भारतीय वैज्ञानिक एवं औद्योगिक अनुसंधान पत्रिका
वर्ष 33 अंक (2) दिसम्बर 2025 पृ. 118-123
DOI : 10.56042/bvaap.v33i2.20894

साइबर अपराध अनुसंधान के विकास का मानचित्रणः एक वैश्विक साइंटोमेट्रिक विश्लेषण

नितिन, अनु एवं एन के प्रसन्ना
सीएसआईआर-राष्ट्रीय विज्ञान संचार और नीति अनुसंधान संस्थान, नई दिल्ली 110 012 (भारत)
वैज्ञानिक और नवीन अनुसंधान अकादमी, गाजियाबाद, उत्तर प्रदेश 201 002 (भारत)
[ई-मेलः nitin@nplindia.org]

सारांश

निरंतर डिजिटल परिवर्तन के युग में, साइबर अपराध और साइबर सुरक्षा महत्वपूर्ण शोध का विषय बन गए हैं क्योंकि सूचना प्रणाली, नेटवर्क और डेटा अखंडता के लिए खतरे लगातार बढ़ रहे हैं। इस शोध में, वर्ष 2020 से 2024 तक प्रकाशित लेखों का साइंटोमेट्रिक और बिब्लियोमेट्रिक विश्लेषण किया गया है, जो 'साइबर अपराध,' 'साइबर सुरक्षा,' एवं 'नेटवर्क सुरक्षा' कीवर्ड द्वारा वेब ऑफ़ साइंस डेटाबेस (Web of Science) से एकत्र किये गए हैं। कुल 274 रिकॉर्ड प्राप्त हुए, और डेटा को 5 वर्षों के लिए छाँटने के बाद, अंतिम डेटासेट में 149 दस्तावेज़ प्राप्त हुए। कीवर्ड सह-घटना मानचित्रण, स्रोतों के ग्रंथ सूची युग्मन और देशों के बीच सह-लेखन के लिए VOSviewer सॉफ्टवेयर का उपयोग किया गया है। इस विश्लेषण से पता चला कि साइबर खतरों के लिए तकनीकी समाधानों को लक्षित करने वाले शोधों का रुझान मजबूत हैं, जो कि विशेष रूप से मशीन लर्निंग, डीप लर्निंग और व्यवहार विश्लेषण का संदर्भ देते हैं। इंग्लैंड, यूएसए और भारत की पहचान अंतर्राष्ट्रीय अनुसंधान सहयोग के प्रमुख केंद्रों के रूप में की गई। IEEE एक्सेस और इलेक्ट्रॉनिक्स जैसी तकनीकी पत्रिकाओं को प्रकाशन का प्राथमिक स्रोत पाया गया। इसके विपरीत, ब्लॉकचेन, साइबर ग्रूमिंग और डीपफेक जैसे उभरते रुझानों को भी शोध में परिवर्तन के क्षेत्रों के रूप में पहचाना गया है। विश्लेषण से यह पता चलता है कि साइबर अपराध का आकलन करने वाले शोध बहु-विषयक और वैश्विक है और जटिल साइबर सुरक्षा मुद्दों को हल करने के लिए वैश्विक सहयोग का संकेत देते हैं।

मुख्य शब्दः साइबर अपराध, साइबर सुरक्षा, नेटवर्क सुरक्षा, साइंटोमेट्रिक

Mapping the Growth of Cybercrime Research: A Global Scientometric Analysis

Nitin Sharma, Anu & N.K. Prasanna
[1]CSIR-National Institute of Science Communication and Policy Research, New Delhi 110 012 (India)
[2]Academy of Scientific and Innovative Research, Ghaziabad, Uttar Pradesh 201 002 (India)
[E-mail: nitin@nplindia.org]

