेंस में भविष्य के ट्रेंड्स पर भी चर्चा की।

डॉ. अवस्थी और अवस्थी (2014) ने भारतीय प्रशासन के अलग-अलग पहलुओं और चुनौतियों पर चर्चा की है जिसमें सूचना प्रौद्योगिकी और ई प्रशासन सम्मिलित है टांगजैम कै सिंह(2024) का मानना है कि पिछले दशकों में साइबर सुरक्षा का परिदृश्य बढ़ती हुई नई तकनीक के कारण तेजी से बड़ा है वह साइबर इकोसिस्टम की वर्तमान और भविष्य की बदलती हुई प्रवृत्तियो और चुनौतियों एवं सरकार की साइबर नीति को बताते हैं।

माइकल ई. मिलाकोविच (2012) पब्लिक सर्विस और भागीदारी को बेहतर बनाने के लिए एक नई टेक्नोलॉजी के तौर पर डिजिटल गवर्नेंस का विश्लेषण करते हैं। डॉ. बी.एल. फादिया (2003) डिजिटल और ई-गवर्नेंस और इन्फॉर्मेशन टेक्नोलॉजी के बारे में वर्णन करते हैं।

रघु संथानम और एम सेतु माधवन एवं मोहित वीरेंद्र (2011) साइबर सुरक्षा साइबर अपराध और साइबर फॉरेंसिक साइंस के प्रयोग और अवधारणा को विश्लेषित करते हैं।

शोध उद्देश्य और शोध विधि – प्रस्तुत शोध पत्र में साइबर अपराध और साइबर सुरक्षा की अवधारणा की व्याख्या की गई है इस शोध पत्र का उद्देश्य साइबर अपराध और साइबर सुरक्षा की उभरती हुई प्रवृत्तियों और चुनौतियों का विश्लेषण करना है भारत में साइबर खतरों से निपटने हेतु साइबर जागरूकता के महत्व की व्याख्या करना है प्रस्तुत शोध पत्र में भारत सरकार के द्वारा इस संदर्भ में उठाए गए कदमों का भी विश्लेषण किया गया हैऔर इस संदर्भ में उत्पन्न चुनौतियों और उन समस्याओं के समाधान को भी प्रस्तुत शोध पत्र में प्रस्तुत किया गया है प्रस्तुत शोध पत्र में प्राथमिक और द्वितीय स्रोतों का प्रयोग किया गया है प्रस्तुत शोध पत्र में ऐतिहासिक विश्लेषणात्मक और वर्णनात्मक शोध पद्धति का प्रयोग किया गया है।

साइबर अपराध और साइबर सुरक्षा– साइबर अपराध वह अपराध है जिसमें इंटरनेट, कंप्यूटर, मोबाइल फोन या किसी डिजिटल सिस्टम का उपयोग करके अपराध को अंजाम दिया जाता है। जैसे – व्यक्तिगत पैसे डेटा चोरी करना, ऑनलाइन बैंकिंग और यूपीआई फ्रॉड कर बैंक डिपॉजिट से बेचना, अश्लील सामग्री फैलाना या सरकारी वेबसाइट हैक करना।

साइबर अपराध में व्यक्ति के विरुद्ध अपराध सम्मिलित है जिसमें पहले साइबर सटॉर्किंग अर्थात किसी व्यक्ति को बार-बार मैसेज करना जिससे कि वह मानसिक रूप से परेशान हो जाए दूसरे साइबर बुलिंग, किसी व्यक्ति का बार-बार ऑनलाइन मजाक उड़ाना धमकाना और सामान बेचना तीसरा, डॉक्सिंग, अर्थात किसी व्यक्ति की निजी जानकारी चुराकर उसे ऑनलाइन साझा करना जिसमें उसकी तस्वीर पता इत्यादि सम्मिलित हो चौथा फिशिंग जिसमें नकली ईमेल या वेबसाइट के माध्यम से लोगों की व्यक्तिगत जानकारी चुराना सम्मिलित है पांचवा ऑनलाइन यौन उत्पीड़न छठ फर्जी सोशल प्रोफाइल बनाना इसमें सम्मिलित किया जाता है।

