

डिजिटल युग में साइबर सुरक्षा एवं राष्ट्रीय सुरक्षा

डॉ. दलीप कुमार

सहायक प्रोफेसर (राजनीति विज्ञान)
राजकीय डिग्री कॉलेज, गंगेश्वरी, अमरोहा- 244255

सारांश (Abstract)

डिजिटल प्रौद्योगिकी के तीव्र विस्तार ने शासन, अर्थव्यवस्था, वित्तीय सेवाओं, रक्षा, संचार और नागरिक जीवन को व्यापक रूप से प्रभावित किया है। इसके साथ ही साइबर अपराध, डेटा उल्लंघन, रैनसमवेयर, फिशिंग, साइबर जासूसी तथा महत्वपूर्ण सूचना अवसंरचना पर संभावित हमलों जैसी चुनौतियाँ भी बढ़ी हैं। प्रस्तुत अध्ययन “डिजिटल युग में साइबर सुरक्षा एवं राष्ट्रीय सुरक्षा” का उद्देश्य साइबर सुरक्षा और राष्ट्रीय सुरक्षा के बीच संबंध का विश्लेषण करना है। अध्ययन में साइबर जागरूकता, डिजिटल साक्षरता, साइबर सुरक्षा प्रशिक्षण, तकनीकी क्षमता, संस्थागत तैयारी, डेटा सुरक्षा और राष्ट्रीय सुरक्षा की धारणा जैसे विभिन्न आयामों को सम्मिलित किया गया है। अध्ययन वर्णनात्मक एवं विश्लेषणात्मक शोध पद्धति पर आधारित है तथा प्राथमिक एवं द्वितीयक दोनों स्रोतों के उपयोग की रूपरेखा प्रस्तुत करता है। उदाहरणात्मक सांख्यिकीय विश्लेषण में आवृत्ति, प्रतिशत, माध्य, मानक विचलन और सहसंबंध जैसे उपकरणों का उपयोग किया गया है। विश्लेषण से यह समझने का प्रयास किया गया है कि साइबर सुरक्षा केवल तकनीकी अवसंरचना की सुरक्षा तक सीमित नहीं है, बल्कि मानव जागरूकता, संस्थागत क्षमता, incident response और नीति-निर्माण से भी संबंधित है। भारतीय संदर्भ में CERT-In, NCIIIPC, NCCC और National Cyber Security Coordinator जैसी संस्थागत व्यवस्थाएँ साइबर सुरक्षा प्रतिक्रिया और समन्वय में महत्वपूर्ण भूमिका निभाती हैं। साथ ही, Digital Personal Data Protection Act, 2023 ने डिजिटल व्यक्तिगत डेटा के संरक्षण के लिए एक महत्वपूर्ण कानूनी आधार प्रदान किया है। अध्ययन निष्कर्षतः साइबर सुरक्षा को राष्ट्रीय सुरक्षा, आर्थिक स्थिरता, सार्वजनिक सेवाओं और डिजिटल विश्वास के साथ एकीकृत रूप में समझने की आवश्यकता पर बल देता है।

प्रमुख शब्द (Keywords)-साइबर सुरक्षा, राष्ट्रीय सुरक्षा, डिजिटल युग, साइबर अपराध, डिजिटल साक्षरता, महत्वपूर्ण सूचना अवसंरचना, साइबर जागरूकता

1. परिचय

21वीं सदी में डिजिटल प्रौद्योगिकी ने शासन, अर्थव्यवस्था, शिक्षा, स्वास्थ्य, संचार, वित्तीय सेवाओं और रक्षा व्यवस्था को व्यापक रूप से प्रभावित किया है। इंटरनेट, क्लाउड कंप्यूटिंग, कृत्रिम बुद्धिमत्ता, इंटरनेट ऑफ थिंग्स (IoT), बिग डेटा और डिजिटल भुगतान जैसी तकनीकों ने सेवाओं को अधिक तेज, सुलभ और परस्पर जुड़ा बनाया है। इसके साथ ही डिजिटल निर्भरता में वृद्धि ने साइबर अपराध, डेटा चोरी, रैनसमवेयर, फिशिंग, पहचान की चोरी, साइबर जासूसी तथा महत्वपूर्ण सूचना अवसंरचना पर हमलों जैसी नई सुरक्षा चुनौतियों को भी जन्म दिया है। इस प्रकार डिजिटल युग में **साइबर सुरक्षा केवल तकनीकी विषय नहीं, बल्कि राष्ट्रीय सुरक्षा का महत्वपूर्ण आयाम** बन गई है। राष्ट्रीय सुरक्षा की पारंपरिक अवधारणा मुख्यतः भौगोलिक सीमाओं, सैन्य शक्ति और प्रत्यक्ष भौतिक खतरों से जुड़ी रही है। डिजिटल परिवर्तन ने इस अवधारणा का विस्तार कर दिया है। आज किसी देश की सुरक्षा केवल उसकी सीमाओं की रक्षा पर निर्भर नहीं करती, बल्कि उसके ऊर्जा तंत्र, बैंकिंग प्रणाली, दूरसंचार नेटवर्क, परिवहन व्यवस्था, सरकारी डेटाबेस और डिजिटल संचार प्रणालियों की सुरक्षा पर भी निर्भर करती है। किसी महत्वपूर्ण डिजिटल प्रणाली पर गंभीर साइबर हमला आर्थिक गतिविधियों, सार्वजनिक सेवाओं और प्रशासनिक कार्यों को प्रभावित कर सकता है। भारत में डिजिटल परिवर्तन ने साइबर सुरक्षा के महत्व को और बढ़ाया है। डिजिटल इंडिया, ऑनलाइन सरकारी सेवाओं, डिजिटल भुगतान, आधार-आधारित सेवाओं और बढ़ती इंटरनेट पहुँच के

कारण नागरिकों और संस्थाओं की डिजिटल प्रणालियों पर निर्भरता बढ़ी है। परिणामस्वरूप व्यक्तिगत डेटा की सुरक्षा के साथ-साथ सरकारी संस्थानों और महत्वपूर्ण डिजिटल अवसंरचना की सुरक्षा भी राष्ट्रीय प्राथमिकता का विषय बन गई है।

1.1 साइबर सुरक्षा की अवधारणा

साइबर सुरक्षा से आशय कंप्यूटर प्रणालियों, नेटवर्क, डिजिटल उपकरणों, सॉफ्टवेयर और डेटा को अनधिकृत पहुँच, दुरुपयोग, क्षति, व्यवधान तथा साइबर हमलों से सुरक्षित रखने की प्रक्रियाओं और उपायों से है। इसमें तकनीकी सुरक्षा के साथ-साथ संस्थागत नीतियाँ, मानव संसाधन, जागरूकता, जोखिम प्रबंधन, घटना-प्रतिक्रिया और कानूनी ढाँचा भी शामिल हैं। साइबर सुरक्षा का मूल उद्देश्य सूचना की **गोपनीयता (Confidentiality)**, **अखंडता (Integrity)** और **उपलब्धता (Availability)** बनाए रखना है। राष्ट्रीय सुरक्षा के संदर्भ में इसके अतिरिक्त महत्वपूर्ण सूचना अवसंरचना की निरंतरता, रणनीतिक सूचनाओं की सुरक्षा तथा साइबर घटनाओं के प्रति संस्थागत प्रतिक्रिया क्षमता भी महत्वपूर्ण है।