Abstract

In the era of continuous digital transformation, cybercrime and cybersecurity have become important research topics as threats to information systems, networks, and data integrity continue to grow. This research conducts a scientometric analysis of articles published from 2020 to 2024, collected from the Web of Science database using the keywords "cybercrime," "cybersecurity," and "network security." A total of 274 records were obtained, and after filtering out the data for 5 years, the final dataset contained 149 documents. VOSviewer software was used for keyword co-occurrence mapping, bibliographic linking of sources, and cross-country co-authorship. This analysis revealed a strong trend toward research targeting technical solutions to cyber threats, particularly those related to machine learning, deep learning, and behavioral analysis. England, the USA, and India were identified as major centers of international research collaboration. Technical journals such as IEEE Access and Electronics were found to be the primary sources of publication. Conversely, emerging trends such as blockchain, cyber grooming, and deepfakes were also identified as areas of research change. The analysis reveals that research assessing cybercrime is multidisciplinary and global, indicating global collaboration to address complex cybersecurity issues.

Keywords: cyber crime, cyber security, Network Security, scientometric Analysis.

प्रस्तावना

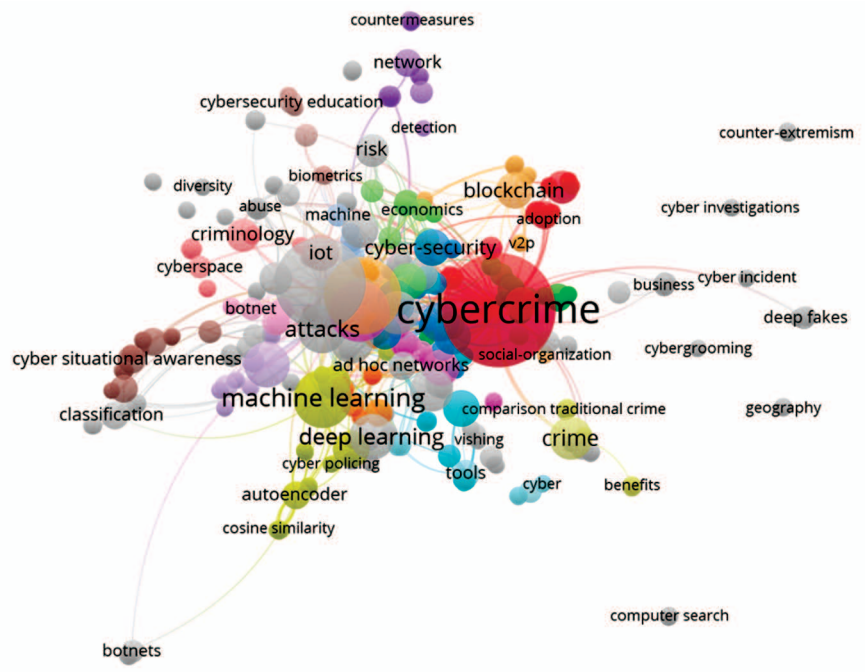
आज की डिजिटल दुनिया में, साइबर सुरक्षा सर्वोच्च प्राथमिकता बनती जा रही है क्योंकि कनेक्टेड सिस्टम का प्रसार बढ़ता जा रहा है, जो साइबर खतरों से अधिक जोखिम पेश करता है। साइबर सुरक्षा की कई अलग-अलग परिभाषाएँ हैं, लेकिन इसे मोटे तौर पर नेटवर्क, सिस्टम और डेटा को हानिकारक हमलों, अनाधिकृत पहुँच और डेटा उल्लंघनों से बचाने के लिए स्थापित प्रक्रियाओं और प्रौद्योगिकी के रूप में परिभाषित किया जा सकता है। खतरों का परिदृश्य काफी बदल गया है, जिसमें विरोधी मैलवेयर, फ़िशिंग, रैनसमवेयर और उन्नत लगातार खतरों के साथ कमजोरियों का फायदा उठाने के लिए नई उन्नत तकनीकों का उपयोग कर रहे हैं (Pfleeger & Pfleeger, 2015)। 2023 की डेटा ब्रीच जांच रिपोर्ट के सबसे खतरनाक आँकड़ों में से एक यह है कि 80% से अधिक उल्लंघनों में क्रेडेंशियल चोरी या सोशल इंजीनियरिंग हमले शामिल हैं, जो संगठनों के भीतर बेहतर साइबर सुरक्षा नियंत्रण की आवश्यकता पर बल देता है (Verizon, 2023)।

