IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

साइबर सुरक्षा, युद्ध और मीडिया: एक त्रिकोणीय संबंध का विश्लेषण

Dr. Ambika Tripathi

Department of Defence and Strategic Studies, Deen Dayal Upadhyay Gorakhpur University, Gorakhpur.

सारांश (Abstract)

इक्कीसवीं सदी में साइबर स्पेस ने युद्ध, सुरक्षा और संचार के स्वरूप को मूल रूप से बदल दिया है। आज के समय में साइबर सुरक्षा, युद्ध और मीडिया के बीच एक गहरा और जटिल त्रिकोणीय संबंध विकसित हो चुका है। यह संबंध केवल तकनीकी या सैन्य स्तर तक सीमित नहीं है, बल्कि इसमें सूचना, विचारधारा, मनोविज्ञान और जनमत निर्माण की प्रक्रियाएँ भी शामिल हैं। आधुनिक युद्ध में साइबर हमले, सूचना युद्ध और मीडिया नैरेटिव एक साथ मिलकर कार्य करते हैं, जिससे शक्ति संतुलन और वैश्विक राजनीति प्रभावित होती है। यह शोध पत्र इन तीनों घटकों,साइबर सुरक्षा, युद्ध और मीडिया,की प्रकृति को स्पष्ट करते हुए उनके अंतर्संबंध का विश्लेषण प्रस्तुत करता है।

मुख्य शब्द (Keywords): साइबर सुरक्षा, युद्ध, मीडिया, सूचना युद्ध, दुष्प्रचार, डिजिटल संचार

1. प्रस्तावना (Introduction)

डिजिटल युग में सूचना और संचार तकनीकों के तीव्र विकास ने मानव समाज के लगभग सभी क्षेत्रों को गहराई से प्रभावित किया है। इंटरनेट, सोशल मीडिया, आर्टिफिशियल इंटेलिजेंस, क्लाउड कंप्यूटिंग और डेटा नेटवर्क जैसी आधुनिक तकनीकों ने न केवल संचार को तीव्र, सुलभ और वैश्विक बनाया है, बल्कि शक्ति, नियंत्रण और प्रभाव के नए आयाम भी स्थापित किए हैं। आज सूचना केवल ज्ञान का माध्यम नहीं रह गई है, बल्कि यह राजनीतिक, आर्थिक और सामरिक शक्ति का एक महत्वपूर्ण साधन बन चुकी है। इस परिवर्तन ने पारंपरिक संरचनाओं को चुनौती देते हुए एक नए डिजिटल वैश्विक परिदृश्य का निर्माण किया है, जहाँ सूचना का प्रवाह और उसका नियंत्रण अत्यंत निर्णायक भूमिका निभाते हैं।

इसी संदर्भ में युद्ध की पारंपरिक अवधारणा भी मूल रूप से परिवर्तित हो चुकी है। पहले युद्ध मुख्यतः भौतिक सीमाओं, सैन्य बलों और प्रत्यक्ष संघर्षों तक सीमित होता था, जिसमें हथियार, सैनिक और भौगोलिक क्षेत्र प्रमुख तत्व होते थे(अशरफ *et al.*, 2025)। किन्तु वर्तमान समय में युद्ध का स्वरूप अधिक जटिल, बहुआयामी और तकनीकी

हो गया है। अब संघर्ष केवल भूमि, जल या वायु तक सीमित नहीं रहा, बल्कि साइबर स्पेस एक नए और महत्वपूर्ण युद्धक्षेत्र के रूप में उभरकर सामने आया है। इस युद्धक्षेत्र की विशेषता यह है कि इसमें आक्रमण अदृश्य होते हैं, सीमाएँ स्पष्ट नहीं होतीं और हमलावर की पहचान करना अत्यंत कठिन होता है।

साइबर स्पेस में होने वाले हमले,जैसे डेटा चोरी, नेटवर्क बाधा, रैनसमवेयर और महत्वपूर्ण अवसंरचनाओं पर आक्रमण,किसी भी देश की आर्थिक, सामाजिक और राजनीतिक स्थिरता को गंभीर रूप से प्रभावित कर सकते हैं। इन हमलों के माध्यम से बिना किसी प्रत्यक्ष सैन्य कार्रवाई के भी विरोधी देश को कमजोर किया जा सकता है। इस प्रकार, साइबर युद्ध ने पारंपरिक युद्ध की सीमाओं को तोड़ते हुए शक्ति संघर्ष के एक नए आयाम को जन्म दिया है, जहाँ तकनीक और सूचना प्रमुख हथियार बन गए हैं।

