International Journal of Humanities and Social Science Research
www.socialsciencejournal.in
ISSN: 2455-2070
Received: 23-06-2026, Accepted: 24-07-2026, Published: 10-08-2026
Volume 12, Issue 3, 2026, Page No. 204-206

साइबर–सुरक्षा के आयाम

डॉ. संजेश कुमार
असिस्टेंट प्रोफेसर, सैन्य विज्ञान, रा. महाविद्यलय मजरा महादेव, पौड़ी गढ़वाल, उत्तराखण्ड, भारत
DOI: https://doi.org/10.66856/ijhssr.2026.12.3.12277

Abstract
वर्तमान डिजिटल एवं सूचना युग में प्रौद्योगिकी का उपयोग तीव्र गति से बढ़ रहा है जिसमें व्यक्तियों तथा सरकारो की कार्यप्रणालियों में सुविधाओं के साथ ही चुनौतियों का समना करना पड़ रहा है जैसे साइबर अपराध, डेटा चोरी हैकिंग रैनसमवेयर फिशिंग तथा पहचान की चोरी जैसी चुनौतियां तेजी से बढ़ी है। ऐसे परिदृश्य में सुरक्षा आर्थिक विकास प्रशासनिक सुशासन तथा सामाजिक विश्वास का महत्वपूर्ण आधार बन चुकी है। यह भोध पत्र साइबर सुरक्षा के विभिन्न आयामों का विश्लेशण करता है इसमें नेटवर्क सुरक्षा सूचना सुरक्षा क्लाउड सुरक्षा साइबर कानून कृत्रिम बुद्धिमत्ता आधारित साइबर सुरक्षा का अध्ययन किया गया है।

मुलशब्द: साइबर सुरक्षा, साइबर अपराध नेटवर्क सुरक्षा फिशिग कृत्रित बुद्धिमत्ता

21वीं सदी में साइबर स्पेस युद्ध कुटनीति,अर्थव्यवस्था और राश्ट्रीय सुरक्षा का एक महत्वपूर्ण क्षेत्र बन चुका है सरकारी संस्थानों रक्षा प्रतिश्ठानों,बैकिंग ऊर्जा संचार तथा महत्वपूर्ण संरचन साओं पर बढ़ते सादबर हमलों ने साइबर सुरक्षा को राश्ट्रीय सुरक्षा की गम्भीर चुनौतियां बना दिया है।

- साइबर सुरक्षा के आयाम–
- तकनीकि आयाम
- राश्ट्रीय सुरक्ष एव्र सामरिकि
- आर्थिक
- सामाजिक एवं मनोविज्ञान
- अन्तर्राट्रीय सहयोग एवं साइबर कूटनीति

साइबर या साइबर–स्पेस–तीव्र डिजिटाइजेशन के इस युग में व्यक्ति और राज्य दोनों की निर्भरता कंप्यूटर, सॉफ्टवेयर एवं इंटरनेट पर बढ़ती जा रही है। सूचना प्रौद्योगिकी के विकास ने इंटरनेट एवं सोशल मीडिया के उपयोग को और भी अधिक बढ़ावा दिया है। डिजिटल उपकरणों (कंप्यूटर, इंटरनेट, सॉफ्टवेयर आदि) के सम्मिलित रूप को ही साइबर या साइबर स्पेस कहते हैं।

साइबर–सुरक्षा–कंप्यूटर, सॉफ्टवेयर अथवा इंटरनेट पर की गई गतिविधियों को सूचना (Data) के रूप में जमा (Store) करके रखा जाता है। इन डाटा तथा उपकरणों की सुरक्षा ही साइबर सुरक्षा कहलाती है। इन्हें बचाने के लिए किए गए सुरक्षात्मक उपाय भी साइबर सुरक्षा के श्रेणी में आते हैं।

साइबर–अपराध–किसी भी कंप्यूटर, सॉफ्टवेयर, वेबसाइट अथवा इलेक्ट्रॉनिक उपकरणों को हैक करना अथवा डाटा चोरी करना साइबर–अपराध (Cyber-Crime) कहलाता है। साधारण शब्दों में ऐसा अपराध जिसमें कंप्यूटर का उपयोग किया गया हो साइबर–अपराध की श्रेणी में आता है।