राष्ट्रीय और अंतर्राष्ट्रीय संगठन कई तरह के बचाव उपायों को लागू करके विरोधियों से होने वाले खतरों का मुकाबला करने के लिए काम कर रहे हैं, जिसमें घुसपैठ का पता लगाने वाले सिस्टम या घुसपैठ की रोकथाम करने वाले सिस्टम, एन्क्रिप्शन प्रोटोकॉल और ज़ीरो-ट्रस्ट आर्किटेक्चर (ZTA), जैसे कुछ प्रमुख तकनीक शामिल हैं (Rose et-al., 2020)। यहां तक कि आर्टिफिशियल इंटेलिजेंस (AI) और मशीन लर्निंग (ML) का उपयोग सुरक्षा टीमों को खतरों का पता लगाने और व्यवहारों का विश्लेषण करके और विसंगतियों का पता लगाकर उन खतरों का जवाब देने में सहायता करने के लिए किया जा रहा है (Sarkar et al., 2024)। सरकारों और नियामकों ने साइबर सुरक्षा की सर्वोत्तम प्रथाओं को लागू करने के लिए रूपरेखाएँ बनाई हैं। उदाहरण के लिए, यूरोपीय संघ में सामान्य डेटा सुरक्षा विनियमन (GDPR) में सख्त डेटा सुरक्षा नियम हैं, और NIST साइबर सुरक्षा रूपरेखा में महत्वपूर्ण बुनियादी ढांचे से संबंधित तकनीकों को सुरक्षित करने के लिए मार्गदर्शन शामिल है (NIST, 2018)। साथ ही, ISO/IEC 27001 जैसे अंतर्राष्ट्रीय मानक सूचना सुरक्षा प्रबंधन प्रणालियों के लिए एक रूपरेखा प्रदान करते हैं। हालाँकि सरकारें, विनियामक साइबर सुरक्षा के लिए मानकों को प्रेरित कर रहे हैं, लेकिन क्वांटम कंप्यूटिंग, इंटरनेट ऑफ़ थिंग्स (IoT) और 5G नेटवर्क सहित उभरती हुई प्रौद्योगिकियाँ नई कमज़ोरियाँ पैदा करती हैं, जिनके लिए नए साइबर सुरक्षा उपायों के निरंतर विकास की आवश्यकता होती है (Cloud Security Alliance [CSA], 2017)। इसके अलावा, साइबर हमले तेजी से AI का उपयोग कर रहे हैं, जो नई सुरक्षा चुनौतियाँ पैदा करता है, जिसके लिए अनुकूलन की आवश्यकता होती है।

मजबूत वैज्ञानिक और ग्रंथ सूची संबंधी अध्ययनों ने साइबर सुरक्षा और साइबर अपराध से संबंधित शोध संदर्भ को समझने के लिए सार्थक तरीके पेश किए हैं। एलेगार्ड और वालिन (2015) ने इन तरीकों का इस्तेमाल किया और बताया कि कैसे साइबर सुरक्षा समय के साथ कैसे एक अकादमिक घटना से एक अकादमिक अनुशासन में परिवर्तित हो गई। जैसे-जैसे डिजिटल खतरों के बारे में चर्चा अंतरराष्ट्रीय स्तर पर व्यापक होती जा रही है, साइबर सुरक्षा अनुसंधान की मात्रा बढ़ रही है।

