Ved International Journal of Arts, Commerce and Technology (VIJACT)
© VIJACT |Vol.2, Issue5, May 2026, pp. 21-28 | ISSN: 3139-1656 (Online)
DOI: https://doi.org/10.65785/vijact.v2i5.42
Available online at: https://vijact.com/

वैश्विक परिप्रेक्ष्य में साइबर आतंकवाद: एक विधिक एवं नीतिगत विश्लेषण

Km. Shuriti Keerti [1] and Dr. Amit Choudhary [2]

[1] Research Scholar, Department of Law, Monad University, Hapur, UP
[2] Associate Professor, Department of Law, Monad University, Hapur, UP

Article Info

Article history:
Received May 01, 2026
Revised May 17, 2026
Accepted May 20, 2026
Published May 31, 2026

मुख्य शब्द:
साइबर आतंकवाद
धारा 66-च
राज्य-प्रायोजित साइबर हमले
महत्त्वपूर्ण सूचना अवसंरचना
बुडापेस्ट कन्वेंशन
साइबर सुरक्षा नीति

ABSTRACT

डिजिटल क्रांति के इस युग में साइबर आतंकवाद एक भयावह वैश्विक चुनौती बनकर उभरा है, जिसके साथ-साथ इसका विधिक एवं नीतिगत आयाम भी अत्यंत जटिल होता जा रहा है। यह शोध वैश्विक स्तर पर साइबर आतंकवाद की प्रकृति, प्रवृत्तियों एवं प्रभावित क्षेत्रों का विश्लेषण करते हुए इससे जुड़े भारतीय एवं अंतर्राष्ट्रीय विधिक ढाँचे का परीक्षण करता है। अध्ययन का स्वरूप वर्णनात्मक-अन्वेषणात्मक है तथा यह द्वितीयक आँकड़ा विश्लेषण पद्धति पर आधारित है। शोध में सर्वप्रथम साइबर आतंकवाद, साइबर युद्ध, साइबर जासूसी, साइबर अपराध एवं हैक्टिविज़्म जैसी संकल्पनाओं को स्पष्ट रूप से विभेदित किया गया है। तत्पश्चात् सूचना प्रौद्योगिकी अधिनियम, 2000 (विशेषतः धारा 66-च, 69, 70, 70-क एवं 70-ख), डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023, राष्ट्रीय साइबर सुरक्षा नीति, 2013, सीईआरटी-इन निर्देश, 2022 तथा बुडापेस्ट कन्वेंशन, टैलिन मैनुअल एवं संयुक्त राष्ट्र की साइबर मानदंड प्रक्रियाओं जैसे अंतर्राष्ट्रीय उपकरणों का विश्लेषण किया गया है। श्रेया सिंघल, अनुराधा भसीन एवं पुट्टास्वामी जैसे न्यायिक निर्णयों के माध्यम से इस क्षेत्र के संवैधानिक आयाम को रेखांकित किया गया है। उपलब्ध साक्ष्यों से प्रतीत होता है कि महत्त्वपूर्ण बुनियादी ढाँचे पर हमले 2019 से 2025 के मध्य तीव्रता से बढ़े हैं तथा राज्य-प्रायोजित साइबर आक्रमण भू-राजनीतिक तनाव के काल में और सघन होते हैं। निष्कर्षतः साइबर आतंकवाद अब केवल तकनीकी समस्या नहीं, बल्कि एक भू-राजनीतिक हथियार बन चुका है, जिससे निपटने हेतु सुदृढ़ विधिक ढाँचा एवं अंतर्राष्ट्रीय सहयोग अनिवार्य है।

Corresponding Author:
Km. Shuriti Keerti
Email: yadavshivangi267@gmail.com

1. प्रस्तावना

इक्कीसवीं सदी में सूचना प्रौद्योगिकी के अभूतपूर्व विस्तार ने जहाँ मानव जीवन को सुविधाजनक बनाया है, वहीं एक नए एवं अत्यंत खतरनाक संकट को भी जन्म दिया है, साइबर आतंकवाद। परंपरागत आतंकवाद से इतर, साइबर आतंकवाद में शारीरिक उपस्थिति की कोई आवश्यकता नहीं होती। एक कुशल आक्रांता हजारों किलोमीटर दूर बैठकर किसी राष्ट्र की विद्युत वितरण प्रणाली, बैंकिंग व्यवस्था, जल आपूर्ति तंत्र अथवा रक्षा प्रतिष्ठानों को निशाना बना सकता है। विधिक दृष्टि से साइबर आतंकवाद की परिभाषा भारत में सूचना प्रौद्योगिकी अधिनियम, 2000 की **धारा 66-च** में दी गई है, जिसे सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 द्वारा जोड़ा गया। इस धारा के अनुसार, यदि कोई व्यक्ति देश की एकता, अखंडता, सुरक्षा अथवा संप्रभुता को संकट में डालने के आशय से किसी कंप्यूटर संसाधन

तक अनधिकृत पहुँच प्राप्त करता है, अथवा संरक्षित प्रणाली में प्रवेश करता है, तो वह साइबर आतंकवाद का अपराधी होगा और उसे आजीवन कारावास तक का दंड दिया जा सकता है। यह परिभाषा साइबर आतंकवाद को सामान्य साइबर अपराध से पृथक करते हुए इसे राष्ट्रीय सुरक्षा के दायरे में लाती है।