इसके साथ ही, मीडिया की भूमिका में भी व्यापक परिवर्तन आया है। पारंपरिक रूप से मीडिया को सूचना प्रसार और जनजागरूकता का माध्यम माना जाता था, जो घटनाओं को निष्पक्ष रूप से प्रस्तुत करता था। किन्तु डिजिटल युग में मीडिया केवल सूचना देने वाला माध्यम नहीं रहा, बल्कि यह विचार निर्माण, धारणा निर्माण और जनमत को प्रभावित करने का एक शक्तिशाली उपकरण बन गया है(वेंगर *et al.*, 2022)। विशेष रूप से सोशल मीडिया प्लेटफॉर्म्स ने सूचना के प्रसार को इतना तेज और व्यापक बना दिया है कि किसी भी घटना का प्रभाव कुछ ही समय में वैश्विक स्तर पर देखा जा सकता है।

युद्ध के संदर्भ में मीडिया की यह भूमिका और अधिक महत्वपूर्ण हो जाती है। अब मीडिया केवल युद्ध की रिपोर्टिंग नहीं करता, बल्कि वह स्वयं युद्ध की रणनीति का हिस्सा बन चुका है। प्रचार, दुष्प्रचार, नैरेटिव निर्माण और मनोवैज्ञानिक प्रभाव उत्पन्न करने के लिए मीडिया का व्यापक उपयोग किया जाता है। इसके माध्यम से न केवल विरोधी पक्ष की छवि को प्रभावित किया जाता है, बल्कि अपने पक्ष को भी वैधता और समर्थन प्रदान किया जाता है। इस प्रकार, मीडिया युद्ध के परिणामों को प्रभावित करने में एक सक्रिय भूमिका निभाता है।

इन परिवर्तनों के परिणामस्वरूप साइबर सुरक्षा, युद्ध और मीडिया के बीच एक गहरा और जटिल त्रिकोणीय संबंध विकसित हुआ है। यह संबंध केवल तीन अलग-अलग क्षेत्रों का संयोजन नहीं है, बल्कि यह एक ऐसी परस्पर जुड़ी हुई संरचना है, जिसमें प्रत्येक घटक अन्य दो को प्रभावित करता है और उनसे प्रभावित होता है। साइबर हमले युद्ध की रणनीतियों का हिस्सा बनते हैं, मीडिया उन हमलों के प्रभाव को बढ़ाता है, और सूचना के माध्यम से जनमत को प्रभावित किया जाता है, जो आगे चलकर राजनीतिक और सैन्य निर्णयों को प्रभावित करता है।

इस प्रकार, आधुनिक वैश्विक परिदृश्य को समझने के लिए इस त्रिकोणीय संबंध का विश्लेषण अत्यंत आवश्यक हो जाता है। यह न केवल युद्ध के बदलते स्वरूप को स्पष्ट करता है, बल्कि यह भी दर्शाता है कि सूचना, तकनीक और मीडिया किस प्रकार मिलकर शक्ति, नियंत्रण और प्रभाव के नए ढांचे का निर्माण कर रहे हैं।

2. साइबर सुरक्षा: अवधारणा और स्वरूप

साइबर सुरक्षा का अर्थ डिजिटल प्रणालियों, नेटवर्क, डेटा तथा सूचना को अनधिकृत पहुँच, दुरुपयोग, हमलों और क्षति से सुरक्षित रखना है(खान *et al.*, 2025)। यह अवधारणा केवल तकनीकी सुरक्षा तक सीमित नहीं है, बल्कि इसका दायरा राष्ट्रीय सुरक्षा, आर्थिक स्थिरता, सामाजिक संरचना और व्यक्तिगत गोपनीयता तक विस्तृत है। डिजिटल

युग में जहाँ लगभग हर गतिविधि,चाहे वह संचार हो, वित्तीय लेन-देन हो, प्रशासनिक कार्य हों या सैन्य संचालन,किसी न किसी रूप में साइबर स्पेस पर निर्भर हो गई है, वहाँ साइबर सुरक्षा की आवश्यकता और भी अधिक महत्वपूर्ण हो जाती है।