विभिन्न अध्ययनों ने पिछले 20 वर्षों में साइबर सुरक्षा और साइबर अपराध साहित्य के विकास और वर्तमान स्थिति को समझने के लिए एक संदर्भ प्रदान किया। Wu, Peng & Lemke (2023) ने 26 साल की अवधि में वैश्विक रुझानों का विश्लेषण करने के लिए आर पैकेज (R-package) बिब्लियोमेट्रिक्स और वीओएसव्यूअर (Vosviewer) का उपयोग किया, जिसमें शीर्ष उद्धरण, सहयोगी अनुसंधान नेटवर्क और साइबर सुरक्षा व साइबर अपराध अनुसंधान से उभरने वाले नए पहलुओं पर चर्चा की गई। Nobanee et.al. (2023) ने 1999 से 2021 तक 749 अध्ययनों की समीक्षा की और साइबर सुरक्षा जोखिम से संबंधित ज्ञान में अंतराल को भरने के लिए लेखकों, देशों, पत्रिकाओं और भविष्य की दिशा की पहचान की। उनका शोध क्षेत्र के विकास और साहित्य के विकास से क्षेत्र में कैसे बदलाव आ रहा है, इस पर एक मजबूत अंतर्दृष्टि थी। Poonam et.al., (2022) ने प्रकाशनों में हाल ही में हुई घातीय वृद्धि को भी नोट किया, साइबर सुरक्षा अनुसंधान के लिए सूचना और कंप्यूटर सुरक्षा को एक प्रमुख आउटलेट के रूप में पहचाना, और प्रकाशनों में सहयोग और अन्य नए विकास (जैसे रुझान) आदि पर प्रकाश डाला।

जिंदोंग एट अलण (2024) ने 2013 से 2023 तक डेटा सुरक्षा पर शोध किया, साथ ही डेटा सुरक्षा से जुड़ी बड़ी मात्रा में जानकारी जो केवल 2018 के बाद से ही तेज होने लगी, और जो न केवल व्यक्तिगत डेटा सुरक्षा के बहुमत में बदलाव को दर्शाता है, बल्कि ब्लॉकचेन तकनीक में भी आम तौर पर बदलाव को दर्शाता है। Ali & Mushtaq (2024) ने 2013 से 2022 तक व्यापक रूप से परिभाषित साइबर सुरक्षा साहित्य का विश्लेषण किया, जिसमें प्रकाशन प्रवृत्तियों, प्रमुख लेखकों और संबद्धताओं की जांच की गई, जिसमें साइबर अपराध या साइंटोमेट्रिक विश्लेषण के किसी भी प्रकार के गहन उपयोग पर कोई विशेष कार्य या ध्यान नहीं दिया गया। इसीलिए ये अध्ययन, शोध के तेजी से बढ़ते और विविध होते क्षेत्र की ओर संकेत



चित्र 1 — कीवर्ड मैपिंग

करते हैं, जिसमें लागू और प्रासंगिक विषयों और निहितार्थों की बढ़ती हुई सीमा शामिल है।

कार्यप्रणाली

अध्ययन में साइबर अपराध और साइबर सुरक्षा में वर्तमान शोध प्रक्षेपवक्र की जांच करने के लिए एक ग्रंथसूची और विज्ञानमितीय दृष्टिकोण का उपयोग किया गया जिसके लिए वेब ऑफ़ साइंस डेटाबेस का प्रयोग किया गया है। खोज को सभी फ़ील्ड का उपयोग करके 'साइबर अपराध,' 'साइबर सुरक्षा,' और 'नेटवर्क सुरक्षा' कीवर्ड के साथ संचालित किया गया ताकि यह सुनिश्चित किया जा सके कि विभिन्न प्रकार के प्रासंगिक दस्तावेज़ कैप्चर किए गए हैं।

कुल 274 परिणाम मिले। दस्तावेजों की समयबद्धता सुनिश्चित करने के लिए, हमने 2020 से 2024 तक की सीमा को सीमित कर दिया, जिसके परिणामस्वरूप कुल 149 रिकॉर्ड प्राप्त हुए। 149 रिकॉर्ड में 50 शोध लेख, आठ समीक्षा लेख और 91 सम्मेलन कार्यवाही पत्र शामिल थे।