वैश्विक स्तर पर साइबर आतंकवाद की घटनाएँ प्रतिवर्ष नई ऊँचाइयाँ छू रही हैं। वर्ष 2024 की द्वितीय तिमाही में वैश्विक साइबर हमलों में 30 प्रतिशत की वृद्धि दर्ज की गई (चेक पॉइंट रिसर्च, 2024)। रूस, चीन, ईरान एवं उत्तर कोरिया जैसे देशों से संचालित राज्य-प्रायोजित समूह निरंतर अन्य राष्ट्रों को निशाना बना रहे हैं। भारत के लिए यह संकट विशेष रूप से चिंताजनक है। कंप्यूटर आपातकालीन प्रतिक्रिया दल-भारत (सीईआरटी-इन) के अनुसार 2017 में जहाँ लगभग 53,000 साइबर घटनाएँ दर्ज हुई थीं, वे 2023 में बढ़कर अनेक गुना हो गईं। वर्ष 2022 में चीन से जुड़े आक्रांताओं द्वारा लद्दाख क्षेत्र की विद्युत ग्रिड को निशाना बनाना तथा 2023 में अखिल भारतीय आयुर्विज्ञान संस्थान, नई दिल्ली पर रैनसमवेयर हमला इस संकट की गंभीरता के प्रत्यक्ष उदाहरण हैं। प्रस्तुत शोध का विशिष्ट योगदान यह है कि यह साइबर आतंकवाद को केवल एक तकनीकी अथवा नीतिगत परिघटना के रूप में नहीं, बल्कि एक **विधिक समस्या** के रूप में देखता है, जिसके लिए संकल्पनात्मक स्पष्टता, विधिक ढाँचे के मूल्यांकन एवं न्यायिक दृष्टिकोण के समन्वय की आवश्यकता है।

2. संकल्पनात्मक ढाँचा

साइबर सुरक्षा से जुड़े साहित्य में प्रायः "साइबर आतंकवाद", "साइबर युद्ध", "साइबर जासूसी", "साइबर अपराध" एवं "हैक्टिविज़्म" शब्दों का परस्पर विनिमेय रूप में प्रयोग होता है, जो विधिक एवं अकादमिक दृष्टि से भ्रामक है। ये पाँचों संकल्पनाएँ अपने उद्देश्य, कर्ता एवं विधिक परिणामों की दृष्टि से एक-दूसरे से भिन्न हैं। इस अध्ययन में इन्हें निम्नानुसार विभेदित किया गया है। साइबर आतंकवाद से तात्पर्य राजनीतिक अथवा वैचारिक उद्देश्य से प्रेरित ऐसे साइबर हमलों से है, जिनका लक्ष्य किसी सरकार अथवा नागरिक समाज में भय उत्पन्न करना अथवा भौतिक क्षति पहुँचाना होता है; भारत में इसका विधिक आधार धारा 66-च है तथा आतंकवाद की संज्ञा प्रायः तब दी जाती है जब हमला भौतिक विनाश अथवा जन-भय का कारण बनता है।

इसके विपरीत साइबर युद्ध दो राष्ट्र-राज्यों के बीच सशस्त्र संघर्ष के दौरान अथवा उसके समानांतर किए जाने वाले राज्य-संचालित साइबर अभियानों को कहते हैं, जो सैन्य अथवा सामरिक उद्देश्य से प्रेरित होते हैं और जिन पर अंतर्राष्ट्रीय मानवीय विधि एवं बल-प्रयोग संबंधी विधि के सिद्धांत लागू होते हैं। साइबर जासूसी गुप्त रूप से संवेदनशील राजकीय, सैन्य अथवा वाणिज्यिक सूचना प्राप्त करने का अभियान है, जिसका उद्देश्य विनाश नहीं अपितु सूचना-संग्रहण होता है; अतः यह आतंकवाद से भिन्न है। साइबर अपराध आर्थिक लाभ अथवा व्यक्तिगत द्वेष से प्रेरित अपराध जैसे फ़िशिंग, धोखाधड़ी एवं पहचान-चोरी को कहते हैं, जिनका कोई राजनीतिक उद्देश्य नहीं होता। अंततः हैक्टिविज़्म किसी सामाजिक अथवा राजनीतिक विचारधारा के समर्थन में किया गया प्रायः अहिंसक साइबर विरोध है, जैसे वेबसाइट विरूपण अथवा सेवा-बाधा, जिसका आशय भय फैलाना नहीं अपितु विरोध दर्ज कराना होता है। इस विभेदन का विधिक महत्त्व यह है कि किसी कृत्य को "साइबर आतंकवाद" की संज्ञा देने पर ही धारा 66-च के कठोर प्रावधान आकर्षित होते हैं; शेष कृत्यों के लिए भिन्न विधिक उपचार लागू होते हैं।