1.2 साइबर खतरे और राष्ट्रीय सुरक्षा

डिजिटल युग में साइबर खतरे अनेक रूपों में सामने आ सकते हैं। साइबर अपराधी वित्तीय लाभ के लिए प्रणालियों को निशाना बना सकते हैं, जबकि संगठित समूह या राज्य-समर्थित साइबर गतिविधियाँ जासूसी, सूचना प्राप्त करने या महत्वपूर्ण प्रणालियों को बाधित करने से संबंधित हो सकती हैं। रैनसमवेयर, मैलवेयर, फिशिंग, DDoS हमले, डेटा उल्लंघन और सोशल इंजीनियरिंग इसके प्रमुख उदाहरण हैं। राष्ट्रीय सुरक्षा के दृष्टिकोण से महत्वपूर्ण चुनौती यह है कि साइबर हमले भौगोलिक सीमाओं से स्वतंत्र हो सकते हैं। हमलावर और प्रभावित प्रणाली अलग-अलग देशों में स्थित हो सकते हैं, जिससे पहचान, attribution और अंतरराष्ट्रीय सहयोग जटिल हो जाता है। इसलिए साइबर सुरक्षा में तकनीकी क्षमता के साथ अंतरराष्ट्रीय सहयोग और संस्थागत समन्वय भी आवश्यक है।

1.3 भारत में साइबर सुरक्षा का संस्थागत परिदृश्य

भारत में साइबर सुरक्षा से संबंधित संस्थागत व्यवस्था में **Indian Computer Emergency Response Team (CERT-In)** की महत्वपूर्ण भूमिका है। CERT-In साइबर सुरक्षा घटनाओं के संबंध में चेतावनी, प्रतिक्रिया और समन्वय से संबंधित कार्य करता है। इसके अलावा राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना की सुरक्षा के लिए **National Critical Information Infrastructure Protection Centre (NCIIPC)** जैसी संस्थागत व्यवस्था भी विकसित की गई है। भारत का **Information Technology Act, 2000** साइबर अपराध और इलेक्ट्रॉनिक लेन-देन से संबंधित महत्वपूर्ण कानूनी आधार प्रदान करता है। हाल के वर्षों में डेटा संरक्षण और डिजिटल व्यक्तिगत डेटा से संबंधित कानूनी व्यवस्था भी विकसित हुई है। इससे स्पष्ट होता है कि साइबर सुरक्षा का क्षेत्र तकनीकी उपायों के साथ कानूनी और नीतिगत उपायों से भी जुड़ा हुआ है।

1.4 साइबर सुरक्षा और महत्वपूर्ण सूचना अवसंरचना

बैंकिंग, ऊर्जा, दूरसंचार, परिवहन, स्वास्थ्य और सरकारी सेवाएँ डिजिटल प्रणालियों पर बढ़ती मात्रा में निर्भर हैं। इन क्षेत्रों में साइबर व्यवधान का प्रभाव केवल किसी एक संगठन तक सीमित नहीं रह सकता। उदाहरण के लिए, वित्तीय नेटवर्क में व्यवधान आर्थिक गतिविधियों को प्रभावित कर सकता है, जबकि ऊर्जा या दूरसंचार प्रणालियों पर गंभीर हमला आवश्यक सेवाओं की निरंतरता को प्रभावित कर सकता है। इसलिए राष्ट्रीय सुरक्षा के लिए महत्वपूर्ण सूचना अवसंरचना की पहचान, जोखिम मूल्यांकन, सुरक्षा परीक्षण, निगरानी, बैकअप व्यवस्था और त्वरित incident response महत्वपूर्ण हैं।

1.5 मानव तत्व और साइबर जागरूकता

साइबर सुरक्षा केवल उन्नत तकनीकी उपकरणों पर निर्भर नहीं है। मानव त्रुटि, कमजोर पासवर्ड, संदिग्ध लिंक पर क्लिक करना, फर्जी ई-मेल पर प्रतिक्रिया देना तथा संवेदनशील जानकारी साझा करना साइबर जोखिमों को बढ़ा सकता है। इसलिए नागरिकों, सरकारी कर्मचारियों, विद्यार्थियों, व्यवसायों और संस्थागत कर्मचारियों में साइबर जागरूकता विकसित करना

आवश्यक है। साइबर सुरक्षा के संदर्भ में “मानव तत्व” विशेष महत्व रखता है क्योंकि अत्यधिक सुरक्षित तकनीकी प्रणाली भी गलत उपयोग या सामाजिक इंजीनियरिंग के माध्यम से प्रभावित हो सकती है। अतः साइबर सुरक्षा रणनीति में तकनीकी प्रशिक्षण के साथ डिजिटल साक्षरता और सुरक्षा व्यवहार को भी शामिल किया जाना चाहिए।

1.6 अध्ययन की प्रासंगिकता

डिजिटल अर्थव्यवस्था और ई-गवर्नेंस के विस्तार के साथ भारत की डिजिटल निर्भरता लगातार बढ़ रही है। ऐसे में साइबर सुरक्षा को केवल सूचना-प्रौद्योगिकी विभाग का विषय मानने के बजाय राष्ट्रीय सुरक्षा, आर्थिक स्थिरता, सार्वजनिक प्रशासन और नागरिक अधिकारों के व्यापक संदर्भ में समझना आवश्यक है। यह अध्ययन डिजिटल युग में साइबर सुरक्षा और राष्ट्रीय सुरक्षा के बीच संबंधों, प्रमुख साइबर खतरों, संस्थागत चुनौतियों, मानव संसाधन एवं जागरूकता की भूमिका तथा भारत के साइबर सुरक्षा ढाँचे की आवश्यकता को समझने का प्रयास करता है।

2. अनुसंधान प्रश्न- डिजिटल युग में साइबर सुरक्षा किस प्रकार भारत की राष्ट्रीय सुरक्षा को प्रभावित करती है तथा साइबर खतरों से निपटने के लिए तकनीकी, संस्थागत और नीतिगत उपायों की क्या भूमिका है?

3. अनुसंधान परिकल्पनाएँ

परिकल्पना 1-H₁: साइबर सुरक्षा जागरूकता और राष्ट्रीय साइबर सुरक्षा के प्रति नागरिकों एवं संस्थाओं की तैयारी के बीच महत्वपूर्ण सकारात्मक संबंध है।

परिकल्पना 2-H₂: तकनीकी सुरक्षा क्षमता में वृद्धि साइबर खतरों के प्रति संस्थागत प्रतिरोधक क्षमता को महत्वपूर्ण रूप से प्रभावित करती है।

परिकल्पना 3-H₃: प्रभावी साइबर सुरक्षा नीतियाँ, संस्थागत समन्वय और साइबर सुरक्षा प्रशिक्षण राष्ट्रीय सुरक्षा को मजबूत करने में महत्वपूर्ण भूमिका निभाते हैं।

4. अध्ययन का महत्व (Significance of the Study)

यह अध्ययन डिजिटल परिवर्तन और राष्ट्रीय सुरक्षा के बीच संबंध को समझने की दृष्टि से महत्वपूर्ण है। डिजिटल सेवाओं के विस्तार ने नागरिकों, सरकार और व्यवसायों को अनेक सुविधाएँ प्रदान की हैं, लेकिन इसी के साथ साइबर जोखिमों का विस्तार भी हुआ है। इसलिए साइबर सुरक्षा को राष्ट्रीय सुरक्षा के व्यापक ढाँचे में समझना आवश्यक है। अध्ययन नीति-निर्माताओं को साइबर सुरक्षा से संबंधित तकनीकी और संस्थागत आवश्यकताओं को समझने में सहायता कर सकता है। यह सरकारी संस्थाओं, शैक्षणिक संस्थानों, निजी संगठनों तथा नागरिकों के लिए साइबर जागरूकता और सुरक्षा प्रशिक्षण के महत्व को स्पष्ट करने में भी उपयोगी हो सकता है। इसके अतिरिक्त, अध्ययन यह समझने में योगदान देगा कि साइबर सुरक्षा केवल डेटा या कंप्यूटर नेटवर्क की सुरक्षा नहीं है, बल्कि आर्थिक स्थिरता, सार्वजनिक सेवाओं, महत्वपूर्ण अवसंरचना और प्रशासनिक निरंतरता से भी जुड़ी हुई है।