निम्नानुसार तीन प्रकार के विश्लेषण निष्पादित किए गए-

1. कीवर्ड सह-घटना (कीवर्ड को अकरंस) विश्लेषण यह बेहतर ढंग से समझने के लिए कि कौन से शोध विषय, उभरते विषय और वैचारिक संबंध साहित्य पर हावी हैं।
2. वैश्विक सहयोगी अनुसंधान नेटवर्क का पता लगाने के लिए राष्ट्रों द्वारा सह-लेखक पैटर्न विश्लेषण।
3. स्रोतों का ग्रंथसूची युग्मन, यह पता लगाने के लिए कि कौन सी पत्रिकाएँ और सम्मेलन कार्यवाही एक-दूसरे से सबसे अधिक संबंधित हैं, जो कि इस क्षेत्र में केंद्रीय अनुसंधान प्रकाशन स्थलों की पहचान करने में मदद करता है।

विश्लेषण और चर्चा

1. कीवर्ड सह-घटना (keyword co-occurrence)

VOSviewer कीवर्ड सह-घटना मैपिंग साइबर अपराध अनुसंधान में मौजूदा विषयों और नए व उभरते विषयों का अवलोकन प्रदान करता है। 'साइबर अपराध' शब्द मैपिंग में सबसे अधिक बार इस्तेमाल किए जाने वाले और जुड़े हुए कीवर्ड के रूप में दिखा। 'साइबर अपराध' और 'साइबर-सुरक्षा,' 'हमले,' 'साइबर खतरे,' और 'मशीन लर्निंग' के बीच मजबूत संबंधों को देखना भी दिलचस्प था, यह दर्शाता है कि अनुसंधान का एक बड़ा हिस्सा तकनीकी मार्गों और विश्लेषणात्मक तरीकों के माध्यम से साइबर खतरों का पता लगाने और उन्हें रोकने पर केंद्रित है। साथ ही साथ यह भी देखने को मिला कि 'साइबर अपराध', 'साइबर-सुरक्षा,' और 'मशीन लर्निंग' जैसे शब्दों के बीच मजबूत संबंध थे, जिसका अर्थ है कि तकनीकी समाधानों और विश्लेषणात्मक तरीकों के माध्यम से साइबर खतरों की पहचान और शमन के लिए काफी हद तक महत्व

दिया गया है। कई शब्द (जैसे, 'डीप लर्निंग,' 'ऑटोएनकोडर,' और 'कोसाइन सिमिलैरिटी') उच्च कम्प्यूटेशनल विधियों (जैसे, परिष्कृत प्रसंस्करण, पैटर्न पहचान के तरीके और वर्गीकरण/टैगिंग) के उपयोग का संकेत देते हैं। 'अपराध विज्ञान', 'साइबरस्पेस', और 'विविधता' जैसे शब्दों का प्रयोग साइबर अपराधी व्यवहार के व्यावहारिक, सामाजिक और नैतिक आयामों पर शोध या संभवतः चर्चा की ओर संकेत करता है, जो साइबर अपराधी गतिविधि के विभिन्न जनसांख्यिकी और प्रेरकों को समझने में योगदान देने के इरादे को प्रकट करता है।

उभरते और अधिक विशिष्ट विषय क्षेत्रों में शामिल हैं 'ब्लॉकचेन,' 'साइबर ग्रूमिंग,' 'डीपफेक,' और 'काउंटर-एक्सट्रीमिज्म')। ये विषय भविष्य के शोध के लिए अवसरों का प्रतिनिधित्व करते हैं क्योंकि डिजिटल खतरे जटिलता में आगे बढ़ते रहते हैं।

2. स्रोतों का ग्रंथसूची युग्मन (Bibliographic linking of sources)