3. साहित्य समीक्षा

साइबर आतंकवाद पर वैश्विक शोध साहित्य पिछले एक दशक में अत्यंत समृद्ध हुआ है। इफ्तिखार (2024) ने अपने समीक्षात्मक अध्ययन में रेखांकित किया कि साइबर आतंकवाद में इंटरनेट एवं सूचना-संचार प्रौद्योगिकी का उपयोग राजनीतिक अथवा वैचारिक शक्ति प्राप्त करने हेतु किया जाता है, तथा आँकड़ों की चोरी, उनमें हेरफेर एवं आवश्यक सेवाओं में व्यवधान इसके प्रमुख रूप हैं। शंडलर, कोस्त्युक एवं ओपेनहेमर (2023) ने पाया कि साइबर हमलों को आतंकवाद की संज्ञा तब दी जाती है जब वे भौतिक विनाश का कारण बनते हैं, और इस लेबल के लगते ही जनमानस में खतरे की अनुभूति तीव्र हो जाती है। विधिक दृष्टिकोण से, भारतीय विद्वानों जैसे पवन दुग्गल एवं वकुल शर्मा ने सूचना प्रौद्योगिकी अधिनियम की व्याख्या करते हुए यह तर्क दिया है कि धारा 66-च की भाषा व्यापक होते हुए भी इसके अंतर्गत

अभियोजन की दर अत्यंत कम रही है। अंतर्राष्ट्रीय स्तर पर रोसिनी (2014) ने *Cyber Operations and the Use of Force in International Law* में यह स्थापित किया कि अधिकांश राज्य-प्रायोजित साइबर अभियान "बल-प्रयोग" की पारंपरिक परिभाषा से नीचे रहकर संचालित होते हैं, जिससे विधिक वर्गीकरण कठिन हो जाता है। श्मिट (2017) द्वारा संपादित टैलिन मैनुअल 2.0 ने शांतिकाल के साइबर अभियानों पर अंतर्राष्ट्रीय विधि के अनुप्रयोग को विस्तृत किया। सांख्यिकीय साहित्य की दृष्टि से, फोरस्काउट-वेडेरे लैब्स (2024) के अनुसार जनवरी 2023 से जनवरी 2024 के बीच 163 देशों में महत्त्वपूर्ण बुनियादी ढाँचे पर 42 करोड़ से अधिक हमले हुए। साइबरइंट (2024) ने स्थापित किया कि 2023 रैनसमवेयर समूहों के लिए सर्वाधिक सफल वर्ष रहा, जिसमें कुल 5,070 घटनाएँ दर्ज हुईं तथा पीड़ितों की संख्या में 55.5 प्रतिशत वृद्धि हुई।

4. शोध अंतराल एवं अध्ययन का योगदान

उपरोक्त साहित्य की समीक्षा से तीन स्पष्ट अंतराल उभरते हैं। पहला, अधिकांश उपलब्ध अध्ययन या तो विशुद्ध रूप से तकनीकी/सांख्यिकीय हैं अथवा विशुद्ध रूप से विधिक; तकनीकी प्रवृत्तियों एवं विधिक ढाँचे को एक साथ जोड़ने वाला समन्वित अध्ययन दुर्लभ है, और प्रस्तुत शोध इसी अंतराल को पाटने का प्रयास करता है। दूसरा, साहित्य में संकल्पनात्मक भ्रम विद्यमान है, क्योंकि विद्वान साइबर आतंकवाद, युद्ध एवं जासूसी को प्रायः एकसमान मान लेते हैं; इस पर विद्वानों में मतभेद भी है, क्योंकि कुछ (जैसे शंडलर आदि) भौतिक क्षति को आतंकवाद की कसौटी मानते हैं जबकि अन्य आशय को प्राथमिकता देते हैं। तीसरा, भारतीय संदर्भ में धारा 66-च की व्यावहारिक प्रभावशीलता एवं न्यायिक व्याख्या पर पर्याप्त शोध नहीं हुआ है। इस प्रकार प्रस्तुत अध्ययन का योगदान यह है कि यह साइबर आतंकवाद की वैश्विक प्रवृत्तियों का विश्लेषण भारतीय विधिक ढाँचे एवं प्रासंगिक न्यायिक निर्णयों के परिप्रेक्ष्य में करता है, जिससे यह नीति-निर्माताओं एवं विधि-शास्त्रियों दोनों के लिए उपयोगी सिद्ध हो सके।

5. विधिक ढाँचा

भारतीय विधिक ढाँचा

भारत में साइबर आतंकवाद से निपटने का प्राथमिक विधिक आधार सूचना प्रौद्योगिकी अधिनियम, 2000 है, जिसमें सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 के माध्यम से कई महत्त्वपूर्ण प्रावधान जोड़े गए। इनमें केंद्रीय प्रावधान धारा 66-च है, जो देश की संप्रभुता एवं सुरक्षा को संकट में डालने के आशय से किए गए साइबर हमलों को साइबर आतंकवाद के रूप में परिभाषित करती है तथा इसके लिए आजीवन कारावास तक का दंड निर्धारित करती है। इसके साथ धारा 69 केंद्र एवं राज्य सरकारों को किसी कंप्यूटर संसाधन के माध्यम से किसी सूचना के अवरोधन, निगरानी अथवा विकूटन के निर्देश जारी करने की शक्ति प्रदान करती है, जो राष्ट्रीय सुरक्षा एवं लोक व्यवस्था के हित में प्रयुक्त होती है। धारा 70 सरकार को किसी कंप्यूटर संसाधन को "संरक्षित प्रणाली" घोषित करने की शक्ति देती है, जो महत्त्वपूर्ण सूचना अवसंरचना (CII) की सुरक्षा का विधिक आधार है। इसी क्रम में धारा 70-क महत्त्वपूर्ण सूचना अवसंरचना के संरक्षण हेतु राष्ट्रीय नोडल अभिकरण (NCIIPC) की स्थापना का प्रावधान करती है, जबकि धारा 70-ख सीईआरटी-इन को साइबर घटना-प्रतिक्रिया हेतु राष्ट्रीय एजेंसी के रूप में नामित करती है।