दूसरे प्रकार का साइबर अपराध संपत्ति के विरुद्ध अपराध है जिसमें हैकिंग सम्मिलित है किसी के कंप्यूटर सिस्टम में अनधिकृत प्रवेश करना, दूसरे किसी के डाटा को नष्ट करने या खत्म करने की साइबर बॉर्बर्टा, तीसरी लाइसेंस के उपयोग या वितरण के बिना साइबर पायरेसी ,नकली फोन करके या नकली तरीके से क्रेडिट कार्ड की जानकारी चुराना और क्रेडिट कार्ड की धोखाधड़ी करना और रन समबियर अटैक कंप्यूटर को लॉक कर देना और उसके बदले में रोजगार की मांग करना।

तीसरे प्रकार का साइबर अपराध समाज और सरकार के प्रति है जिसमें

साइबर आतंकवाद सम्मिलित है जिसके अंतर्गत देश की रक्षा अथवा सरकारी नेटवर्क में घुसपैठ करना क्या उसे पर हमला करना सरकार की गुप्त जानकारी चलाने के लिए साइबर जासूसी करना इसके अतिरिक्त इसमें साइबर युद्ध भी सम्मिलित है जिसमें एक देश के द्धारा दूसरे देश पर साइबर तरीकों से उसको बाधित किया जाता है अभी हाल ही में रूस और यूक्रेन के युद्ध के दौरान इस तरीके की गतिविधि देखी गई वर्तमान समय में इंटरनेट के बढ़ते उपयोग के कारण सोशल नेटवर्क का प्रयोग भी बड़ा है इसीलिए इन सोशल नेटवर्क साइट के जरिए गलत समाचार प्रसारित करके हिंसा भड़काई जाती है या भ्रम फैलाया जाता है यह भी साइबर अपराध की श्रेणी में आता है

साइबर सुरक्षा कंप्यूटर सिस्टम, नेटवर्क और डेटा को अनधिकृत पहुंच या हमलों से बचाने की प्रक्रिया है। इसमें नेटवर्क सुरक्षा, एंडपॉइंट सुरक्षा, क्लाउड सुरक्षा और डेटा सुरक्षा जैसे प्रमुख क्षेत्र शामिल हैं। साइबर सुरक्षा में महत्वपूर्ण बुनियादी सुरक्षा ढांचा हैं।बचाव के तरीक में मजबूत पासवर्ड ,हमेशा कठिन और अलग-अलग पासवर्ड का उपयोग करना चाहिए साथ में टू-फैक्टर ऑथेंटिकेशन (2FA)अर्थात लॉगिन के लिए पासवर्ड के साथ ओटीपी (OTP) का उपयोग करना चाहिए।अपने डिवाइस और ऐप्स को हमेशा अपडेट रखें ताकि सुरक्षा खामियां दूर हो सकें।

एक भरोसेमंद एंटी-वायरस का उपयोग करें। किसी भी अनजान लिंक (URL) पर क्लिक न करें और अपना पासवर्ड या OTP किसी के साथ शेयर न करें।किसी भी अनजान क्यूआर (QR) कोड को स्कैन करने या UPI पिन डालने से पहले सोचें, क्योंकि पिन हमेशा पैसे भेजने के लिए होता है, प्राप्त करने के लिए नहीं।अपने महत्वपूर्ण डेटा का बैकअप हमेशा सुरक्षित रखें।सोशल मीडिया पर अपनी व्यक्तिगत जानकारी सार्वजनिक न करें और समय-समय पर अपने सभी ऑनलाइन खातों के पासवर्ड बदलते रहें। यदि कोई आपको ऑनलाइन परेशान कर रहा है, तो उसका स्क्रीनशॉट लें, उसे ब्लॉक करें और तुरंत नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल पर रिपोर्ट करें।