चुनौतियां– क्योंकि सारी व्यवस्था आभासीय (Virtual) होती है इसलिए इसकी प्रकृति परंपरागत अपराध के मुकाबले और भी ज्यादा घातक होती है। इसमें अपराधी दुनिया के किसी भी कोने में बैठकर अपराध को अंजाम दे सकता है। उसे पकड़े जाने, घायल होने अथवा मारे जाने का भय नहीं होता। यह कार्य केवल एक पेशेवर व्यक्ति के द्वारा भी किया जा सकता है।

साइबर खतरे
कंप्यूटर और इंटरनेट मानव जीवन के प्रत्येक क्षेत्र में ऐसे समाया है कि इसके बिना जीवन की परिकल्पना भी नहीं की जा सकती। डिजिटल उपकरणों पर अत्यधिक निर्भरता ने साइबर खतरे को और भी अधिक व्यापक बना दिया है।

साइबर–अपराध के क्षेत्र अथवा प्रकार
डेनियल आफ सर्विस (DoS)– इसमें यूजर के कंप्यूटर पर सेवाओं को बाधित कर दिया जाता है।

मालवेयर (Malware)– इस प्रकार के सॉफ्टवेयर का प्रयोग उपभोगता (User) के कंप्यूटर संचालन को बाधित कर अवैध तरीके से सूचनाओं को इकट्ठा करने के लिए किया जाता है। कुछ मालवेयर निम्न होते हैं–

1. **कंप्यूटर–वायरस** (Computer VIRUS-Vital Information Resource Under Siege) यह एक ऐसा प्रोग्राम होता है जो यूजर के मुख्य सूचनाओं को क्षति पहुंचाता है। इस वायरस से संक्रमित कंप्यूटर में किसी अन्य डिवाइस को जोड़ने पर यह वायरस उसमें भी अपनी एक प्रतिलिपि बना देता है।

2. **ट्रोजन–हॉर्स** (Trojan-Horse)– ये प्रोग्राम ऐसे बनाए जाते हैं कि देखने में बेहद उपयोगी लगते हैं। इन्हें खासकर गेम, वेबसाइटों आदि पर लुभाने विज्ञापन के रूप में प्रदर्शित किया जाता है। यह प्रोग्राम यूजर के डाटा को इसे स्थापित करने वाले (इसके मालिक) के पास भेज देते हैं।

3. **स्पाइवेयर** (Spyware)– यह एक ऐसा प्रोग्राम है जो यूजर के द्वारा इंटरनेट पर किए गए कार्य एवं गोपनीय जानकारी को इसके मालिक के पास भेज देता है और युजर को पता भी नहीं चलता।

4. **की–लॉगर** (Key-Logger)– इस प्रोग्राम के द्वारा यूजर के की–बोर्ड को नियंत्रित किया जाता है । यूजर के द्वारा टाइप किए गए डाटा को यह, प्रोग्राम स्थापित करने वाले के पास भेज देता है।

5. **रैनसमवेयर** (Ransomeware)– यह प्रोग्राम उपभोगकर्ता के कंप्यूटर में प्रविष्ट होकर, उसके मुख्य फाइलों तक पहुंच को बाधित कर फिरौती (Ransome) के रूप में कुछ मांग करता है।

हैकिंग (Hacking)– दुर्भावना पूर्वक किसी यूज़र के कंप्यूटर नेटवर्क में अवैध तरीके से घुसकर कब्जा कर लेना हैकिंग कहलाता है। इस गतिविधि को करने वाले हैकर कहे जाते हैं। इनके भी दो प्रकार होते हैं –

1. **ब्लैक हैट हैकर–** यह यूजर के सिस्टम में वर्षों तक बिना पकड़े गए रह सकते हैं । यह डाटा चोरी के साथ उस सिस्टम में भी खराबी ला सकते हैं। इस श्रेणी में अनवांछित या आपराधिक गतिविधि करने वाले हैकर्स को क्रैकर कहते हैं।

2. **व्हाइट हैट हैकर–** इस कैटेगरी में प्रोगामर, डेवलपर, नेटवर्क–इंजीनियर, सॉफ्टवेयर–इंजीनियर और वेब पोर्टल के सुरक्षा सलाहकार सम्मिलित होते हैं। ये सुरक्षा कंपनियों द्वारा प्रोग्राम तथा सॉफ्टवेयरों की सुरक्षा जांच के लिए आधिकारिक रूप से नियुक्त किए जाते हैं।