5. अनुसंधान की आवश्यकता (Need of the Study)

डिजिटल तकनीकों के तीव्र विस्तार ने भारत में इंटरनेट, डिजिटल भुगतान, ई-गवर्नेंस और ऑनलाइन सेवाओं का व्यापक उपयोग संभव बनाया है। इसके परिणामस्वरूप व्यक्तिगत, संस्थागत और राष्ट्रीय स्तर पर डिजिटल प्रणालियों पर निर्भरता बढ़ी है। इस बढ़ती निर्भरता के कारण साइबर हमलों से होने वाले संभावित व्यवधानों को समझना आवश्यक हो गया है। साइबर अपराधों की प्रकृति भी लगातार बदल रही है। पारंपरिक साइबर अपराधों के साथ रैनसमवेयर, डेटा उल्लंघन, सामाजिक इंजीनियरिंग, कृत्रिम बुद्धिमत्ता-सहायित धोखाधड़ी तथा महत्वपूर्ण सूचना अवसंरचना को लक्षित करने वाले हमले नई चुनौतियाँ प्रस्तुत करते हैं। इसलिए केवल तकनीकी सुरक्षा उपाय पर्याप्त नहीं हैं; कानूनी व्यवस्था, संस्थागत समन्वय,

प्रशिक्षित मानव संसाधन और साइबर जागरूकता को भी समान महत्व देना आवश्यक है। इस अध्ययन की आवश्यकता इसलिए भी है क्योंकि साइबर सुरक्षा और राष्ट्रीय सुरक्षा के बीच संबंध बहुआयामी है। साइबर घटना का प्रभाव आर्थिक, सामाजिक, प्रशासनिक और रणनीतिक स्तर पर दिखाई दे सकता है। अतः भारतीय संदर्भ में साइबर सुरक्षा की चुनौतियों और राष्ट्रीय सुरक्षा पर उनके संभावित प्रभाव का समग्र अध्ययन आवश्यक है।

6. शोध-अंतराल (Research Gap)

उपलब्ध साहित्य में साइबर अपराध, सूचना सुरक्षा, डेटा संरक्षण और डिजिटल सुरक्षा पर पर्याप्त चर्चा मिलती है। इसी प्रकार राष्ट्रीय सुरक्षा पर भी व्यापक साहित्य उपलब्ध है। लेकिन **साइबर सुरक्षा, राष्ट्रीय सुरक्षा, महत्वपूर्ण सूचना अवसंरचना, संस्थागत क्षमता और मानव साइबर जागरूकता** को एकीकृत ढाँचे में देखने वाले अध्ययनों की आवश्यकता बनी हुई है। विशेष रूप से डिजिटल शासन और डिजिटल अर्थव्यवस्था के विस्तार के संदर्भ में यह अध्ययन आवश्यक है कि तकनीकी सुरक्षा उपायों के साथ संस्थागत तैयारी, मानव व्यवहार, प्रशिक्षण और नीतिगत समन्वय राष्ट्रीय साइबर सुरक्षा को किस प्रकार प्रभावित करते हैं। इसके अतिरिक्त, साइबर सुरक्षा को केवल तकनीकी समस्या मानने के बजाय इसे **राष्ट्रीय सुरक्षा, आर्थिक स्थिरता और नागरिक डिजिटल अधिकारों** के संयुक्त परिप्रेक्ष्य में देखने की आवश्यकता है। प्रस्तुत अध्ययन इसी व्यापक शोध-अंतराल को संबोधित करने का प्रयास करता है।

2. साहित्य समीक्षा (Review of Literature)

डिजिटल युग में साइबर सुरक्षा और राष्ट्रीय सुरक्षा पर उपलब्ध साहित्य यह दर्शाता है कि साइबर स्पेस आधुनिक राज्य व्यवस्था, अंतरराष्ट्रीय राजनीति और रणनीतिक सुरक्षा का महत्वपूर्ण क्षेत्र बन चुका है। प्रारंभिक अध्ययनों में साइबर सुरक्षा को मुख्यतः कंप्यूटर नेटवर्क और सूचना प्रणालियों की सुरक्षा के रूप में देखा गया, लेकिन बाद के शोधों ने इसे राष्ट्रीय शक्ति, आर्थिक सुरक्षा, रक्षा, शासन और अंतरराष्ट्रीय संबंधों से जोड़कर देखा। Rid (2012) ने साइबर युद्ध की अवधारणा का विश्लेषण करते हुए साइबर गतिविधियों और पारंपरिक युद्ध के संबंध पर प्रश्न उठाया। उनके अध्ययन ने यह बहस आगे बढ़ाई कि प्रत्येक साइबर हमला पारंपरिक अर्थों में युद्ध का रूप नहीं लेता। इसके विपरीत, Kello (2017) ने साइबर गतिविधियों को अंतरराष्ट्रीय व्यवस्था के लिए व्यापक रणनीतिक चुनौती के रूप में देखा और बताया कि साइबर स्पेस ने राज्यों की शक्ति और सुरक्षा के स्वरूप को बदल दिया है। Nye (2017) ने साइबर स्पेस में deterrence और dissuasion की अवधारणाओं का अध्ययन किया तथा यह स्पष्ट किया कि साइबर क्षेत्र में पारंपरिक प्रतिरोध रणनीतियों को लागू करना जटिल हो सकता है। Rid और Buchanan (2015) ने साइबर हमलों के attribution की समस्या पर चर्चा करते हुए यह दिखाया कि हमले के पीछे वास्तविक अभिनेता की पहचान करना अक्सर कठिन होता है। यह समस्या राष्ट्रीय सुरक्षा नीति और अंतरराष्ट्रीय प्रतिक्रिया को प्रभावित कर सकती है। Buchanan (2017) ने "cybersecurity dilemma" की अवधारणा के माध्यम से बताया कि एक राज्य द्वारा अपनी साइबर क्षमता बढ़ाने के प्रयास दूसरे राज्यों द्वारा संभावित खतरे के रूप में देखे जा सकते हैं। उन्होंने baseline defenses, bilateral cooperation और international security mechanisms को जोखिम कम करने के संभावित उपायों के रूप में चर्चा की। बाद में Buchanan (2020) ने साइबर हमलों को आधुनिक geopolitics के संदर्भ में देखा और बैंकिंग, स्वास्थ्य, तकनीकी प्रणालियों तथा लोकतांत्रिक संस्थाओं पर साइबर गतिविधियों के व्यापक प्रभावों की चर्चा की। Hansen और Nissenbaum (2009) ने साइबर सुरक्षा को securitization के दृष्टिकोण से देखा और बताया कि डिजिटल खतरों की सामाजिक एवं राजनीतिक व्याख्या भी सुरक्षा नीति को प्रभावित करती है। इसी प्रकार Gartzke और Lindsay (2015) ने साइबर क्षेत्र में offense, defense और deception के संबंध का विश्लेषण किया। इन अध्ययनों से स्पष्ट होता है कि साइबर सुरक्षा को केवल तकनीकी समस्या के रूप में समझना पर्याप्त नहीं है। भारतीय संदर्भ में साइबर सुरक्षा का महत्व डिजिटल शासन, डिजिटल भुगतान और महत्वपूर्ण सूचना अवसंरचना के विस्तार के साथ बढ़ा है। भारत में CERT-In को साइबर सुरक्षा घटनाओं के लिए राष्ट्रीय एजेंसी तथा NCIIIPC को महत्वपूर्ण सूचना अवसंरचना की सुरक्षा के लिए संस्थागत व्यवस्था के रूप में स्थापित किया गया है। सरकारी स्रोतों के अनुसार National Cyber Coordination Centre तथा National Cyber Security Coordinator भी विभिन्न एजेंसियों के बीच साइबर सुरक्षा समन्वय में भूमिका निभाते हैं। NIC-CERT भी सरकारी सूचना प्रणालियों के लिए cyber incident response और threat intelligence में कार्य करता है। डेटा संरक्षण भी साइबर सुरक्षा का महत्वपूर्ण आयाम बन गया है। Digital Personal Data Protection Act, 2023 डिजिटल व्यक्तिगत डेटा के प्रसंस्करण और व्यक्तिगत डेटा की सुरक्षा से संबंधित कानूनी ढाँचा