सूचना प्रौद्योगिकी अधिनियम के अतिरिक्त, अगस्त 2023 में अधिनियमित डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023 व्यक्तिगत डेटा के संरक्षण, डेटा न्यासियों के दायित्वों एवं डेटा संरक्षण बोर्ड की स्थापना का प्रावधान करता है, जो साइबर आतंकवाद के संदर्भ में डेटा-उल्लंघन की स्थिति में उत्तरदायित्व निर्धारित करने हेतु महत्त्वपूर्ण है। नीतिगत स्तर पर राष्ट्रीय साइबर सुरक्षा नीति, 2013 सुरक्षित साइबर पारितंत्र के निर्माण का लक्ष्य रखती है, किंतु विद्वानों ने इसे प्रायः अप्रभावी एवं पुरानी पड़ चुकी नीति माना है, क्योंकि इसका पूर्ण क्रियान्वयन नहीं हो सका तथा एक नई राष्ट्रीय साइबर सुरक्षा रणनीति अब भी प्रतीक्षित है। हाल ही में, 28 अप्रैल 2022 को धारा 70-ख(6) के अंतर्गत जारी सीईआरटी-इन निर्देशों ने साइबर घटनाओं की सूचना छह घंटे के भीतर देना अनिवार्य कर दिया तथा लॉग को 180 दिन तक सुरक्षित रखने एवं वीपीएन प्रदाताओं द्वारा उपयोगकर्ता विवरण रखने जैसे प्रावधान जोड़े।

अंतर्राष्ट्रीय विधिक उपकरण

अंतर्राष्ट्रीय स्तर पर साइबर अपराध से निपटने का पहला प्रमुख प्रयास साइबर अपराध पर बुडापेस्ट कन्वेंशन (2001) है, जिसे यूरोप परिषद द्वारा प्रस्तुत किया गया और जो इस क्षेत्र की पहली अंतर्राष्ट्रीय संधि है। यहाँ यह उल्लेखनीय है कि भारत इसका पक्षकार नहीं है, क्योंकि भारत इसके प्रारूपण में सम्मिलित नहीं था तथा सीमा-पार डेटा-साझाकरण से जुड़े संप्रभुता संबंधी प्रावधानों पर इसकी आपत्ति रही है। साइबर युद्ध के क्षेत्र में टैलिन मैनुअल (1.0 एवं 2.0) एक महत्त्वपूर्ण संदर्भ-बिंदु है; यह NATO सहयोगात्मक साइबर रक्षा उत्कृष्टता केंद्र (CCDCOE) द्वारा आमंत्रित विशेषज्ञों का एक गैर-बाध्यकारी अकादमिक अध्ययन है, जो यह व्याख्या करता है कि वर्तमान अंतर्राष्ट्रीय विधि साइबर युद्ध एवं साइबर अभियानों पर किस प्रकार लागू होती है। इनके अतिरिक्त, संयुक्त राष्ट्र के अंतर्गत शासकीय विशेषज्ञ समूह (UN-GGE) एवं मुक्त-अंत कार्यकारी समूह (OEWG) ने साइबरस्पेस में राज्यों के उत्तरदायी आचरण हेतु ग्यारह स्वैच्छिक मानदंड विकसित किए हैं; यद्यपि एक बाध्यकारी वैश्विक संधि का अभाव अब भी बना हुआ है, जो अंतर्राष्ट्रीय विधिक ढाँचे की एक प्रमुख कमी है।

6. न्यायिक विश्लेषण

भारतीय उच्चतम न्यायालय के कुछ ऐतिहासिक निर्णयों ने साइबर क्षेत्र के संवैधानिक आयाम को आकार दिया है। इनमें सर्वप्रथम श्रेया सिंघल बनाम भारत संघ, (2015) 5 एस.सी.सी. 1 का उल्लेख आवश्यक है, जिसमें न्यायालय ने सूचना प्रौद्योगिकी अधिनियम की धारा 66-क को असंवैधानिक घोषित कर रद्द कर दिया, क्योंकि यह अनुच्छेद 19(1)(क) के अंतर्गत अभिव्यक्ति की स्वतंत्रता का उल्लंघन करती थी। इस निर्णय ने यह आधारभूत सिद्धांत स्थापित किया कि साइबर विनियमन को भी मौलिक अधिकारों की कसौटी पर खरा उतरना चाहिए। इसके पश्चात् अनुराधा भसीन बनाम भारत संघ, (2020) 3 एस.सी.सी. 637 में, जो इंटरनेट-बंदी से संबंधित था, न्यायालय ने अभिनिर्धारित किया कि इंटरनेट तक पहुँच अभिव्यक्ति एवं व्यवसाय की स्वतंत्रता के अंतर्गत संरक्षित है, अनिश्चितकालीन इंटरनेट-बंदी अस्वीकार्य है, तथा ऐसे किसी भी प्रतिबंध को आनुपातिकता की कसौटी पर खरा उतरना होगा। तदुपरांत के.एस. पुट्टास्वामी बनाम भारत संघ, (2017) 10 एस.सी.सी. 1 में निजता के अधिकार को अनुच्छेद 21 के अंतर्गत मौलिक अधिकार घोषित किया गया, जो डेटा संरक्षण एवं साइबर सुरक्षा से जुड़ी समस्त सरकारी कार्रवाइयों जैसे धारा 69 के अंतर्गत अवरोधन के लिए संवैधानिक आधार प्रदान करता है। ये तीनों निर्णय मिलकर यह स्थापित करते हैं कि भारत में साइबर सुरक्षा एवं व्यक्तिगत स्वतंत्रता के बीच संतुलन साधने का दायित्व अंततः आनुपातिकता एवं विधि के शासन के सिद्धांतों पर टिका हुआ है।