साइबर सुरक्षा की मूलभूत अवधारणा तीन प्रमुख तत्वों पर आधारित मानी जाती है: गोपनीयता (Confidentiality), अखंडता (Integrity) और उपलब्धता (Availability)। गोपनीयता का तात्पर्य यह सुनिश्चित करना है कि संवेदनशील जानकारी केवल अधिकृत व्यक्तियों तक ही सीमित रहे। अखंडता का अर्थ है कि डेटा में किसी प्रकार का अनधिकृत परिवर्तन न हो, जबकि उपलब्धता यह सुनिश्चित करती है कि आवश्यक समय पर सूचना और प्रणालियाँ सुचारु रूप से उपलब्ध रहें। इन तीनों तत्वों के संतुलन के बिना किसी भी डिजिटल प्रणाली को सुरक्षित नहीं माना जा सकता।

साइबर सुरक्षा के अंतर्गत विभिन्न प्रकार के खतरे और हमले आते हैं, जो समय के साथ अधिक जटिल और परिष्कृत होते जा रहे हैं। हैकिंग के माध्यम से अनधिकृत व्यक्ति या समूह किसी सिस्टम में प्रवेश कर संवेदनशील जानकारी प्राप्त कर सकते हैं या उसे नुकसान पहुँचा सकते हैं। डेटा चोरी (Data Breach) के मामलों में व्यक्तिगत, वित्तीय या सरकारी जानकारी का दुरुपयोग किया जाता है, जिससे न केवल व्यक्तियों बल्कि संस्थानों की विश्वसनीयता भी प्रभावित होती है।

रैनसमवेयर हमले विशेष रूप से गंभीर होते हैं, जिनमें हमलावर किसी सिस्टम या डेटा को लॉक कर देते हैं और उसे पुनः प्राप्त करने के लिए धन की मांग करते हैं। इसी प्रकार फ़िशिंग हमलों में उपयोगकर्ताओं को धोखे से संवेदनशील जानकारी साझा करने के लिए प्रेरित किया जाता है, जबकि DDoS (Distributed Denial of Service) हमलों के माध्यम से किसी वेबसाइट या नेटवर्क को अत्यधिक ट्रैफिक भेजकर निष्क्रिय कर दिया जाता है। ये सभी हमले यह दर्शाते हैं कि साइबर खतरों की प्रकृति कितनी विविध और व्यापक हो चुकी है।

महत्वपूर्ण बात यह है कि ये साइबर हमले केवल व्यक्तिगत स्तर तक सीमित नहीं रहते, बल्कि इनका प्रभाव व्यापक संस्थागत और राष्ट्रीय स्तर पर भी देखा जाता है। सरकारों, सैन्य संस्थानों, बैंकिंग प्रणालियों, स्वास्थ्य सेवाओं, ऊर्जा नेटवर्क और परिवहन प्रणालियों जैसी महत्वपूर्ण अवसंरचनाएँ साइबर हमलों का प्रमुख लक्ष्य बनती जा रही हैं। इन क्षेत्रों पर हमला किसी देश की कार्यप्रणाली को बाधित कर सकता है और सामाजिक अस्थिरता उत्पन्न कर सकता है।

आधुनिक समय में साइबर सुरक्षा एक रणनीतिक क्षेत्र के रूप में उभरकर सामने आई है। अब यह केवल तकनीकी विशेषज्ञों का विषय नहीं रहा, बल्कि यह राष्ट्रीय नीतियों और अंतरराष्ट्रीय संबंधों का एक महत्वपूर्ण हिस्सा बन चुका है। कई देश अपनी साइबर क्षमताओं को मजबूत करने के लिए विशेष साइबर कमांड, सुरक्षा एजेंसियाँ और नीतिगत ढाँचे विकसित कर रहे हैं। इसका कारण यह है कि साइबर स्पेस में किया गया हमला बिना किसी पारंपरिक सैन्य संघर्ष के भी अत्यधिक प्रभाव उत्पन्न कर सकता है।

इस संदर्भ में साइबर सुरक्षा और साइबर शक्ति (Cyber Power) का संबंध भी महत्वपूर्ण हो जाता है। जिस देश की डिजिटल अवसंरचना मजबूत और सुरक्षित होती है, वह न केवल अपने संसाधनों की रक्षा कर सकता है, बल्कि