प्रदान करता है। इससे साइबर सुरक्षा का संबंध नागरिक अधिकारों और डिजिटल विश्वास से भी स्थापित होता है। समग्र साहित्य से यह स्पष्ट होता है कि साइबर सुरक्षा पर तकनीकी और रणनीतिक अध्ययन पर्याप्त हैं, लेकिन **साइबर जागरूकता, डिजिटल साक्षरता, प्रशिक्षण, तकनीकी क्षमता, संस्थागत तैयारी और राष्ट्रीय सुरक्षा धारणा को एकीकृत अनुभवजन्य मॉडल में देखने की आवश्यकता बनी हुई है**। प्रस्तुत अध्ययन इसी शोध-अंतराल को संबोधित करने का प्रयास करता है।

3. अनुसंधान पद्धति (Research Methodology)

प्रस्तुत अध्ययन **वर्णनात्मक एवं विश्लेषणात्मक अनुसंधान डिजाइन** पर आधारित है। इसका उद्देश्य डिजिटल युग में साइबर सुरक्षा और राष्ट्रीय सुरक्षा के बीच संबंधों का व्यवस्थित अध्ययन करना है। अध्ययन में साइबर जागरूकता, डिजिटल साक्षरता, साइबर सुरक्षा प्रशिक्षण, तकनीकी क्षमता, संस्थागत तैयारी, डेटा सुरक्षा और राष्ट्रीय सुरक्षा की धारणा को प्रमुख अध्ययन चर के रूप में लिया गया है। प्राथमिक आँकड़ों के लिए संरचित प्रश्नावली का उपयोग किया जा सकता है, जिसमें उत्तरदाताओं की आयु, लिंग, शैक्षिक योग्यता, निवास क्षेत्र, इंटरनेट उपयोग, डिजिटल भुगतान, साइबर प्रशिक्षण और साइबर सुरक्षा व्यवहार से संबंधित प्रश्न शामिल होंगे। साइबर खतरे के संदर्भ में फिशिंग, मैलवेयर, रैनसमवेयर, सोशल इंजीनियरिंग, डेटा चोरी, पासवर्ड सुरक्षा, दो-स्तरीय प्रमाणीकरण और साइबर अपराध रिपोर्टिंग जैसे अनेक संकेतकों को शामिल किया जाएगा। उत्तरदाताओं की धारणाओं को पाँच-बिंदु Likert Scale पर मापा जा सकता है, जिसमें 1 = पूर्णतः असहमत तथा 5 = पूर्णतः सहमत होगा। नमूना चयन के लिए purposive तथा stratified sampling का उपयोग किया जा सकता है। द्वितीयक आँकड़े CERT-In, NCIIPC, भारत सरकार, NIC, कानूनी दस्तावेजों, शोध-पत्रों, पुस्तकों और अंतरराष्ट्रीय साइबर सुरक्षा frameworks से प्राप्त किए जा सकते हैं। भारत में CERT-In, NCIIPC और अन्य संस्थागत व्यवस्थाएँ साइबर incident response तथा critical information infrastructure protection से संबंधित महत्वपूर्ण भूमिकाएँ निभाती हैं। सांख्यिकीय विश्लेषण में **frequency, percentage, mean, standard deviation, Pearson correlation, chi-square, ANOVA तथा multiple regression** का उपयोग किया जा सकता है। Cronbach's Alpha द्वारा प्रश्नावली की आंतरिक विश्वसनीयता जाँची जा सकती है। Correlation analysis के माध्यम से साइबर जागरूकता, प्रशिक्षण, तकनीकी क्षमता और संस्थागत तैयारी के बीच संबंधों का अध्ययन किया जाएगा, जबकि regression analysis यह निर्धारित करने में सहायक होगा कि कौन-से कारक राष्ट्रीय सुरक्षा की धारणा से अधिक संबंधित हैं। प्रस्तुत तालिकाओं में दिए गए आँकड़े **सिमुलेटेड/उदाहरणात्मक** हैं और वास्तविक क्षेत्रीय डेटा का विकल्प नहीं हैं।

सांख्यिकीय विश्लेषण

तालिका 1: उत्तरदाताओं की सामाजिक-जनसांख्यिकीय एवं डिजिटल पृष्ठभूमि का विस्तृत वितरण

पैरामीटर	श्रेणी	आवृत्ति	प्रतिशत (%)
आयु	18-25 वर्ष	68	22.67
	26-35 वर्ष	86	28.67
	36-45 वर्ष	64	21.33
	46-55 वर्ष	48	16.00
	56 वर्ष से अधिक	34	11.33
लिंग	पुरुष	164	54.67
	महिला	136	45.33
शिक्षा	माध्यमिक तक	38	12.67
	उच्च माध्यमिक	57	19.00
	स्नातक	103	34.33
	स्नातकोत्तर	72	24.00
	व्यावसायिक/तकनीकी	30	10.00
निवास	ग्रामीण	118	39.33
	अर्ध-शहरी	74	24.67

	शहरी	108	36.00
इंटरनेट उपयोग	प्रतिदिन 1 घंटे से कम	36	12.00
	1-3 घंटे	91	30.33
	3-5 घंटे	103	34.33
	5 घंटे से अधिक	70	23.33
डिजिटल भुगतान का उपयोग	कभी नहीं	29	9.67
	कभी-कभी	74	24.67
	नियमित	197	65.67
साइबर सुरक्षा प्रशिक्षण	प्राप्त नहीं	161	53.67
	एक बार	82	27.33
	नियमित	57	19.00
डिजिटल साक्षरता	निम्न	47	15.67
	मध्यम	156	52.00
	उच्च	97	32.33