इलेक्ट्रॉनिक स्पैमिंग (Electronic Spamming)– किसी इंटरनेट यूजर को वेबसाइट तथा ईमेल के माध्यम से अनवांछित सामग्रियां भेजना स्पैमिंग कहलाता है। इसका सर्वाधिक प्रचलित रूप स्पैम ईमेल–मैसेज है जो विज्ञापनों हेतु भेजे जाते हैं।

फिशिंग (Phishing)– यह जालसाजी का सबसे कुख्यात तरीका है । इसमें अपराधी उपयोगकर्ता को फर्जी ई–मेल या मैसेजेस के माध्यम से यूजर नेम, ओटीपी, पासवर्ड और बैंक–डिटेल की जानकारी जुटाने का प्रयास करते हैं ।

साइबर स्टॉकिंग–ऑनलाइन माध्यम से किसी व्यक्ति के साइबर प्रोफाइल पर नजर रखना साइबर स्टॉकिंग कहलाता है ।

साइबर आतंकवाद–जब किसी आतंकवादी संगठन द्वारा किसी देश में साइबर स्पेस के माध्यम से आतंकी गतिविधियों का संचालन किया जाता है, तो इसे साइबर आतंकवाद कहते हैं । यह किसी देश की आंतरिक सुरक्षा के सम्मुख सबसे बड़ा खतरा होता है ।

इसी तरह के कुछ अन्य प्रकार हैं– ई–मेल बांम्बिग, डाटा डिडलिंग, सलामी अटैक, मार्फिंग, लॉजिक–बम या स्लोगन कोड, चाइल्ड पोर्नोग्राफी, बूटनेट, ऑनलाइन गैंबलिंग, विशिंग (वॉइस फिशिंग) टैबनेबीग, जॉम्बीज, ड्राइव–बाई इत्यादि भी साइबर अपराध के अंतर्गत आते हैं ।

स्नोडेन का खुलासा–

एडवर्ड जोसेफ स्नोडेन अमेरिका के केंद्रीय खुफिया एजेंसी (CIA) का पूर्व कर्मचारी व राष्ट्रीय सुरक्षा एजेंसी (NSA) का तकनीकी ठेकेदार था। इसने हजारों की संख्या में खुफिया दस्तावेज अंतरराष्ट्रीय मीडिया के सामने लीक कर दिये थें। यह अमेरिकी इतिहास में अब तक का बहुत बड़ा सनसनी खेज खुलासा था। इन दस्तावेजों से यह ज्ञात हुआ कि अमेरिका, यूरोपीय देश और 5–Eyes (UK, USA, Canada, NZ, Austreli) भारत सहित दुनिया के 38 देशों की जासूसी कर रहे थें। NSA द्वारा लक्षित देशों में भारत का स्थान 5 वां था। स्नोडेन के खुलासे के परिणाम स्वरुप भारत सरकार की नींद खुली और फिर भारत ने महत्वपूर्ण प्रतिष्ठानों की बुनियादी ढांचे को सुदृढ़ बनाने की दिशा में कदम उठाए। दुनिया भर में निजता के अधिकार का मुद्दा जोर–शोर से उठा और विश्व में साइबर सुरक्षा के उपाय ढूँढने की होड़ मच गई। इसी के परिणाम स्वरूप माइक्रोसॉफ्ट ने ग्राहकों को अमेरिका के बाहर डाटा स्टोर करने की अनुमति दी।

भारत की स्थिति–

स्नोडेन के खुलासे के अनुसार भारत का साइबर स्पेस लगभग असुरक्षित है। बेहतर रणनीतिक तैयारी के अभाव में भारत डिजिटल घुसपैठ एवं साइबर अपराध के प्रति अधिक सुभेद्य है। सूचना प्रौद्योगिकी पर आधारित बैंकिंग, यातायात, स्वास्थ्य, ऊर्जा इत्यादि व्यवस्थाएं भी इन खतरों के प्रति संवेदनशील है। भारत विभिन्न प्रकार के कट्टरपंथी व उग्रवादी विचारधाराओं के समूह के निशाने पर है, उनका लक्ष्य भारत को अस्थिर करने का है। जिसके लिए वे सूचना प्रौद्योगिकी का उपयोग कर रहे हैं। कावेरी जल विवाद, जल्लीकट्टू, मुजफ्फरनगर दंगे, किसान आंदोलन, एनआरसी, कुडनकुलम न्यूक्लियर पावर प्लांट और कॉमनवेल्थ गेम्स के समय हुआ साइबर अटैक इसका प्रत्यक्ष उदाहरण है। दूसरी ओर चीन साइबर स्पेस में एक प्रबल विरोधी बनकर उभरा है। चीन ने साइबर क्षेत्र के महत्व को समझते हुए एक साइबर सेना खड़ी कर दी है। जो किसी भी संभावित खतरे से निपट सकने में सक्षम है और अन्य देशों पर भी जासुसी कार्यवाही करती है।