भारत में साइबर अपराध और साइबर सुरक्षा के उभरते खतरे और चुनौतियां -वर्तमान समय में डिजिटल इंडिया के क्षेत्र में भारत आगे पहुंचा है और उसे आर्थिक लाभ भी इसमें प्राप्त हुआ है भारत में ऑनलाइन सुरक्षा बाजार 2025 में लगभग 10.84 बिलियन अमेरिकी डॉलर का हो गया है वहीं दूसरी और साइबर अपराध और साइबर धोखाधड़ी भी बड़ी है 2025 की पहली छमाही में भारत को साइबर धोखाधड़ी के कारण प्रति माह औसतन रू 1,000 करोड़ का नुकसान हुआ, जो कुल रू 7,000 करोड़ तक पहुँच गया।प्रमुख धोखाधड़ी शेयर बाजारधनिवेश धोखाधड़ी, डिजिटल अरेस्ट स्कैम, कार्य-आधारित और निवेश-आधारित धोखाधड़ी भारत में सक्रिय भरती एजेंट जरिए के द्धारा की जाती है।भारत के साइबर धोखाधड़ी पारिस्थितिकी तंत्र का दुरुपयोग के कारणों में डिजिटल बैंकिंग लेनदेन में खामियाँ, टेलीकॉम सेक्टर में PoS एजेंटों द्धारा फर्जी सिम कार्ड जारी करना, आव्रजन में कमजोर सत्यापन प्रक्रियाएँ, आदि शामिल हैं, जिससे अज्ञात और सीमापार साइबर अपराध संभव हो पाते हैं। असंतोष, निजी लाभ, विचारधारा के आधार पर हिंसक होने पर और भू राजनीतिक स्थितियों के कारण साइबर अपराधों में वृद्धि हुई है राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (NCRB) के आंकड़ों के अनुसार, भारत में साइबर अपराधों में लगातार तेजी दर्ज की गई है। मामलों में लगभग 18% से 24% की वार्षिक वृद्धि हुई है। इन मामलों में लगभग 73% से अधिक घटनाएं वित्तीय धोखाधड़ी और ऑनलाइन ठगी से संबंधित हैं।

AI का खतरा 2025 में उसके बढ़ते प्रयोग के कारण साइबर अपराधों की श्रेणी में वृद्धि कर रहा है ।AIआधारित हमले और डीपफेक तकनीक सुरक्षा के लिए बड़ी चुनौती बन गए हैंआज के साइबर सिक्योरिटी खतरे, साइबर अटैक और सिक्योरिटी प्रोटोकॉल मुख्य चुनौतियों के रूप में उभर रहे हैं। भारत में इंटरनेट यूजर्स 25.15 करोड़ (2014) से बढ़कर 96.96 करोड़ (2024) हो गएय 97.65% गांवों में मोबाइल है, 96.80% में 4G है (मई 2025), लेकिन UN ई-गवर्नमेंट इंडेक्स (2024) में भारत 97वें स्थान पर है। भारत खास IT कानून वाला 12वां देश बन गया, जो भारत की डिजिटल इकॉनमी और इंटरनेट गवर्नेंस के लिए एक मजबूत फ्रेमवर्क देता है। लेकिन इसके बावजूद भी भारत में डिजिटल साक्षरता की कमी है और डिजिटल जागरूकता का अभाव निरंतर साइबर अपराध में वृद्धि करता है और साइबर सुरक्षा को चुनौती देता है भारत प्रौद्योगिकी और डिजिटल भुगतान का एक विशाल केंद्र है। इसी वजह से यह वैश्विक हैकर्स के लिए एक प्रमुख लक्ष्य बन जाता है। यहां मोबाइल आधारित हमलों की संख्या बहुत अधिक है।