साइबर स्पेस में रणनीतिक बढ़त भी प्राप्त कर सकता है। इसके विपरीत, कमजोर साइबर सुरक्षा वाले देश बाहरी हमलों के प्रति अधिक संवेदनशील होते हैं, जिससे उनकी संप्रभुता और स्थिरता पर खतरा उत्पन्न हो सकता है।

अतः यह स्पष्ट है कि साइबर सुरक्षा केवल तकनीकी उपायों का समूह नहीं है, बल्कि यह एक व्यापक और बहुआयामी अवधारणा है, जो आधुनिक समाज के सुचारु संचालन और सुरक्षा के लिए अनिवार्य है। डिजिटल युग में इसकी प्रासंगिकता निरंतर बढ़ती जा रही है, और यह भविष्य के वैश्विक शक्ति संतुलन को निर्धारित करने वाले प्रमुख कारकों में से एक बन चुकी है।

3. युद्ध का बदलता स्वरूप (Nature of Modern Warfare)

युद्ध की पारंपरिक अवधारणा, जिसमें सैनिकों, हथियारों और भौतिक सीमाओं के भीतर प्रत्यक्ष संघर्ष प्रमुख होता था, समय के साथ एक व्यापक और बहुआयामी रूप में परिवर्तित हो चुकी है। पूर्व में युद्ध मुख्यतः दो या अधिक राष्ट्रों के बीच सैन्य शक्ति के प्रदर्शन और भौगोलिक नियंत्रण के लिए लड़ा जाता था, जहाँ विजय का निर्धारण क्षेत्रीय अधिग्रहण, सैन्य क्षति और राजनीतिक प्रभुत्व के आधार पर किया जाता था। किन्तु इक्कीसवीं सदी में तकनीकी प्रगति और डिजिटल क्रांति ने इस पारंपरिक ढांचे को मूल रूप से बदल दिया है।

आधुनिक युद्ध अब केवल भौतिक युद्धक्षेत्रों तक सीमित नहीं रहा, बल्कि साइबर स्पेस एक नए और अत्यंत महत्वपूर्ण युद्धक्षेत्र के रूप में उभरकर सामने आया है(क्लार *et al.*, 2025)। साइबर युद्ध के माध्यम से किसी भी देश की महत्वपूर्ण डिजिटल अवसंरचनाओं,जैसे संचार प्रणाली, ऊर्जा नेटवर्क, बैंकिंग प्रणाली, परिवहन व्यवस्था और सैन्य सूचना तंत्र,को लक्ष्य बनाया जा सकता है। इन प्रणालियों पर आक्रमण करके किसी देश की कार्यक्षमता को बाधित किया जा सकता है, जिससे उसकी आर्थिक और सामाजिक संरचना पर गंभीर प्रभाव पड़ता है।

साइबर युद्ध की एक प्रमुख विशेषता यह है कि इसमें प्रत्यक्ष भौतिक टकराव आवश्यक नहीं होता। हमलावर दूर बैठकर ही डिजिटल माध्यमों से अपने लक्ष्य को प्रभावित कर सकता है, जिससे युद्ध की पारंपरिक सीमाएँ और परिभाषाएँ धुंधली हो जाती हैं। इसके अतिरिक्त, साइबर हमलों की पहचान करना और उनके स्रोत का पता लगाना अत्यंत कठिन होता है, जिससे जवाबी कार्रवाई (retaliation) और जिम्मेदारी निर्धारण (attribution) जटिल हो जाते हैं। यह अनिश्चितता आधुनिक युद्ध को और अधिक चुनौतीपूर्ण बनाती है।

आधुनिक युद्ध के स्वरूप में एक और महत्वपूर्ण परिवर्तन "हाइब्रिड युद्ध" की अवधारणा के रूप में सामने आया है। हाइब्रिड युद्ध वह स्थिति है, जिसमें पारंपरिक सैन्य शक्ति के साथ-साथ साइबर हमले, सूचना युद्ध, आर्थिक दबाव और मनोवैज्ञानिक रणनीतियों का समन्वित उपयोग किया जाता है। इस प्रकार का युद्ध किसी एक माध्यम तक सीमित नहीं होता, बल्कि विभिन्न रणनीतियों के संयोजन के माध्यम से संचालित किया जाता है, जिससे विरोधी पक्ष को बहुआयामी स्तर पर कमजोर किया जा सके।