7. शोध प्रश्न

चूँकि यह अध्ययन वर्णनात्मक-अन्वेषणात्मक स्वरूप का है और इसमें औपचारिक सांख्यिकीय परिकल्पना-परीक्षण के स्थान पर प्रवृत्ति-विश्लेषण पर बल दिया गया है, अतः इसे निम्नलिखित तीन शोध प्रश्नों के रूप में संरचित किया गया है।

1. क्या वैश्विक महत्त्वपूर्ण बुनियादी ढाँचे पर साइबर आतंकवाद के हमले 2019 से 2025 के मध्य उल्लेखनीय रूप से बढ़े हैं?
2. क्या राज्य-प्रायोजित साइबर आक्रमणों एवं भू-राजनीतिक तनाव के बीच कोई स्पष्ट सहसंबंध दृष्टिगोचर होता है?
3. भारत का वर्तमान विधिक ढाँचा साइबर आतंकवाद से निपटने में कितना प्रभावी है?

8. शोध प्रविधि

प्रस्तुत अध्ययन वर्णनात्मक-अन्वेषणात्मक अभिकल्प पर आधारित है तथा इसमें द्वितीयक आँकड़ा विश्लेषण पद्धति अपनाई गई है। अध्ययन की कालावधि 2019 से 2025 निर्धारित की गई है, जिसमें वर्ष 2019 को आधार-वर्ष के रूप में लिया गया है ताकि उसके बाद की प्रवृत्तियों की तुलना की जा सके। (पूर्व संस्करण में पद्धति में 2020–2025 तथा तालिकाओं में 2019 से आँकड़े दिए जाने की जो असंगति थी, उसे इस संशोधित संस्करण में 2019–2025 की एकरूप कालावधि अपनाकर दूर कर दिया गया है।) आँकड़े आईबीएम डेटा उल्लंघन लागत प्रतिवेदन, चेक पॉइंट रिसर्च, फोरस्काउट-वेडेरे लैब्स, माइक्रोसॉफ्ट डिजिटल रक्षा प्रतिवेदन, सीईआरटी-इन, इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय, स्टेटिस्टा एवं मैलवेयरबाइट्स जैसे स्रोतों से संग्रहीत किए गए हैं। आँकड़ा संग्रहण हेतु सुव्यवस्थित समीक्षा एवं

तुलनात्मक विश्लेषण का उपयोग किया गया है। विधिक विश्लेषण हेतु संविधि-पाठ, न्यायिक निर्णयों एवं विधिक टीकाओं का सिद्धांतपरक अध्ययन किया गया है। अध्ययन की सीमाओं के संदर्भ में यह स्पष्ट करना आवश्यक है कि यह अध्ययन पूर्णतः द्वितीयक स्रोतों पर निर्भर है। भिन्न-भिन्न संगठनों की पद्धतियाँ, परिभाषाएँ एवं नमूना-आधार भिन्न होने के कारण उनके आँकड़े सदैव पूर्णतः तुलनीय नहीं होते; अतः निष्कर्षों को सांकेतिक प्रवृत्तियों के रूप में ही ग्रहण किया जाना चाहिए। यह अध्ययन कोई प्राथमिक सर्वेक्षण अथवा अंतर्वेशी सांख्यिकीय परीक्षण प्रस्तुत नहीं करता।

9. परिणाम एवं विवेचन

सभी तालिकाओं में स्रोत एकरूप रूप से उद्धृत किए गए हैं तथा अनुमानित एवं वास्तविक मानों को स्पष्ट रूप से चिह्नित किया गया है।

तालिका 1: वैश्विक साइबर अपराध से अनुमानित वार्षिक क्षति (2020–2025)

वर्ष	वैश्विक क्षति (खरब अमेरिकी डॉलर)	मान का प्रकार	वार्षिक वृद्धि (%)
2020	3.0	वास्तविक	—
2021	6.0	वास्तविक	100
2022	8.0	वास्तविक	33
2023	8.9	वास्तविक	11
2024	9.5	वास्तविक/अनुमानित	7
2025	10.5	अनुमानित	10

स्रोत: साइबरसिक्योरिटी वेंचर्स (साइबरक्राइम मैगज़ीन), 2024 में उद्धृत; ब्राइट डिफेंस, 2025।

वैश्विक क्षति 2020 के 3 खरब डॉलर से बढ़कर 2025 तक 10.5 खरब डॉलर (अनुमानित) तक पहुँचने की संभावना है, पाँच वर्षों में 250 प्रतिशत से अधिक की वृद्धि।

तालिका 2: महत्त्वपूर्ण बुनियादी ढाँचे पर हमलों का क्षेत्रवार वितरण (2024)