साइबर टेररिज्म के अंतर्गत पेशेवर व्यक्तियों से काम लिया जाता है जिससे उन्हें कानूनी रूप से पकड़ना अत्यंत मुश्किल हो जाता है भारत में सरकारी विभागों में कुशल तकनीकी विशेषज्ञों की कमी है भारत में साइबर हमले की प्रमुख घटनाओं में एक मामला आधार डेटा लीक (2018) से संबंधित है जिसमें 1.1 अरब आधार कार्डधारकों की व्यक्तिगत जानकारी लीक हुई जिसमें आधार संख्या,PAN और बैंक विवरण शामिल थे। वर्ष 2022 में 9M कार्ड धारको का वित्तीय डाटा लीक हुआ जिसमें एसबीआई भी सम्मिलित था भारत में इंटरनेट उपयोगकर्ता की संख्या अधिक है लेकिन वह यह नहीं जानते कि अपना पासवर्ड साइबर सुरक्षा के लिए कैसे बनाएं साइबर सुरक्षा के लिए कौन सा एंटीवायरस डाउनलोड करें और साइबर सुरक्षा हेतु क्या-क्या प्रक्रिया है अपना ही जा सकती है ऑनलाइन बैंकिंग का कैसे इस्तेमाल किया जा सकता है सुरक्षित तरीके से ऑनलाइन व्यक्तिगत जानकारी कैसे साझा की जा सकती है बहुत सारे लोग साइबर अपराध होने पर भी उसकी रिपोर्ट दर्ज नहीं करते हैं।

मौजूदा सिस्टम में कई चुनौतियाँ हैं, जिसमें अलग-अलग एजेंसियों के बीच रेगुलेटरी ओवरलैप और टेलीकम्युनिकेशन, IT और ब्रॉडकास्टिंग के कन्वर्जेंस को ठीक करने के लिए एक ज्यादा यूनिफाइड अप्रोच की जरूरत शामिल है डिजिटलाइजेशन के कारण लोगों को रोजगार खाना पड़ रहा है और यह असंतोष का कारण बन रहा है यह लोगों के शारीरिक, मानसिक और भावनात्मक स्वास्थ्य को भी प्रभावित कर रहा है बच्चे और युवा वर्ग पर इसका अधिक प्रभाव हो रहा है।

IT एक्ट 2000 मुख्य कानून बना हुआ है, नए डेवलपमेंट IT रूल्स 2021 और प्रस्तावित डिजिटल इंडिया एक्ट के जरिए रेगुलेटरी फ्रेमवर्क को कड़ा करना है, जो इंटरमीडियरी अकाउंटेबिलिटी और कंटेंट रेगुलेशन पर बहुत ज्यादा फोकस करता है।खतरों में आए बदलावों से निपटने के लिए राष्ट्रीय साइबर सुरक्षा नीति (2013) जैसी नीतियों में संशोधन काफी समय से लंबित हैं।वर्तमान भारतीय साइबर सुरक्षा नीति को बढ़ते हुए मुद्दों का सामना करना पड़ रहा है जिसमें की आधुनिकतम तकनीक जैसे आर्टिफिशियल इंटेलिजेंस या 5G का बढ़ता हुआ प्रयोग है अधिकांश सरकारी और निजी संस्थानों में पुराने आईटी सिस्टम का इस्तेमाल किया जाता है जो नए साइबर हमलों का मुकाबला करने में असमर्थ है एआई (AI) और डीपफेक जैसी नई तकनीकों के दुरुपयोग से निपटने के लिए कानूनों

को तेजी से अपग्रेड करने की भी चुनौती है साइबर अपराधियों का संगठन अब अंतर्राष्ट्रीय रैकेट और डार्क वेब के माध्यम से संगठित अपराध का रूप ले चुका है।साइबर अपराध अंतरराष्ट्रीय सीमाएं पर कर चुके हैं और उस समय अन्य देशों की कानून-प्रवर्तन एजेंसियों के साथ तालमेल और साक्ष्य जुटाना कठिन होता है।