सूचना युद्ध (Information Warfare) भी आधुनिक युद्ध का एक महत्वपूर्ण घटक बन चुका है। इसमें मीडिया और डिजिटल प्लेटफॉर्म्स के माध्यम से सूचना का नियंत्रण, दुष्प्रचार और नैरेटिव निर्माण किया जाता है। इसका उद्देश्य केवल जानकारी देना नहीं, बल्कि लोगों की सोच, विश्वास और व्यवहार को प्रभावित करना होता है। इस प्रकार, युद्ध अब केवल युद्धक्षेत्र में नहीं, बल्कि समाज और जनमानस के भीतर भी लड़ा जाता है।

इसके अतिरिक्त, आधुनिक युद्ध में गैर-राज्यीय तत्वों की भूमिका भी बढ़ गई है। पहले युद्ध मुख्यतः राष्ट्र-राज्यों के बीच होता था, किन्तु अब हैकर समूह, आतंकवादी संगठन, निजी कंपनियाँ और अन्य संगठन भी युद्ध जैसी गतिविधियों में सक्रिय भूमिका निभा रहे हैं। यह परिवर्तन युद्ध के स्वरूप को और अधिक जटिल और अप्रत्याशित बना देता है, क्योंकि इन तत्वों को नियंत्रित करना और उनके कार्यों की जिम्मेदारी तय करना कठिन होता है।

तकनीकी प्रगति, विशेष रूप से आर्टिफिशियल इंटेलिजेंस, मशीन लर्निंग और स्वचालित प्रणालियों का उपयोग, आधुनिक युद्ध को और अधिक उन्नत और प्रभावशाली बना रहा है। ड्रोन, स्वायत्त हथियार प्रणाली और साइबर टूल्स के माध्यम से युद्ध की गति, सटीकता और प्रभाव में वृद्धि हुई है। इसके साथ ही, डिजिटल प्लेटफॉर्म्स के माध्यम से वास्तविक समय में जानकारी का आदान-प्रदान युद्ध की रणनीतियों को और अधिक गतिशील बना देता है।

इस प्रकार, यह स्पष्ट है कि आधुनिक युद्ध अब केवल हथियारों और सैनिकों का संघर्ष नहीं रह गया है, बल्कि यह सूचना, तकनीक, मनोविज्ञान और रणनीति का एक समन्वित रूप बन चुका है(बाकीरोव *et al.*, 2025)। साइबर स्पेस और सूचना माध्यमों के बढ़ते महत्व ने युद्ध को एक ऐसे जटिल तंत्र में परिवर्तित कर दिया है, जिसमें पारंपरिक और आधुनिक दोनों तत्व एक साथ कार्य करते हैं। इसलिए, आधुनिक युद्ध को समझने के लिए इसके इस बहुआयामी स्वरूप का विश्लेषण अत्यंत आवश्यक हो जाता है।

4. मीडिया: सूचना से रणनीति तक

मीडिया की भूमिका समय के साथ अत्यधिक परिवर्तनशील रही है, और डिजिटल युग में यह परिवर्तन और भी अधिक स्पष्ट रूप से सामने आया है। पारंपरिक रूप से मीडिया को सूचना के प्रसार का माध्यम माना जाता था, जिसका मुख्य उद्देश्य घटनाओं, विचारों और तथ्यों को समाज तक पहुँचाना था। समाचार पत्र, रेडियो और टेलीविजन जैसे माध्यमों के माध्यम से जनता को जानकारी प्रदान की जाती थी, और मीडिया को लोकतांत्रिक व्यवस्था का एक महत्वपूर्ण स्तंभ माना जाता था। किन्तु वर्तमान समय में मीडिया की भूमिका केवल सूचना देने तक सीमित नहीं रह गई है, बल्कि यह विचार निर्माण, धारणा निर्माण और जनमत को प्रभावित करने का एक अत्यंत शक्तिशाली उपकरण बन चुका है।

डिजिटल क्रांति ने मीडिया के स्वरूप को मूल रूप से बदल दिया है। सोशल मीडिया प्लेटफॉर्म्स, ऑनलाइन समाचार पोर्टल्स, ब्लॉग्स और वीडियो साझा करने वाले प्लेटफॉर्म्स ने सूचना के प्रसार को अत्यंत तेज, सुलभ और वैश्विक बना दिया है। अब कोई भी सूचना कुछ ही क्षणों में लाखों लोगों तक पहुँच सकती है। इस तीव्रता और व्यापकता ने मीडिया की शक्ति को कई गुना बढ़ा दिया है, किन्तु इसके साथ ही नई चुनौतियाँ भी उत्पन्न हुई हैं, विशेष रूप से सूचना की सत्यता और विश्वसनीयता के संदर्भ में।