तालिका 1 में 300 उदाहरणात्मक उत्तरदाताओं की सामाजिक-जनसांख्यिकीय तथा डिजिटल पृष्ठभूमि प्रस्तुत की गई है। आयु-वर्ग के आधार पर 26-35 वर्ष के उत्तरदाताओं की संख्या सर्वाधिक 86 (28.67%) है। इसके बाद 18-25 वर्ष के 68 (22.67%) और 36-45 वर्ष के 64 (21.33%) उत्तरदाता हैं। इस प्रकार नमूने में अपेक्षाकृत युवा एवं कार्यशील आयु वर्ग की पर्याप्त उपस्थिति दिखाई गई है। यह डिजिटल तकनीकों के उपयोग तथा साइबर सुरक्षा जागरूकता के अध्ययन के लिए उपयोगी हो सकता है। शैक्षिक स्तर के संदर्भ में स्नातक उत्तरदाताओं की संख्या 103 (34.33%) तथा स्नातकोत्तर उत्तरदाताओं की संख्या 72 (24.00%) है। इससे संकेत मिलता है कि उदाहरणात्मक नमूने में उच्च शिक्षा प्राप्त उत्तरदाताओं का पर्याप्त प्रतिनिधित्व है। निवास क्षेत्र में ग्रामीण उत्तरदाता 39.33%, शहरी 36.00% तथा अर्ध-शहरी 24.67% हैं, जिससे डिजिटल पहुँच के विभिन्न सामाजिक संदर्भों की तुलना की जा सकती है। इंटरनेट उपयोग के आँकड़े विशेष रूप से महत्वपूर्ण हैं। 34.33% उत्तरदाता प्रतिदिन 3-5 घंटे इंटरनेट का उपयोग करते हैं, जबकि 23.33% पाँच घंटे से अधिक समय ऑनलाइन रहते हैं। अर्थात् उदाहरणात्मक नमूने में डिजिटल निर्भरता अपेक्षाकृत अधिक है। डिजिटल भुगतान का नियमित उपयोग करने वाले उत्तरदाताओं की संख्या 197 (65.67%) है। इससे वित्तीय डिजिटल सेवाओं पर निर्भरता का संकेत मिलता है। इसके विपरीत, 161 (53.67%) उत्तरदाताओं ने कोई औपचारिक साइबर सुरक्षा प्रशिक्षण प्राप्त नहीं किया है। केवल 57 (19.00%) ने नियमित प्रशिक्षण प्राप्त किया है। डिजिटल साक्षरता में 52% उत्तरदाता मध्यम स्तर पर हैं। यह अंतर महत्वपूर्ण है क्योंकि डिजिटल सेवाओं का व्यापक उपयोग और साइबर सुरक्षा प्रशिक्षण का सीमित प्रसार एक साथ मौजूद हो सकते हैं। अतः साइबर सुरक्षा केवल तकनीकी अवसंरचना का प्रश्न नहीं, बल्कि डिजिटल व्यवहार और मानव क्षमता का भी विषय है।

तालिका 2: विभिन्न साइबर खतरों के प्रति उत्तरदाताओं की जागरूकता एवं अनुभव

साइबर सुरक्षा संकेतक	निम्न जागरूकता (%)	मध्यम (%)	उच्च (%)	माध्य	मानक विचलन
फिशिंग की पहचान	14	43	43	3.68	0.91
रैनसमवेयर की जानकारी	21	46	33	3.39	0.96
मैलवेयर की जानकारी	16	47	37	3.52	0.93
पासवर्ड सुरक्षा	9	38	53	3.91	0.86
दो-स्तरीय प्रमाणीकरण	23	41	36	3.47	1.01
डेटा चोरी के जोखिम की जानकारी	13	42	45	3.73	0.89
सोशल इंजीनियरिंग की जानकारी	27	44	29	3.24	1.02
सार्वजनिक Wi-Fi के जोखिम	25	43	32	3.31	1.00
साइबर धोखाधड़ी की पहचान	12	40	48	3.79	0.88
संदिग्ध लिंक से बचाव	11	35	54	3.94	0.84

व्यक्तिगत डेटा की सुरक्षा	10	39	51	3.87	0.87
साइबर अपराध की रिपोर्टिंग	28	45	27	3.18	1.04

तालिका 2 में विभिन्न प्रकार के साइबर खतरों के संबंध में उत्तरदाताओं की जागरूकता का उदाहरणात्मक विश्लेषण प्रस्तुत किया गया है। परिणामों में पासवर्ड सुरक्षा का माध्य 3.91 तथा संदिग्ध लिंक से बचाव का माध्य 3.94 है। क्रमशः 53% और 54% उत्तरदाता इन क्षेत्रों में उच्च जागरूकता श्रेणी में हैं। इससे संकेत मिलता है कि सामान्य स्तर की डिजिटल सुरक्षा सावधानियाँ अपेक्षाकृत अधिक परिचित हो सकती हैं। व्यक्तिगत डेटा की सुरक्षा का माध्य 3.87 और साइबर धोखाधड़ी की पहचान का माध्य 3.79 है। 51% उत्तरदाता व्यक्तिगत डेटा सुरक्षा और 48% साइबर धोखाधड़ी पहचान में उच्च जागरूकता रखते हैं। डिजिटल सेवाओं और ऑनलाइन वित्तीय गतिविधियों के विस्तार के संदर्भ में ये दोनों आयाम विशेष महत्व रखते हैं। दूसरी ओर, सोशल इंजीनियरिंग की जानकारी का माध्य 3.24 तथा साइबर अपराध की रिपोर्टिंग का माध्य 3.18 है। यह उदाहरणात्मक पैटर्न संकेत देता है कि सामान्य साइबर सावधानियों की तुलना में जटिल साइबर खतरों और घटना-रिपोर्टिंग की जानकारी अपेक्षाकृत कम हो सकती है। रैनसमवेयर की जानकारी का माध्य 3.39 और सार्वजनिक Wi-Fi के जोखिम का माध्य 3.31 है। इससे यह संभावना सामने आती है कि साइबर सुरक्षा प्रशिक्षण को केवल पासवर्ड और फिशिंग तक सीमित रखने के बजाय आधुनिक और बहुआयामी साइबर खतरों को भी शामिल करना चाहिए। दो-स्तरीय प्रमाणीकरण का माध्य 3.47 है। डिजिटल खातों की सुरक्षा में यह एक महत्वपूर्ण व्यवहारिक उपाय है, लेकिन उदाहरणात्मक आँकड़े बताते हैं कि सभी उपयोगकर्ता इससे समान रूप से परिचित नहीं हो सकते। समग्र रूप से तालिका यह दर्शाती है कि साइबर जागरूकता एक समान अवधारणा नहीं है। कोई व्यक्ति पासवर्ड सुरक्षा के प्रति जागरूक हो सकता है, लेकिन सोशल इंजीनियरिंग या साइबर घटना की रिपोर्टिंग की प्रक्रिया से अपरिचित हो सकता है। इसलिए साइबर सुरक्षा प्रशिक्षण में **खतरे की पहचान, रोकथाम, सुरक्षित डिजिटल व्यवहार और घटना की रिपोर्टिंग**—चारों पहलुओं को शामिल करना आवश्यक है।

तालिका 3: राष्ट्रीय सुरक्षा पर साइबर खतरों के संभावित प्रभाव के संबंध में उत्तरदाताओं की धारणा

राष्ट्रीय सुरक्षा आयाम	असहमत (%)	तटस्थ (%)	सहमत (%)	माध्य	मानक विचलन
साइबर हमले आर्थिक सुरक्षा को प्रभावित कर सकते हैं	8	13	79	4.12	0.82
बैंकिंग प्रणाली साइबर हमलों के प्रति संवेदनशील है	7	15	78	4.08	0.85
महत्वपूर्ण सूचना अवसंरचना की सुरक्षा आवश्यक है	5	9	86	4.31	0.74
ऊर्जा क्षेत्र की साइबर सुरक्षा राष्ट्रीय सुरक्षा से जुड़ी है	8	17	75	4.02	0.88
दूरसंचार नेटवर्क की सुरक्षा आवश्यक है	6	11	83	4.18	0.79
सरकारी डेटाबेस की सुरक्षा महत्वपूर्ण है	4	8	88	4.36	0.71
साइबर जासूसी रणनीतिक जोखिम पैदा कर सकती है	9	16	75	4.01	0.91
रैनसमवेयर सार्वजनिक सेवाओं को प्रभावित कर सकता है	10	18	72	3.94	0.94
साइबर हमले प्रशासनिक निरंतरता को प्रभावित कर सकते हैं	8	14	78	4.08	0.84
साइबर सुरक्षा रक्षा व्यवस्था का हिस्सा है	7	12	81	4.16	0.82
अंतरराष्ट्रीय साइबर सहयोग आवश्यक है	6	10	84	4.25	0.76
साइबर संकट के लिए राष्ट्रीय स्तर की तैयारी आवश्यक है	4	8	88	4.37	0.69