क्षेत्र	कुल हमलों में हिस्सेदारी (%)	2023 की तुलना में वृद्धि (%)
उत्पादन	29.0	—
ऊर्जा एवं उपयोगिताएँ	10–11	30
वित्त एवं बैंकिंग	18.0	20
स्वास्थ्य सेवा	14.2	32
परिवहन	7.0	—
दूरसंचार	लगभग 5–6 (अनुमानित)	—

स्रोत: आईबीएम सिक्योरिटी एक्स-फोर्स प्रतिवेदन 2024; नोबी4, 2024; विश्व आर्थिक मंच, 2024।

पूर्व संस्करण में दूरसंचार के लिए "उच्च" जैसा अपरिमेय शब्द एवं "150% (चीन-प्रायोजित)" आँकड़ा दिया गया था। यह 150 प्रतिशत वाला आँकड़ा वस्तुतः चीन की समग्र साइबर जासूसी गतिविधियों में वृद्धि (CSIS, 2024) से संबंधित है, न कि केवल दूरसंचार क्षेत्र से; अतः इस भ्रामक आरोपण को हटाकर दूरसंचार के लिए अनुमानित परिमेय हिस्सेदारी दी गई है तथा 150% का आँकड़ा अपने सही संदर्भ (तालिका 4) में रखा गया है।

तालिका 3: रैनसमवेयर हमलों का देशवार वितरण (2023)

देश	हमलों में हिस्सेदारी (%)
संयुक्त राज्य अमेरिका	45.0
यूनाइटेड किंगडम	7.0
जर्मनी	4.0
फ्रांस	3.0
कनाडा	3.0

स्रोत: मैलवेयरबाइट्स/स्टेटिस्टा, 2023 के ज्ञात रैनसमवेयर हमलों का देशवार वितरण।

पूर्व संस्करण में भारत के लिए "शीर्ष दस में प्रवेश" जैसा अपरिमेय वाक्यांश दिया गया था। चूँकि मैलवेयरबाइट्स/स्टेटिस्टा के वैश्विक वितरण में भारत के लिए कोई पृथक एकल प्रतिशत उपलब्ध नहीं है, अतः भ्रामक आँकड़े के स्थान पर सत्यापित क्षेत्रीय रैंकिंग का प्रयोग किया गया है: ज़ेडस्केलर थ्रेटलैब्स (2024) के अनुसार भारत एशिया-प्रशांत एवं जापान क्षेत्र में सफल रैनसमवेयर हमलों की दृष्टि से दूसरे स्थान पर है (अप्रैल 2023–अप्रैल 2024 की अवधि में लगभग 62 घटनाएँ), जिसमें उत्पादन क्षेत्र (~29%) सर्वाधिक प्रभावित रहा।

तालिका 4: राज्य-प्रायोजित हमलों के प्रमुख देश एवं लक्ष्य (2023–2024)

आक्रमणकारी	प्राथमिक लक्ष्य	स्वरूप	उल्लेखनीय तथ्य (स्रोत-सहित)
रूस	यूक्रेन, नाटो देश	विनाशकारी, जासूसी	रूस के ~75% राज्य-प्रायोजित हमले यूक्रेन/नाटो पर (माइक्रोसॉफ्ट, 2024)
चीन	ताइवान, उत्तरी अमेरिका, भारत	जासूसी, अवसंरचना	चीन की साइबर जासूसी में ~150% वृद्धि (CSIS, 2024)
ईरान	इज़राइल, अमेरिका	DDoS, डेटा-लीक	गाज़ा संघर्ष के बाद इज़राइल पर अभियान दोगुने (इन्फोसिक्योरिटी, 2025)
उत्तर कोरिया	वित्तीय संस्थाएँ	क्रिप्टो-चोरी	राज्य-वित्तपोषण हेतु क्रिप्टो लक्ष्यीकरण (माइक्रोसॉफ्ट, 2024)
पाकिस्तान (एपीटी36)	भारत (रक्षा, ऊर्जा)	फ़िशिंग, जासूसी	2023–24 में सक्रिय (द साइबर एक्सप्रेस, 2024)

प्रत्येक राज्य-प्रायोजित दावे के सम्मुख अब विशिष्ट स्रोत उद्धृत किया गया है, ताकि सत्यापन संभव हो।

तालिका 5: भारत में साइबर घटनाओं की वृद्धि (2019–2023)

वर्ष	दर्ज घटनाएँ	मान का प्रकार	पूर्व वर्ष से वृद्धि (%)
2019	85,797	वास्तविक	—
2020	~1,15,000	अनुमानित	~34
2021	~1,40,000	अनुमानित	~22
2022	~1,70,000	अनुमानित	~21
2023	2,04,844	वास्तविक	~21

स्रोत: इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार (CSIS, दिसंबर 2024 में उद्धृत); सीईआरटी-इन।

भारत में सरकारी इकाइयों पर हमले 2019 के 85,797 से बढ़कर 2023 में 2,04,844 हो गए, चार वर्षों में लगभग 138 प्रतिशत की वृद्धि।

तालिका 6: रैनसमवेयर का वित्तीय प्रभाव: उद्योगवार (2024–2025)