साइबर खतरों की प्रभावी पहचान और खतरों का उचित प्रबंधन भी एक जटिल चुनौती है तकनीकी प्रगति के साथ-साथ साइबर खतरे और अधिक चुनौती प्रस्तुत करते हैं मैलवेयर अर्थात दुर्भावना पूर्ण सॉफ्टवेयर और रेंनसमव्हेयर लगातार और तेजी से विकसित होने वाले साइबर खतरों में से एक बना हुआ है एआई-संचालित मैलवेयर, जीरो-डे एक्सप्लॉइट और फाइललेस अटैक के कारण व्यवसायों के लिए इन खतरों का पता लगाना और उनसे बचाव करना तेजी से मुश्किल होता जा रहा है।एक डिस्ट्रिब्यूटेड डिनायल-ऑफ-सर्विस (DDoS) हमले की विशेषता किसी नेटवर्क या सर्वर पर ट्रैफिक की मात्रा को अत्यधिक बढ़ा देना, उसे घेर लेना और अंतत: उसे ठप कर देना है। ऐसा हमला बहुत अधिक विघटनकारी होता है, जो वेबसाइटों को ठप कर देता है, ऑनलाइन लेनदेन को बाधित करता है, और डिजिटल सेवाओं को अनुपलब्ध कर देता है, जिससे डाउनटाइम कई घंटों या दिनों तक बना रहता है। साइबर सुरक्षा के लिए यह एक महत्वपूर्ण खतरा है।

साइबर अपराध रोकने और साइबर सुरक्षा के लिए भारत में सरकार के द्वारा किए गए प्रयास – डिजिटल इंडिया और डिजिटल गवर्नेंस सेवाओं को अधिक उपयोगकर्ता के अनुकूल और नागरिकों के लिए उत्तरदायी बनाता है ताकि पारदर्शिता और नागरिक प्रबंधन बढ़े। भारत ने कोविड 19 के समय डिजिटल महत्व को देखा। आजकल सभी नागरिक मोबाइल, इंटरनेट, व्हाट्सएप, सोशल मीडिया, इंटरनेट आधारित उपकरणों, ई-गवर्नेंस आदि जैसी डिजिटल संपत्तियों पर निर्भर हैं। ये उनके जीवन का हिस्सा हैं।भारत में इंटरनेट उपयोगकर्ताओं की संख्या 2010 से 2022 के बीच 10 गुना बढ़ी है और 2040 तक 100 मिलियन तक पहुंचने की उम्मीद है। मार्च 2014 तक कुल इंटरनेट ग्राहक 251.59 मिलियन से बढ़कर मार्च 2024 में 954.40 मिलियन हो गए। अप्रैल 2024 तक, प्रेस सूचना ब्यूरो की अगस्त 2024 की रिपोर्ट के अनुसार 95.15% गांवों में 3 जी / 4 जी मोबाइल कनेक्टिविटी के साथ इंटरनेट की सुविधा थी। इसके अलावा, अप्रैल 2024 तक, देश के 6,44,131 गांवों में से (गांवों का डेटा रजिस्ट्रार जनरल ऑफ इंडिया के अनुसार) 6,12,952 गांवों में 3जी/4जी मोबाइल कनेक्टिविटी है। इस तरह 95.15% गांवों में इंटरनेट की सुविधा है। इसका श्रेय सिर्फ मोबाइल डेटा प्लान को जाता है जो बहुत सस्ते दामों पर उपलब्ध हैं, भारत में 1GB की कीमत सिर्फ रू14 है।