तालिका 3 साइबर सुरक्षा और राष्ट्रीय सुरक्षा के बीच संबंध को समझने के लिए विभिन्न आयामों का विश्लेषण प्रस्तुत करती है। उदाहरणात्मक परिणामों में सरकारी डेटाबेस की सुरक्षा का माध्य 4.36 और राष्ट्रीय स्तर की साइबर संकट तैयारी का माध्य 4.37 है। क्रमशः 88% उत्तरदाता दोनों बिंदुओं से सहमत हैं। यह दर्शाता है कि सरकारी डिजिटल प्रणालियों और राष्ट्रीय साइबर प्रतिक्रिया क्षमता को महत्वपूर्ण सुरक्षा आयाम के रूप में देखा जा सकता है। महत्वपूर्ण सूचना अवसंरचना की सुरक्षा का माध्य 4.31 है तथा 86% उत्तरदाता इससे सहमत हैं। ऊर्जा, दूरसंचार, बैंकिंग, परिवहन और अन्य आवश्यक प्रणालियों की डिजिटल निर्भरता के कारण इनकी सुरक्षा का संबंध व्यापक राष्ट्रीय सुरक्षा से हो सकता है। अंतरराष्ट्रीय साइबर सहयोग का माध्य 4.25 है और 84% उत्तरदाता इसके पक्ष में हैं। साइबर गतिविधियों की अंतरराष्ट्रीय प्रकृति के कारण सीमा-पार सूचना साझा करना, तकनीकी सहयोग और साइबर अपराध से संबंधित समन्वय महत्वपूर्ण हो सकते हैं। दूरसंचार नेटवर्क की सुरक्षा का माध्य 4.18 और साइबर सुरक्षा को रक्षा व्यवस्था का हिस्सा मानने का माध्य 4.16 है। यह दर्शाता है कि साइबर सुरक्षा को केवल IT विभाग की जिम्मेदारी मानने के बजाय राष्ट्रीय सुरक्षा के व्यापक ढाँचे में रखने की धारणा मजबूत हो सकती है। आर्थिक सुरक्षा के संदर्भ में 79% उत्तरदाता साइबर हमलों के संभावित प्रभाव से सहमत हैं। बैंकिंग प्रणाली की संवेदनशीलता का माध्य 4.08 है। इसी प्रकार प्रशासनिक निरंतरता और साइबर हमलों के बीच संबंध का माध्य 4.08 है। रैनसमवेयर के संदर्भ में सहमति 72% है, जो अन्य कुछ संकेतकों की तुलना में कम है। इसका कारण संभावित रूप से रैनसमवेयर के प्रभाव की समझ में अंतर हो सकता है। समग्र रूप से तालिका का उदाहरणात्मक पैटर्न यह दर्शाता है कि साइबर सुरक्षा को **आर्थिक, प्रशासनिक, रणनीतिक और महत्वपूर्ण अवसंरचना सुरक्षा** से जोड़कर देखना आवश्यक है।

तालिका 4: साइबर सुरक्षा को मजबूत करने के लिए संस्थागत एवं नीतिगत उपायों पर उत्तरदाताओं की राय

सुरक्षा उपाय	निम्न प्राथमिकता (%)	मध्यम प्राथमिकता (%)	उच्च प्राथमिकता (%)	माध्य	मानक विचलन
साइबर सुरक्षा प्रशिक्षण	7	20	73	4.02	0.86
सरकारी साइबर सुरक्षा ढाँचे को मजबूत करना	5	15	80	4.21	0.77
महत्वपूर्ण सूचना अवसंरचना की निगरानी	4	14	82	4.28	0.73
साइबर अपराध रिपोर्टिंग प्रणाली	8	19	73	4.01	0.88
डेटा संरक्षण उपाय	5	13	82	4.26	0.75
साइबर विशेषज्ञों की नियुक्ति	6	17	77	4.11	0.81
स्कूल/विश्वविद्यालय साइबर शिक्षा	9	21	70	3.94	0.91
नियमित सुरक्षा ऑडिट	5	16	79	4.17	0.78
साइबर incident response क्षमता	4	15	81	4.25	0.76
निजी क्षेत्र के साथ सहयोग	8	18	74	4.03	0.85
अंतरराष्ट्रीय सहयोग	7	16	77	4.12	0.82
AI आधारित साइबर निगरानी	10	20	70	3.91	0.93

तालिका 4 में साइबर सुरक्षा को मजबूत करने के लिए विभिन्न संस्थागत, तकनीकी और नीतिगत उपायों की प्राथमिकता का उदाहरणात्मक विश्लेषण प्रस्तुत किया गया है। महत्वपूर्ण सूचना अवसंरचना की निगरानी का माध्य 4.28 और डेटा संरक्षण का माध्य 4.26 है। क्रमशः 82% उत्तरदाता इन उपायों को उच्च प्राथमिकता देते हैं। यह दर्शाता है कि डिजिटल प्रणालियों की सुरक्षा के साथ-साथ संवेदनशील डेटा की सुरक्षा को भी महत्वपूर्ण माना जा सकता है। Incident response क्षमता का माध्य 4.25 है और 81% उत्तरदाता इसे उच्च प्राथमिकता देते हैं। साइबर सुरक्षा केवल हमले रोकने तक सीमित नहीं है; हमला होने की स्थिति में उसकी पहचान, containment, recovery और services की बहाली भी महत्वपूर्ण है। इसलिए incident response व्यवस्था राष्ट्रीय साइबर लचीलापन का महत्वपूर्ण हिस्सा हो सकती है। सरकारी साइबर सुरक्षा ढाँचे को मजबूत करने का माध्य 4.21 है, जबकि नियमित सुरक्षा ऑडिट का माध्य 4.17 है। इससे यह संकेत मिलता है कि साइबर

सुरक्षा के लिए संस्थागत क्षमता और निरंतर परीक्षण दोनों आवश्यक हो सकते हैं। साइबर विशेषज्ञों की नियुक्ति का माध्य 4.11 है। यह साइबर सुरक्षा में प्रशिक्षित मानव संसाधन की आवश्यकता की ओर संकेत करता है। इसी प्रकार निजी क्षेत्र के साथ सहयोग का माध्य 4.03 है। चूँकि डिजिटल अवसंरचना का एक महत्वपूर्ण भाग सार्वजनिक और निजी संस्थाओं दोनों से जुड़ा हो सकता है, इसलिए समन्वित सुरक्षा दृष्टिकोण उपयोगी हो सकता है। विद्यालय एवं विश्वविद्यालय स्तर पर साइबर शिक्षा का माध्य 3.94 है। यह संकेत देता है कि दीर्घकालिक साइबर सुरक्षा के लिए कम आयु से डिजिटल सुरक्षा व्यवहार विकसित करना महत्वपूर्ण हो सकता है। AI आधारित साइबर निगरानी का माध्य 3.91 है। यद्यपि इसे उच्च प्राथमिकता देने वाले उत्तरदाताओं की संख्या 70% है, लेकिन इसका माध्य अन्य कुछ उपायों से कम है। इससे संकेत मिलता है कि नई तकनीकों को अपनाने के साथ उनके जोखिम, विश्वसनीयता, लागत और मानव निगरानी जैसे पहलुओं पर भी विचार आवश्यक है।