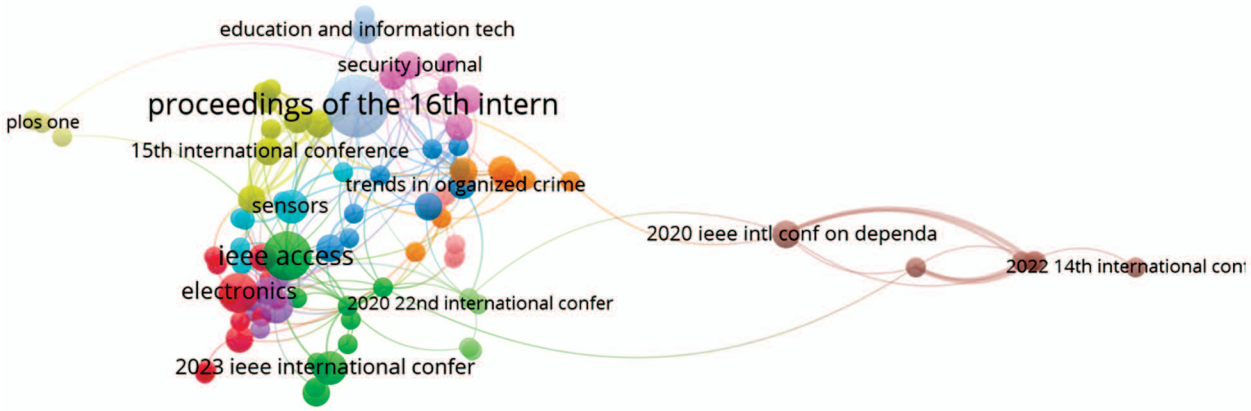
चित्र 2, VOSviewer के माध्यम से निर्मित एक ग्रंथसूची युग्मन या स्रोत सह-उद्धरण मानचित्र का प्रतिनिधित्व करता है। मानचित्र का केंद्र सबसे प्रमुख स्रोत, 'प्रोसीडिंग्स ऑफ़ द 16जी इंटरनेशनल कांफ्रेंस ऑन साइबर वारफेयर एंड सिक्योरिटी (ICCWS 2021)' का प्रतिनिधित्व करता है, जो संभवतः साइबर सुरक्षा के संदर्भ में या सूचना प्रणालियों पर आधारित एक अंतर्राष्ट्रीय सम्मेलन का प्रतिनिधित्व करता है। जो कि बताता है कि यह क्षेत्र में विश्लेषित स्रोत से सबसे अधिक उद्धृत या संदर्भित स्रोतों में से एक है और अनुसंधान प्रसार का एक प्रमुख स्रोत था।

सबसे महत्वपूर्ण स्रोत से निकटता से संबंधित अन्य मीट्रिक भी हैं, जैसे "IEEE Access," "Electronics," और "Sensors," जिन्हें सबसे प्रमुख स्रोत के साथ सह-उद्धृत भी किया गया था। इन पत्रिकाओं की कंप्यूटर, इलेक्ट्रॉनिक्स और उभरती प्रौद्योगिकियों में एक मजबूत प्रतिष्ठा है। विशिष्ट स्रोत, जैसे कि "PLOS ONE," "2020 IEEE इंटेलिजेंट ऑन डिपेंडेबल,' और मानचित्र के किनारे पर स्थित विभिन्न अंतर्राष्ट्रीय सम्मेलन कार्यवाही, मुख्य क्लस्टर स्रोतों से बहुत अधिक जुड़े नहीं हैं, जो विशेषज्ञता के एक क्षेत्र का सुझाव देता है जो अधिक अनन्य या अंतःविषय है। मानचित्रण ने प्रौद्योगिकी, अपराध और सामाजिक प्रथाओं पर केंद्रित बढ़ती अंतःविषयता को भी दर्शाया है, विशेष रूप से उन स्रोतों के माध्यम से जो इलेक्ट्रॉनिक्स को अपराध विज्ञान और संगठित अपराध से जोड़ते हैं। यह शोधकर्ताओं द्वारा सामाजिक और व्यवहार विज्ञान के साथ तकनीकी अनुसंधान को जोड़ने के लिए बढ़े हुए प्रयास का प्रतिनिधित्व करता है।