भारत द्वारा उठाए गए कदम –

स्नोडेन ने 21वीं सदी में साइबर स्पेस को युद्ध का उपयुक्त जगह बताया है। साइबर स्पेस के महत्व को समझते हुए भारत द्वारा इस क्षेत्र में प्रमुख कदम उठाए गए हैं–

- सन् 2000 में आईटी अधिनियम लाया गया जिसे बढ़ती आवश्यकताओं के कारण 2008 में संशोधित कर इसके अधिकार क्षेत्र को बढ़ा दिया गया।
- 2 जुलाई 2013 में राष्ट्रीय साइबर सुरक्षा नीति (National Cyber Security Policy) बनाई गई। इसी के तहत नेशनल क्रिटिकल इनफॉरमेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर (NCIIPC) का निर्माण किया गया।
- NASSCOM(National Association of Software and Service Companies) के साथ मिलकर बेंगलुरु, पुणे तथा कोलकाता में साइबर फॉरेंसिक लैब की स्थापना की गई है। ऐसी ही 9 और प्रयोगशालाओं की स्थापना का प्रयास सरकार के द्वारा किया जा रहा है।
- NCIIPC, 'राष्ट्रीय तकनीकी अनुसंधान संगठन' (NTRO) के अंतर्गत कार्य करता है। NTRO की स्थापना सन् 2004 में की गई थी। NTRO की धारा 70–। के तहत NCIIPC को भारत की समीक्षा सूचना संरक्षण के लिए नोडल एजेंसी बनाया गया है।
- NTRO में नेशनल इंस्टीट्यूट आफ क्रिप्टोलॉजी रिसर्च एंड डेवलपमेंट (NICRD) भी शामिल है।
- साइबर हमलों से निपटने के लिए नोडल एजेंसी CERT-IN(Computer Emergency Response Team & India) है जिसकी स्थापना भी सन् 2004 में की गई थी।
- पर्सनल डाटा सिक्योरिटी बिल सन् 2018 में लाया गया।
- नेशनल डिजिटल कम्युनिकेशन प्रोग्राम 2018 में लाया गया।
- साइबर सुरक्षित भारत अभियान 19 जनवरी 2018 से चलाया जा रहा है ।
- राष्ट्रीय साइबर सहयोग केंद्र (NCCC) हैकिंग, जासूसी तथा ऑनलाइन आतंकवादी गतिविधियों का पता लगाने तथा रोकने का प्रयास करता है।
- साइबर डोम परियोजना साइबर अपराध से निपटने में कर्नाटक पुलिस के द्वारा उठाया गया एक सराहनीय कदम है, इसे राष्ट्रीय स्तर पर लागू किया जाना चाहिए।
- सरकारी भवनों में अब नेटवर्किंग उपकरण IPV6 का प्रयोग किया जा रहा है।

साइबर सुरक्षा के क्षेत्र में अंतरराष्ट्रीय सहयोग

साइबर अपराध का क्षेत्र वैश्विक होता है इसके माध्यम से दुनिया के सबसे मजबूत नेटवर्क सिस्टम को भी हैकर अपना निशाना बनाने से नहीं चूकते । इससे विकसित देश भी परेशान हैं इसलिए अंतर्राष्ट्रीय स्तर पर साइबर क्राइम से निपटने के लिए ये सभी देश सहमत हुए और इस क्षेत्र में मिलकर महत्वपूर्ण कदम भी उठाए जो निम्न है–