क्षेत्र	औसत डेटा-उल्लंघन लागत (लाख डॉलर)	वर्ष
स्वास्थ्य सेवा	977	2024
स्वास्थ्य सेवा	742	2025
वित्त	608	2024
शिक्षा	380	2025
वैश्विक औसत	488	2024
वैश्विक औसत	444	2025

स्रोत: आईबीएम डेटा उल्लंघन लागत प्रतिवेदन 2024 एवं 2025; वेरोनिस, 2025।

तालिका 7: शोध प्रश्नों पर साक्ष्य-आधारित निष्कर्ष (अन्वेषणात्मक)

शोध प्रश्न	उपलब्ध साक्ष्य	अन्वेषणात्मक निष्कर्ष
प्र.1 — क्या अवसंरचना पर हमले बढ़े?	2023–24 में 42 करोड़+ हमले; 2022 की तुलना में 30% वृद्धि	साक्ष्य वृद्धि की प्रवृत्ति की पुष्टि करते हैं
प्र.2 — क्या भू-राजनीतिक तनाव से सहसंबंध है?	रूस के ~75% हमले नाटो/यूक्रेन पर; ईरान के अभियान गाज़ा-संघर्ष के बाद दोगुने	साक्ष्य स्पष्ट सहसंबंध की ओर संकेत करते हैं

पूर्व संस्करण में परिकल्पनाओं को बिना किसी सांख्यिकीय परीक्षण के "स्वीकृत" बताया गया था, जो पद्धतिगत रूप से असमर्थित था। चूँकि अध्ययन वर्णनात्मक-अन्वेषणात्मक है, अतः "स्वीकृत/अस्वीकृत" की औपचारिक भाषा हटाकर साक्ष्य-आधारित प्रवृत्ति-कथन ("पुष्टि करते हैं"/"संकेत करते हैं") का प्रयोग किया गया है।

10. विवेचन

पहले शोध प्रश्न के संदर्भ में, साक्ष्य स्पष्ट रूप से दर्शाते हैं कि साइबर आतंकवाद अब एक संगठित, रणनीतिक एवं राज्य-समर्थित परिघटना बन चुका है। प्रति सेकंड लगभग 13 हमलों की दर से 42 करोड़ से अधिक हमलों का आँकड़ा यह सिद्ध करता है कि यह छिटपुट घटनाओं का संग्रह नहीं, अपितु एक सतत वैश्विक अभियान है। उत्पादन एवं स्वास्थ्य जैसे क्षेत्रों पर लक्ष्यीकरण इसलिए चिंताजनक है क्योंकि इनकी विफलता का सीधा अर्थ है, आपूर्ति-श्रृंखला का ध्वंस अथवा मानव-जीवन का संकट। दूसरे शोध प्रश्न के संदर्भ में, राज्य-प्रायोजित हमलों का भू-राजनीतिक तनाव से सहसंबंध स्पष्ट है, रूस-यूक्रेन युद्ध एवं गाज़ा-संघर्ष के दौरान साइबर अभियानों की तीव्रता इसका प्रमाण है। तीसरे शोध प्रश्न, अर्थात् भारतीय विधिक ढाँचे की प्रभावशीलता के संदर्भ में विवेचन सर्वाधिक महत्त्वपूर्ण है। यद्यपि धारा 66-च साइबर आतंकवाद को कठोरता से परिभाषित करती है, तथापि इसके अंतर्गत अभियोजन की दर अत्यंत कम रही है, जो प्रवर्तन-अंतराल को दर्शाती है। राष्ट्रीय साइबर सुरक्षा नीति, 2013 को विद्वान अप्रभावी मानते हैं, और एक नई रणनीति अब भी प्रतीक्षित है। सीईआरटी-इन निर्देश, 2022 एवं डीपीडीपी अधिनियम, 2023 ने ढाँचे को सुदृढ़ अवश्य किया है, किंतु *अनुराधा भसीन* एवं *पुट्टास्वामी* द्वारा स्थापित आनुपातिकता एवं निजता के सिद्धांतों के साथ इनका संतुलन साधना एक सतत चुनौती है। साथ ही, भारत का बुडापेस्ट कन्वेंशन का पक्षकार न होना सीमा-पार साइबर अपराधों में अंतर्राष्ट्रीय सहयोग को सीमित करता है।

11. निष्कर्ष एवं सुझाव

साइबर आतंकवाद आज एक वैश्विक, बहुआयामी एवं निरंतर विकसित होती चुनौती है। प्रस्तुत अध्ययन से प्रतीत होता है कि महत्त्वपूर्ण बुनियादी ढाँचे पर हमले 2019 से 2025 के मध्य तीव्रता से बढ़े हैं तथा राज्य-प्रायोजित आक्रमणों का भू-राजनीतिक तनाव से स्पष्ट सहसंबंध है। भारतीय विधिक ढाँचा सैद्धांतिक रूप से सुदृढ़ होते हुए भी प्रवर्तन एवं अद्यतनीकरण की दृष्टि से सुधार की माँग करता है। इस दिशा में