3. देशों का सह-लेखन

चित्र 3 यह समझने में मदद करता है कि किस प्रकार देश सह-लेखक या सहयोगी प्रकाशनों के माध्यम से जुड़े हुए हैं, जो विद्वान समुदाय के सह-सहयोग नेटवर्क में प्रदर्शित अंतर्राष्ट्रीय सहयोग की सीमा (या गहराई) को दर्शाता है। मानचित्रण ने इंग्लैंड को इस सह-लेखन 'मानचित्र' का केंद्रबिंदु बनाया, जो अंतर्राष्ट्रीय सहयोग के लिए एक प्रमुख केंद्र का सुझाव देता है, विशेष रूप से भारत, यूएसए, पाकिस्तान, सऊदी अरब और ऑस्ट्रेलिया के साथ सह-लेखन संबंधों के साथ। यह केंद्रीय स्थान बताता है कि शोधकर्ता या संस्थान साइबर अपराध अनुसंधान के एक सहयोगी निकाय के साथ जुड़े हुए थे और यथा संभव कई क्षेत्रों में उत्पादक शैक्षणिक संबंध विकसित किए।

यूएसए एक प्रमुख वैश्विक सहयोगी खिलाड़ी भी है, जैसा कि इंग्लैंड (जैसा कि पहले उल्लेख किया गया है), इज़राइल, जर्मनी और चेक गणराज्य के साथ इसके सुविकसित संबंधों से प्रमाणित होता है।



चित्र 2 — सबसे अधिक चुने गए स्रोत

चित्र 3 — देशों का सह-लेखन पैटर्न

नेटवर्क के इस विशेष मानचित्रण ने न केवल यूएसए को वैश्विक साइबर अपराध अनुसंधान में एक खिलाड़ी के रूप में पहचाना, बल्कि बहुपक्षीय परियोजनाओं में यूएसए की भागीदारी का भी संकेत दिया, विशेष रूप से तुलनीय पश्चिमी और मध्य यूरोपीय देशों (इज़राइल सहित) के साथ।

भारत इस मानचित्र में एक और केंद्रीय नोड है, जो पाकिस्तान, सऊदी अरब, ऑस्ट्रेलिया, दक्षिण कोरिया और इंग्लैंड जैसे देशों के साथ संबंध स्थापित करता है, जहाँ कनेक्शनों का घनत्व वैश्विक साइबर अपराध अनुसंधान नेटवर्क में विकासशील निवेश को दर्शाता है, विशेष रूप से एशिया और राष्ट्रमंडल राज्यों में। छोटे नोड्स का प्रतिनिधित्व नाइजीरिया, फ्रांस, मलेशिया, कनाडा और पीपुल्स रिपब्लिक ऑफ चाइना कर रहे हैं। सभी छोटे और कम कनेक्शन लेकिन फिर भी महत्वपूर्ण - चुनिंदा या विकासशील अनुसंधान नेटवर्क में भागीदारी का संकेत देते हैं। सहयोगी नेटवर्क के केंद्र में विशेष रूप से नहीं होने पर, उनकी उपस्थिति साइबर अपराध अनुसंधान में बढ़ी हुई वैश्विक रुचि को इंगित करती है।

मानचित्रण साइबर अपराध अनुसंधान पर सहयोग करने वाले देशों के अधिक विविध और परस्पर जुड़े नेटवर्क का प्रतिनिधित्व करता है। इंग्लैंड, यूएसए और भारत सबसे केंद्रीय हैं, जो वैश्विक साझेदारी स्थापित करने में उनके महत्व और प्रभुत्व को दर्शाता है।