डिजिटल डिवाइस का बढ़ता प्रयोग साइबर सुरक्षा की आवश्यकता को जन्म देता है भारत में साइबर अपराध को नियंत्रित करने की जानकारी के लिए सूचना प्रौद्योगिकी अधिनियम, 2000 (आईटी अधिनियम, 2000) लागू है, जिसे 2008 में बनाया गया कानूनी ढांचा सूचना प्रौद्योगिकी (IT) अधिनियम, 2000 भारत का प्राथमिक साइबर कानून है। साथ ही, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम (DPDP), 2023 नागरिकों के डेटा की गोपनीयता और सुरक्षा को मजबूत करता है। Ministry of Electronics and Information Technology (MeitY) द्वारा 25 फरवरी 2021 में एक नई गाइडलाइन दी गई जो सूचना तकनीक नियम 2021 के नाम से जानी जाती है राष्ट्रीय सुरक्षा साइबर सुरक्षा नीति 2013 का निर्माण किया गया है जिसमें सुरक्षित साइबर पर्यावरण बनाए रखने के लिए उचित दिशा निर्देश दिए गए हैं साइबर स्पेस को सुरक्षित करने के लिए एक समन्वित दृष्टिकोण का नीति का दृष्टिकोण देश की अर्थव्यवस्था के हर क्षेत्र में सरकार, उद्योग और डिजिटल समुदाय को शामिल करता है।2008 के संशोधन के माध्यम से साइबर आतंकवाद (धारा 66F) को दंडनीय बनाकर ऑनलाइन राष्ट्रीय सुरक्षा के लिए भारत की राष्ट्रीय नीति में सुधार करता है।

CERT-In (कंप्यूटर इमरजेंसी रिस्पांस टीम - भारत) भारत की एक एजेंसी है जो साइबर सुरक्षा का पता लगाती है,यह कंप्यूटर सुरक्षा से संबंधित घटनाओं पर प्रतिक्रिया देने वाली राष्ट्रीय नोडल एजेंसी है। उनका विश्लेषण करती है और अपनी कंपनी की रणनीति बनाती है। वायरस हटाने के लिए साइबर स्वच्छता केंद्र बुद्धि पोर्टल का निर्माण भी किया गया है CyMAC (Cyber Multi-Agency Centre)साइबर अपराध, जासूसी और आतंकवाद पर विभिन्न एजेंसियों के बीच बेहतर समन्वय के लिए इसे 2025 में और सशक्त बनाया गया है।

गृह मंत्रालय के द्वारा एक भारतीय साइबर अपराध समन्वय सहायता केंद्र भी बनाया गया है जिसके द्वारा राज्य और केंद्र के बीच समन्वय स्थापित करके व्यापक रूप से साइबर अपराधों से निपटने के लिए कार्य किया जाता है।कानून प्रवर्तन एजेंसियों को खोजी साइबर अपराध-केंद्रित डिजिटल फोरेंसिक उपकरण प्रदान करता है। साइबर अपराध का पता लगाने और जांच पर पुलिस और कानून प्रवर्तन एजेंसियों को प्रशिक्षण प्रदान करता है।वर्तमान में, साइबर अपराध मामलों की जांच में सहायता के लिए देश भर में सात केंद्रीय फोरेंसिक विज्ञान प्रयोगशालाएं और 27 राज्य फोरेंसिक विज्ञान प्रयोगशालाएं कार्यरत हैं।साइबर अपराध रिपोर्टिंग पोर्टल http://www.cybercrime.gov.in भी बनाया गया है जो ऑनलाइन शिकायत दर्ज करता है हेल्पलाइन नंबर साइबर अपराध की मदद के लिए 1930 डायल किया जा सकता हैं।NCIIPC राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र राष्ट्रीय सुरक्षा, अर्थव्यवस्था और सार्वजनिक सुरक्षा के लिए महत्वपूर्ण विभिन्न क्षेत्रों में महत्वपूर्ण सूचना अवसंरचना (CII) के संरक्षण के लिए जिम्मेदार केंद्रीय एजेंसी के रूप में कार्य करता है।CII ऑपरेटरों और सरकारी संस्थाओं को परामर्श, दिशानिर्देश और घटना रिपोर्ट जारी करता है।साइबर खतरों के खिलाफ CII की सुरक्षा के लिए विभिन्न सार्वजनिक और निजी क्षेत्र के हितधारकों के बीच साइबर सुरक्षा उपायों और प्रतिक्रियाओं का समन्वय करता है।