तालिका 5: साइबर जागरूकता, संस्थागत क्षमता और राष्ट्रीय सुरक्षा के बीच सहसंबंध

चर	साइबर जागरूकता	डिजिटल साक्षरता	साइबर प्रशिक्षण	तकनीकी क्षमता	संस्थागत तैयारी	राष्ट्रीय सुरक्षा धारणा
साइबर जागरूकता	1.00	0.64**	0.59**	0.46**	0.51**	0.63**
डिजिटल साक्षरता	0.64**	1.00	0.55**	0.49**	0.48**	0.57**
साइबर प्रशिक्षण	0.59**	0.55**	1.00	0.61**	0.66**	0.68**
तकनीकी क्षमता	0.46**	0.49**	0.61**	1.00	0.72**	0.75**
संस्थागत तैयारी	0.51**	0.48**	0.66**	0.72**	1.00	0.81**
राष्ट्रीय सुरक्षा धारणा	0.63**	0.57**	0.68**	0.75**	0.81**	1.00

टिप्पणी: $p < 0.01$; सभी मान उदाहरणात्मक/सिमुलेटेड हैं।

तालिका 5 में साइबर जागरूकता, डिजिटल साक्षरता, प्रशिक्षण, तकनीकी क्षमता, संस्थागत तैयारी और राष्ट्रीय सुरक्षा धारणा के बीच उदाहरणात्मक Pearson correlation प्रस्तुत किया गया है। इसका उद्देश्य यह दिखाना है कि अध्ययन में अनेक चरों के बीच संबंधों का सांख्यिकीय परीक्षण किस प्रकार किया जा सकता है। संस्थागत तैयारी और राष्ट्रीय सुरक्षा धारणा के बीच $r = 0.81$ का सकारात्मक संबंध प्रस्तुत किया गया है। तकनीकी क्षमता और राष्ट्रीय सुरक्षा धारणा के बीच 0.75 तथा साइबर प्रशिक्षण और राष्ट्रीय सुरक्षा धारणा के बीच 0.68 का संबंध दिखाई देता है। यह पैटर्न संकेत करता है कि राष्ट्रीय साइबर सुरक्षा को केवल तकनीकी उपकरणों से नहीं, बल्कि संस्थागत तैयारी और प्रशिक्षित मानव संसाधन के साथ समझना आवश्यक है। तकनीकी क्षमता और संस्थागत तैयारी के बीच 0.72 का सकारात्मक संबंध है। इससे यह संभावना सामने आती है कि तकनीकी अवसंरचना और संस्थागत प्रक्रियाएँ एक-दूसरे की पूरक हो सकती हैं। उदाहरण के लिए, आधुनिक सुरक्षा प्रणाली उपलब्ध होने के बावजूद यदि incident response, monitoring और trained personnel की व्यवस्था कमजोर हो, तो तकनीकी निवेश का अपेक्षित प्रभाव सीमित हो सकता है। साइबर जागरूकता और राष्ट्रीय सुरक्षा धारणा के बीच 0.63 का सकारात्मक संबंध तथा डिजिटल साक्षरता और राष्ट्रीय सुरक्षा धारणा के बीच 0.57 का संबंध प्रस्तुत किया गया है। इससे संकेत मिलता है कि नागरिक स्तर की डिजिटल क्षमता भी व्यापक साइबर सुरक्षा पारिस्थितिकी तंत्र का हिस्सा हो सकती है। साइबर प्रशिक्षण और संस्थागत तैयारी के बीच 0.66 का सकारात्मक संबंध है। यह विशेष रूप से महत्वपूर्ण है क्योंकि साइबर सुरक्षा में मानव संसाधन की भूमिका लगातार बढ़ रही है। प्रशिक्षण कर्मचारियों को साइबर खतरों की पहचान, सुरक्षा प्रोटोकॉल और incident reporting के प्रति अधिक तैयार करने में सहायक हो सकता है। हालाँकि, इन सहसंबंधों से **कारण-परिणाम संबंध स्थापित नहीं किया जा सकता**। उदाहरण के लिए, उच्च संस्थागत तैयारी राष्ट्रीय सुरक्षा की बेहतर धारणा

से संबंधित हो सकती है, लेकिन इससे यह स्वतः सिद्ध नहीं होता कि केवल संस्थागत तैयारी ही राष्ट्रीय सुरक्षा को बढ़ाती है। वास्तविक अध्ययन में multiple regression, ANOVA, chi-square तथा reliability analysis जैसे परीक्षणों के माध्यम से इन संबंधों की आगे जाँच की जानी चाहिए। इस प्रकार पाँचों तालिकाओं का संयुक्त उदाहरणात्मक विश्लेषण यह दर्शाता है कि डिजिटल युग में साइबर सुरक्षा एक **बहुआयामी सुरक्षा व्यवस्था** है, जिसमें नागरिक जागरूकता, डिजिटल साक्षरता, प्रशिक्षण, तकनीकी क्षमता, संस्थागत तैयारी, डेटा सुरक्षा और राष्ट्रीय स्तर की incident response क्षमता सभी परस्पर जुड़े हुए आयाम हैं।

4. चर्चा (Discussion)

प्रस्तुत अध्ययन से यह स्पष्ट होता है कि डिजिटल युग में साइबर सुरक्षा को केवल कंप्यूटर या नेटवर्क सुरक्षा के सीमित अर्थ में नहीं समझा जा सकता। यह राष्ट्रीय सुरक्षा, आर्थिक स्थिरता, सार्वजनिक प्रशासन, नागरिक डेटा और महत्वपूर्ण सूचना अवसंरचना से जुड़ा बहुआयामी विषय है। साहित्य में Buchanan, Kello, Nye तथा Rid जैसे विद्वानों के अध्ययन साइबर गतिविधियों के रणनीतिक और भू-राजनीतिक प्रभावों को रेखांकित करते हैं। विशेष रूप से साइबर हमलों के attribution, deterrence और interstate competition से संबंधित प्रश्न राष्ट्रीय सुरक्षा के लिए महत्वपूर्ण हैं। प्रस्तुत उदाहरणात्मक सांख्यिकीय विश्लेषण में साइबर सुरक्षा जागरूकता के विभिन्न स्तर दिखाई देते हैं। पासवर्ड सुरक्षा, संदिग्ध लिंक से बचाव और व्यक्तिगत डेटा सुरक्षा जैसे सामान्य सुरक्षा व्यवहारों में अपेक्षाकृत उच्च जागरूकता दिखाई गई है। इसके विपरीत, सोशल इंजीनियरिंग, रैनसमवेयर और साइबर अपराध की रिपोर्टिंग जैसे जटिल विषयों में जागरूकता अपेक्षाकृत कम दिखाई गई है। यह अंतर बताता है कि साइबर सुरक्षा प्रशिक्षण को केवल सामान्य डिजिटल सावधानियों तक सीमित नहीं रखा जाना चाहिए। अध्ययन का एक महत्वपूर्ण आयाम मानव संसाधन और प्रशिक्षण है। डिजिटल प्रणालियों की सुरक्षा के लिए अत्याधुनिक तकनीक आवश्यक है, लेकिन प्रशिक्षित कर्मचारी और जागरूक उपयोगकर्ता भी उतने ही महत्वपूर्ण हैं। उदाहरणात्मक सहसंबंधों में साइबर प्रशिक्षण और संस्थागत तैयारी के बीच सकारात्मक संबंध दिखाई दिया है। यह परिणाम इस दृष्टिकोण के अनुरूप है कि cybersecurity resilience में technical controls के साथ organizational preparedness भी आवश्यक है। राष्ट्रीय सुरक्षा के संदर्भ में महत्वपूर्ण सूचना अवसंरचना विशेष महत्व रखती है। बैंकिंग, ऊर्जा, दूरसंचार, स्वास्थ्य और सरकारी डिजिटल प्रणालियों में व्यवधान का प्रभाव व्यापक हो सकता है। भारत में NCIIPC की स्थापना critical information infrastructure protection के लिए की गई है, जबकि CERT-In राष्ट्रीय स्तर पर cybersecurity incidents के response में महत्वपूर्ण भूमिका निभाता है। डेटा संरक्षण भी राष्ट्रीय साइबर सुरक्षा का महत्वपूर्ण घटक है। Digital Personal Data Protection Act, 2023 व्यक्तिगत डिजिटल डेटा के संरक्षण और lawful processing के लिए कानूनी ढाँचा प्रदान करता है। इससे साइबर सुरक्षा का संबंध केवल राष्ट्रीय संस्थाओं से नहीं, बल्कि नागरिकों के डिजिटल अधिकार और विश्वास से भी जुड़ता है। हालाँकि, सहसंबंधात्मक परिणामों को कारण-परिणाम संबंध के रूप में नहीं समझना चाहिए। उदाहरणात्मक डेटा केवल संभावित संबंधों को प्रदर्शित करता है। वास्तविक अध्ययन में inferential statistical tests तथा वास्तविक क्षेत्रीय डेटा के आधार पर ही परिकल्पनाओं का परीक्षण किया जाना चाहिए।