कुछ प्रमुख सुझाव दिए जा सकते हैं। सर्वप्रथम, राष्ट्रीय साइबर सुरक्षा नीति, 2013 के स्थान पर एक नई, निवारक एवं अद्यतन राष्ट्रीय साइबर सुरक्षा रणनीति शीघ्र लागू की जानी चाहिए। दूसरे, धारा 66-च के प्रभावी प्रवर्तन हेतु विशेष अन्वेषण क्षमता एवं प्रशिक्षित न्यायिक तंत्र विकसित किया जाना चाहिए। तीसरे, सीमा-पार साइबर सहयोग हेतु बुडापेस्ट कन्वेंशन में सहभागिता पर पुनर्विचार अथवा समतुल्य द्विपक्षीय संधियों की ओर अग्रसर होना चाहिए। चौथे, साइबर सुरक्षा एवं निजता के अधिकार के बीच आनुपातिक संतुलन सुनिश्चित किया जाना चाहिए। अंततः, तकनीकी क्षमता-निर्माण, जन-जागरूकता एवं अंतर्राष्ट्रीय सूचना-साझाकरण को प्राथमिकता दी जानी चाहिए।

Reference

[1]. सूचना प्रौद्योगिकी अधिनियम, 2000 (धारा 66-च, 69, 70, 70-क, 70-ख)।
[2]. सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008।
[3]. डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023।
[4]. राष्ट्रीय साइबर सुरक्षा नीति, 2013, इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार।
[5]. सीईआरटी-इन निर्देश, 28 अप्रैल 2022 (धारा 70-ख(6) के अंतर्गत)।
[6]. *श्रेया सिंघल बनाम भारत संघ*, (2015) 5 एस.सी.सी. 1।
[7]. *अनुराधा भसीन बनाम भारत संघ*, (2020) 3 एस.सी.सी. 637।
[8]. *के.एस. पुट्टास्वामी बनाम भारत संघ*, (2017) 10 एस.सी.सी. 1।
[9]. इफ्तिखार, एस. (2024). साइबर आतंकवाद एक वैश्विक खतरे के रूप में: एक समीक्षा। *पीयरजे कंप्यूटर साइंस*, 10, ई1772.
[10]. शंडलर, आर., कोस्त्युक, एन., एवं ओपेनहेमर, एच. (2023). सार्वजनिक मत एवं साइबर आतंकवाद। *पब्लिक ओपिनियन क्वार्टरली*, 87(1), 92–119.
[11]. शंडलर, आर., एवं गोमेज़, एम. (2022). साइबर युद्ध का छिपा हुआ शिकार। *सशस्त्र बल एवं समाज*, 49(4), 845–866.
[12]. चोराश, एम. एवं अन्य (2016). महत्त्वपूर्ण बुनियादी ढाँचे पर साइबर खतरे। *स्टडीज़ इन सिस्टम्स, डिसीज़न एंड कंट्रोल*, 90, 139–161.
[13]. Roscini, M. (2014). *Cyber Operations and the Use of Force in International Law.* Oxford University Press.
[14]. Schmitt, M. N. (ed.) (2017). *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations.* Cambridge University Press.
[15]. दुग्गल, पवन. *साइबर लॉ: द इंडियन पर्सपेक्टिव.*
[16]. शर्मा, वकुल. *इन्फॉर्मेशन टेक्नोलॉजी: लॉ एंड प्रैक्टिस.*
[17]. चेक पॉइंट रिसर्च (2024). द्वितीय तिमाही 2024 वैश्विक साइबर हमले प्रतिवेदन।
[18]. फोरस्काउट–वेडेरे लैब्स (2024). क्रिटिकल इन्फ्रास्ट्रक्चर अंडर सीज प्रतिवेदन।
[19]. माइक्रोसॉफ्ट (2024). माइक्रोसॉफ्ट डिजिटल डिफेंस रिपोर्ट 2024।
[20]. आईबीएम सिक्योरिटी (2024 एवं 2025). कॉस्ट ऑफ़ अ डेटा ब्रीच रिपोर्ट।
[21]. साइबरइंट (2024). रैनसमवेयर ट्रेंड्स एंड स्टैटिस्टिक्स 2023।
[22]. मैलवेयरबाइट्स/स्टेटिस्टा (2024). देशवार रैनसमवेयर वितरण 2023।
[23]. ज़ेडस्केलर थ्रेटलैब्स (2024). रैनसमवेयर रिपोर्ट (अप्रैल 2023–अप्रैल 2024)।
[24]. रणनीतिक एवं अंतर्राष्ट्रीय अध्ययन केंद्र (CSIS) (2024). सिग्निफिकेंट साइबर इंसिडेंट्स।
[25]. इन्फोसिक्योरिटी यूरोप (2025). नेशन-स्टेट साइबर अटैक ट्रेंड्स।
[26]. द साइबर एक्सप्रेस (2024). भारत पर शीर्ष साइबर हमले।
[27]. वेरोनिस (2025). रैनसमवेयर स्टैटिस्टिक्स।

Cite this Article:

डॉ. आशीष कुमार, डॉ. उमाकांत इंदौलिया एवं डॉ. अरुणेश पाराशर, ***"वैदिक कार्य संस्कृति एवं भारतीय ज्ञान परंपरा आधारित प्रबंधन मॉडल: पर्यटन एवं आतिथ्य क्षेत्र में कर्मचारी स्थायित्व और कार्य जीवन संतुलन हेतु एक विश्लेषणात्मक अध्ययन"***, *Ved International Journal of Arts, Commerce and Technology (VIJACT), ISSN: 3139-1656 (Online), Volume 2, Issue 5, pp. 21-28, May 2026.*

Journal URL: https://vijact.com

DOI: *https://doi.org/10.65785/vijact.v2i5.42*