चर्चा और निष्कर्ष

विश्लेषण यह दर्शाता है कि 'साइबर अपराध' इस शोध क्षेत्र का केंद्रीय विषय है, और साइबर खतरों की जांच में कृत्रिम बुद्धिमत्ता, मशीन लर्निंग और व्यवहार विश्लेषण के बढ़ते परिचय ने बढ़े हुए एकीकरण का संकेत दिया। तकनीकी और अपराध संबंधी पहलुओं के बीच एक सहक्रियात्मक संबंध से उभरने वाले अंतःविषय अनुसंधान प्रवृत्तियाँ साहित्य में पाई गईं। ग्रंथसूची युग्मन विश्लेषण ने तकनीकी साहित्य में महत्वपूर्ण एकाग्रता का संकेत दिया, जिसमें जर्नल या सम्मेलन प्रकाशन (जैसे, IEEE एक्सेस और इलेक्ट्रॉनिक्स) शामिल हैं, जो उभरती प्रौद्योगिकियों पर एक मजबूत केंद्र का संकेत देते हैं।

सह-लेखक मानचित्रण ने एक मजबूत सहयोगी अंतरराष्ट्रीय उपस्थिति का भी संकेत दिया, जिसमें इंग्लैंड, यूएसए और भारत वैश्विक साइबर सुरक्षा अनुसंधान संरचना में महत्वपूर्ण योगदानकर्ता के रूप में उभरे। परिणाम साइबर अपराध पर अनुसंधान की चल रही और विकसित प्रकृति को उजागर करते हैं। जैसे-जैसे डिजिटल खतरे तेजी से जटिल होते जा रहे हैं, शिक्षाविदों को वास्तविक समय में उभरने वाली कमजोरियों का जवाब देते हुए विभिन्न विषयों में सहयोगात्मक रूप से काम करना चाहिए। यह अध्ययन साइबर सुरक्षा अनुसंधान के बौद्धिक और सहयोगी परिदृश्य की समझ को बढ़ाता है। यह भविष्य के अध्ययनों का आधार है जो लक्षित ज्ञान अंतराल को संबोधित करते हुए वैश्विक अनुसंधान गतिविधि नेटवर्क को बढ़ाता है।

संदर्भ

1. Ali, S., & Mushtaq, M. (2024). Publication pattern and research assessment of cyber security: A bibliometric study. IntechOpen. https://doi.org/10.5772/intechopen.1005272
2. Cloud Security Alliance. (2017). *Security guidance for critical areas of focus in cloud computing* (Version 4.0). https://cloudsecurityalliance.org
3. Hu, J., Li, N., Liu, X., Liang, J., & Yan, X. (2024). Bibliometric analysis of data security research. *Occupation and Professional Education*, 1(3).

4. Khurana, P., Narula, S., Tiwari, N., Kapoor, R., & Arora, M. (2022). Bibliometric analysis on cybersecurity. I*nternational Journal of Experimental Research and Review*, 46, 202-211.
5. National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity* (Version 1.1). U.S. Department of Commerce. https://doi.org/10.6028/NIST.CSWP.04162018
6. Nobanee, H., Alodat, A., Bajodah, R., Al-Ali, M., & Al Darmaki, A. (2023). Bibliometric analysis of cybercrime and cybersecurity risks literature. *Journal of Financial Crime*, 30(6), 1736-1754. https://doi.org/10.1108/JFC-03-2023-0070
7. Pfleeger, C. P., Pfleeger, S. L., & Margulies, J. (2015). *Security in computing* (5th ed.). Pearson.
8. Rose, S., Borchert, O., Mitchell, S., & Connelly, S. (2020). *Zero trust architecture* (NIST Special Publication 800-207). National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-207
9. Sarker, I. H., Janicke, H., Mohsin, A., Gill, A., & Maglaras, L. (2024). Explainable AI for cybersecurity automation, intelligence and trustworthiness in digital twin: Methods, taxonomy, challenges and prospects. *ICT Express*, 10(4), 935-958. https://doi.org/10.1016/j.icte.2023.07.009
10. Verizon. (2023). *Data breach investigations report* (*DBIR*): Public sector snapshot. https://www.verizon.com/business/resources/reports/dbir/
11. Wu, L., Peng, Q., & Lemke, M. (2023). Research trends in cybercrime and cybersecurity: A review based on Web of Science core collection database. I*nternational Journal of Cybersecurity Intelligence and Cybercrime*, 6(1), 5-28. https://doi.org/10.52306/03010720233