5. निष्कर्ष (Conclusion)

डिजिटल परिवर्तन ने राष्ट्रीय सुरक्षा की पारंपरिक अवधारणा का विस्तार किया है। आज किसी देश की सुरक्षा केवल उसकी भौगोलिक सीमाओं और सैन्य क्षमताओं पर निर्भर नहीं है, बल्कि डिजिटल नेटवर्क, डेटा, संचार प्रणाली, वित्तीय संस्थानों, ऊर्जा प्रणालियों और महत्वपूर्ण सूचना अवसंरचना की सुरक्षा भी राष्ट्रीय सुरक्षा का अभिन्न हिस्सा है। अध्ययन से यह निष्कर्ष निकाला जा सकता है कि साइबर सुरक्षा को **तकनीकी क्षमता, मानव जागरूकता, संस्थागत तैयारी और प्रभावी नीतिगत व्यवस्था** के संयुक्त ढाँचे में समझना आवश्यक है। केवल firewall, encryption या antivirus जैसे तकनीकी उपाय पर्याप्त नहीं हैं। नियमित training, security audits, incident response, information sharing और public awareness भी साइबर resilience के आवश्यक घटक हैं। भारत में CERT-In, NCIIPC, NCCC, National Cyber Security Coordinator और NIC-CERT जैसी संस्थागत व्यवस्थाएँ साइबर सुरक्षा प्रतिक्रिया, समन्वय और महत्वपूर्ण सूचना अवसंरचना की सुरक्षा में महत्वपूर्ण भूमिका निभाती हैं। साथ ही, Digital Personal Data Protection Act, 2023 ने डिजिटल व्यक्तिगत डेटा संरक्षण के लिए एक महत्वपूर्ण कानूनी आधार उपलब्ध कराया है। भविष्य की साइबर सुरक्षा रणनीति में तीन स्तरों पर विशेष ध्यान आवश्यक है—**नागरिक स्तर पर साइबर जागरूकता, संस्थागत स्तर पर तकनीकी**

एवं प्रशासनिक क्षमता तथा राष्ट्रीय स्तर पर रणनीतिक समन्वय। विशेष रूप से महत्वपूर्ण सूचना अवसंरचना की सुरक्षा, प्रशिक्षित साइबर विशेषज्ञों की उपलब्धता, incident response क्षमता और अंतरराष्ट्रीय सहयोग को मजबूत करना आवश्यक है। अतः डिजिटल युग में साइबर सुरक्षा को केवल IT-sector की जिम्मेदारी के रूप में देखना पर्याप्त नहीं है। यह **राष्ट्रीय सुरक्षा, आर्थिक सुरक्षा, प्रशासनिक निरंतरता और नागरिक डिजिटल विश्वास** से संबंधित व्यापक विषय है। एक प्रभावी राष्ट्रीय साइबर सुरक्षा व्यवस्था वही होगी जो तकनीकी सुरक्षा को मानव क्षमता, संस्थागत समन्वय, कानूनी व्यवस्था और निरंतर जोखिम प्रबंधन के साथ जोड़ सके।

संदर्भ सूची (References)

- [1]. Arquilla, J., & Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, 12(2), 141–165.
- [2]. Buchanan, B. (2017). *The cybersecurity dilemma: Hacking, trust and fear between nations*. Oxford University Press.
- [3]. Buchanan, B. (2020). *The hacker and the state: Cyber attacks and the new normal of geopolitics*. Harvard University Press.
- [4]. Choucri, N., & Clark, D. D. (2019). *International relations in the cyber age*. MIT Press.
- [5]. Dunn Cavelty, M. (2013). From cyber-bombs to political fallout: Threat representations with an impact in the cyber-security discourse. *International Studies Review*, 15(1), 105–122.
- [6]. Gartzke, E. (2013). The myth of cyberwar: Bringing war in cyberspace back down to earth. *International Security*, 38(2), 41–73.
- [7]. Gartzke, E., & Lindsay, J. R. (2015). Weaving tangled webs: Offense, defense, and deception in cyberspace. *Security Studies*, 24(2), 316–348.
- [8]. Hansen, L., & Nissenbaum, H. (2009). Digital disaster, cyber security, and the Copenhagen School. *International Studies Quarterly*, 53(4), 1155–1175.
- [9]. Kello, L. (2017). *The virtual weapon and international order*. Yale University Press.
- [10]. Libicki, M. C. (2009). *Cyberdeterrence and cyberwar*. RAND Corporation.
- [11]. National Informatics Centre. (n.d.). *Security: NIC-CERT*. Government of India.
- [12]. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce.
- [13]. Nye, J. S., Jr. (2017). Deterrence and dissuasion in cyberspace. *International Security*, 41(3), 44–71.
- [14]. Perkovich, G., & Levite, A. E. (Eds.). (2017). *Understanding cyber conflict: Fourteen analogies*. Georgetown University Press.
- [15]. Rid, T. (2012). Cyber war will not take place. *Journal of Strategic Studies*, 35(1), 5–32.
- [16]. Rid, T., & Buchanan, B. (2015). Attributing cyber attacks. *Journal of Strategic Studies*, 38(1–2), 4–37.
- [17]. Government of India. (2000). *Information Technology Act, 2000*. Ministry of Electronics and Information Technology.
- [18]. Government of India. (2023). *Digital Personal Data Protection Act, 2023*. Ministry of Law and Justice.
- [19]. Government of India. (2025). *Cybersecurity framework and capacity-building measures*. Ministry of Electronics and Information Technology.
- [20]. Valeriano, B., Jensen, B. M., & Maness, R. C. (2018). *Cyber strategy: The evolving character of power and coercion*. Oxford University Press.
- [21]. Valeriano, B., & Maness, R. C. (2015). *Cyber war versus cyber realities: Cyber conflict in the international system*. Oxford University Press.