निष्कर्ष व सुझाव – 21वीं सदी में बढ़ते हुए डिजिटल उपयोग के कारण मनुष्य के जीवन को आसान तो बना दिया है लेकिन उसके साथ कहीं मुश्किलों को भी उत्पन्न किया है जिनमें एक है साइबर अपराध साइबर स्पेस आज के समय में लोगों को एक दूसरे के साथ जोड़ने और विश्व में अपना डाटा शेयर करने अर्थात सोशल नेटवर्क से संबंधित हो गया हैभारत में एक संपूर्ण साइबर सुरक्षा अधिनियम की आवश्यकता है जो डेटा की सुरक्षा, नेटवर्क सुरक्षा और साइबर खतरों से संबंधित सभी अलग-अलग ढांचों को जोड़ता हो। साइबर सुरक्षा का ढांचा तैयार करने में निजी क्षेत्र की कंपनियों का भी योगदान दिया जाए एवं अंतर्राष्ट्रीय स्तर पर विभिन्न देशों के साथ साइबर सुरक्षा ढांचा तैयार किया जाए साइबर अपराध को रोकने के लिए साइबर मामलों के तुरंत संस्थान के लिए फास्ट ट्रैक साइबर कोर्ट की स्थापना की जाए व्यक्तिगत टाटा संरक्षण के लिए वर्तमान कानून में व्यापक संशोधन

किया जाए स्वदेशी साइबर सुरक्षा नवाचार, अनुसंधान को बढ़ावा देना, तकनीकी और संस्थागत बुनियादी ढांचे का विकास करना,कॉर्पोरेट एवं बैंकिंग सुरक्षा उपाय को अपनाना, व्यवसायों और बैंकों में दो-चरणीय प्रमाणीकरण (2FA), डेटा एन्क्रिप्शन और सतत् निगरानी प्रणाली को अनिवार्य करना साइबर सुरक्षा के लिए जरूरी है साइबर शिक्षा को स्कूली शिक्षा में अनिवार्य बनाया जाए और सबसे महत्वपूर्ण साइबर सुरक्षा बनाए रखने के लिए और साइबर अपराध को रोकने के लिए साइबर सुरक्षा के बुनियादी सिद्धांतों को प्रयोग में लाना, व्यक्तिगत साइबर स्वच्छता अपनाना और साइबर सुरक्षा जागरूकता सबसे महत्वपूर्ण है।

संदर्भ ग्रंथ सूची :-

1. डॉक्टर एस. मार्सेलिन पुष्पा (2024) 'डिजिटल गवर्नेंस ट्रांसफॉर्मिंग पब्लिक सर्विस', आ. जी. पब्लिशिंग हाउस, भोपाल ,मध्य प्रदेश, भारत।
2. डॉक्टर टांगजैम कै सिंह(2024),'इंडिया साइबर सिक्योरिटी पॉलिसी', रुटलज ,न्यूयॉर्क।
3. डॉ. अवस्थी और अवस्थी (2014),भारतीय प्रशासन,लक्ष्मी नारायण अग्रवाल, आगरा।
4. डॉ. बी.एल. फादिया (2003), 'भारतीय प्रशासन',साहित्य भवन पब्लिकेशन, आगरा।
5. माइकल ई. मिलाकोविच (2012) 'डिजिटल गवर्नेंस', रुटलज, यू.के।
6. रघु संथानम और एम सेतु माधवन एवं मोहित वीरेंद्र (2011)'साइबर सिक्योरिटी साइबर क्राइम और साइबर फॉरेंसिक एप्लीकेशंस एंड पर्सपेक्टिव्स', इनफॉरमेशन साइंस रेफरेंस ,न्यूयॉर्क, अमेरिका।
7. योजना, अगस्त 2021
8. योजना नवंबर 2021
9. योजना नवंबर 2023
10. योजना फरवरी 2024
11. www.sanskritiias.com
12. www.livehindustan.com
13. http:/pib.gov.in/pressreleasepage

****