- जुलाई 2001 में बुडापेस्ट में अवांछित साइबर गतिविधियों को रोकने हेतु एक सम्मेलन का आयोजन किया गया। इस सम्मेलन का उद्देश्य अंतरराष्ट्रीय सहयोग को बढ़ावा देने के साथ ही एक अंतर्राष्ट्रीय नीति का निर्माण भी करना था।
- साइबर स्पेस पर ग्लोबल कॉन्फ्रेंस 2011 की शुरुआत हुई । इस बैठक को प्रत्येक दो वर्ष पर आयोजित किया जाता है। भारत ने 2017 में इसकी मेजबानी की थी।
- नेट विश्व सम्मेलन– अप्रैल 2014 में नेट गवर्नेंस पर दो दिवसीय सम्मेलन ब्राजील में आयोजित किया गया था। जिसका विषय था– 'शासन के भविष्य पर वैश्विक बहुहित धारी बैठक'
- राष्ट्रमंडल शिखर सम्मेलन 2018 का साइबर घोषणा पत्र
- विश्व आर्थिक मंच द्वारा साइबर सुरक्षा पर वैश्विक केंद्र की स्थापना

वर्तमान घटनाक्रम

- 6 सितंबर 2023 को CERT-IN के द्वारा साइबर जागरूकता दिवस मनाया गया।
- डप्ज रिव्यू 2023– साइबर डिफेंस में भारत को 20 में से 17 वां स्थान दिया गया। पहला स्थान ऑस्ट्रेलिया का था।
- साइबर स्पेस संबंधी चुनौतियों से निपटने के लिए सेना "कमांड साइबर ऑपरेशन एंड सपोर्ट विंग" (CCOSW) को संचालित करने जा रही है। CCOSW शत्रुओं की प्रबल होती युद्धक क्षमताओं से उत्पन्न साइबर सुरक्षा संबंधी खतरों से निपटने में सेना की सहायता करेगा।
- 21वीं सदी की साइबर सुरक्षा और साइबर अपराध की चुनौतियों से निपटने के लिए अखिल भारतीय तकनीकी शिक्षा परिषद (AICTE), पुलिस अनुसंधान और विकास ब्यूरो (BPR&D) तथा भारतीय साइबर अपराध समन्वय केंद्र (I4C) ने संयुक्त रूप से कवच–2023 लांच किया है। कवच एक राष्ट्रीय स्तर का है थकान है जिसे दो चरणों में आयोजित किया गया। पहला चरण शिक्षण संस्थान तथा औद्योगिक क्षेत्र व दूसरा चरण भारतीय सेना द्वारा सैन्य रण क्षेत्रम् 2.0 के नाम से आयोजित किया गया।

सुझाव

1. देश में डाटा के स्थानीयकरण डिजिटल संप्रभुता और इंटरनेट गवर्नेंस को बढ़ावा देना चाहिए।
2. देश में पर्याप्त साइबर सुरक्षा प्रोफेशनल्स (2020 की स्थिति के अनुसार 10 लाख से अधिक) की नियुक्ति की जानी चाहिए।
3. साइबर खतरों को कम करने के लिए प्रिडिक्शन, प्रिवेंशन, रिस्पांस तथा डिटेक्शन प्रक्रिया को अपनाया जाना चाहिए।
4. इस क्षेत्र में निवेश और R&D को बढ़ावा देना चाहिए।
5. एक एकीकृत साइबर कमांड की स्थापना की जानी चाहिए।
6. युरोपियन यूनियन (EU) के General Data Protection Regulation और अमेरिका के Cloud Act की तरह भारत में भी डाटा सुरक्षा के लिए कदम उठाए जाने चाहिए।

निष्कर्ष

बदलते वैश्विक परिवेश में जैसे–जैसे भारत डिजिटलाइजेशन के तरफ बढ़ता जा रहा है वैसे–वैसे साइबर अपराध का जोखिम भी बढ़ता जा रहा है। साइबर जागरूकता का राष्ट्रीय स्तर पर क्रियान्वयन के साथ ही नीतिगत निवेश और R&D पर भी भारत को ध्यान देने की आवश्यकता है। जिससे भारत साइबर सुरक्षा के क्षेत्र में मजबूत स्थिति को प्राप्त कर सके।

संदर्भ ग्रंथ –

1. आंतरिक सुरक्षा एवं आपदा प्रबंधन– डॉ. टी.सी. डामोर (Kiran Prakashan)
2. भारत की आंतरिक सुरक्षा मुख्य चुनौतियां– अशोक कुमार, विपुल,IPS Danips (Mc Grow Hill) India's national security in the 21st century-Adhikari Sanjeev (Pentagon Press)
3. Newspaper-The Hindu, Economic Times India Times, BBC India.
4. Current Affairs Magazine- Vision IAS, Drishti IAS.
5. Related website- Wikipedia, www.aicte-india.org/cybersecurity