युद्ध के संदर्भ में मीडिया की भूमिका और भी अधिक महत्वपूर्ण और रणनीतिक हो जाती है। आधुनिक युद्ध में मीडिया केवल घटनाओं का वर्णन करने वाला माध्यम नहीं है, बल्कि यह स्वयं युद्ध की रणनीति का एक अभिन्न हिस्सा बन चुका है(लिंडसे *et al.*, 2025)। युद्ध के दौरान मीडिया का उपयोग विभिन्न उद्देश्यों की पूर्ति के लिए किया जाता है, जो सीधे तौर पर युद्ध की दिशा और परिणाम को प्रभावित कर सकते हैं।

सबसे पहले, मीडिया सूचना प्रसार का कार्य करता है, जिसके माध्यम से जनता को युद्ध से संबंधित घटनाओं, परिस्थितियों और निर्णयों की जानकारी मिलती है। यह भूमिका लोकतांत्रिक समाज में अत्यंत महत्वपूर्ण होती है, क्योंकि इसके माध्यम से पारदर्शिता और जागरूकता बनी रहती है।

दूसरे, मीडिया का उपयोग प्रचार (propaganda) के रूप में किया जाता है, जिसके माध्यम से किसी देश या समूह के दृष्टिकोण को सकारात्मक रूप में प्रस्तुत किया जाता है। इसमें अपने सैन्य कार्यों को उचित ठहराना, राष्ट्रीय भावना को प्रोत्साहित करना और जनता का समर्थन प्राप्त करना शामिल होता है।

तीसरे, दुष्प्रचार (disinformation) आधुनिक मीडिया रणनीति का एक महत्वपूर्ण पहलू बन चुका है। इसके अंतर्गत जानबूझकर गलत या भ्रामक जानकारी फैलाकर विरोधी पक्ष की छवि को कमजोर करने का प्रयास किया जाता है। यह प्रक्रिया विशेष रूप से सोशल मीडिया के माध्यम से तेज़ी से संचालित होती है, जहाँ सूचना की सत्यता की जाँच करना कठिन होता है।

चौथे, मीडिया जनमत निर्माण में महत्वपूर्ण भूमिका निभाता है। सूचना के चयन, प्रस्तुति और विश्लेषण के माध्यम से लोगों की सोच, दृष्टिकोण और निर्णयों को प्रभावित किया जाता है। इस प्रकार मीडिया केवल जानकारी नहीं देता, बल्कि यह यह भी तय करता है कि लोग उस जानकारी को किस प्रकार समझेंगे और उस पर कैसी प्रतिक्रिया देंगे।

इसके अतिरिक्त, मीडिया का मनोवैज्ञानिक प्रभाव भी अत्यंत महत्वपूर्ण होता है। युद्ध के दौरान भावनात्मक सामग्री, दृश्य चित्रण और कथानक (narratives) के माध्यम से लोगों में भय, राष्ट्रवाद या सहानुभूति जैसी भावनाएँ उत्पन्न की जाती हैं। यह मनोवैज्ञानिक प्रभाव युद्ध की रणनीति का एक महत्वपूर्ण हिस्सा होता है, क्योंकि इसके माध्यम से सामाजिक व्यवहार और जनसमर्थन को नियंत्रित किया जा सकता है।

डिजिटल मीडिया के संदर्भ में एल्गोरिदम और सामग्री के निजीकरण (personalization) की भूमिका भी महत्वपूर्ण हो जाती है। उपयोगकर्ताओं को उनकी रुचियों और पूर्वाग्रहों के अनुसार सामग्री दिखाई जाती है, जिससे वे एक ही प्रकार की जानकारी के संपर्क में रहते हैं। इससे "इको चैंबर" की स्थिति उत्पन्न होती है, जहाँ विभिन्न दृष्टिकोणों के बीच संवाद कम हो जाता है और ध्रुवीकरण बढ़ता है।

इस प्रकार, यह स्पष्ट है कि मीडिया अब केवल एक निष्क्रिय दर्शक या सूचना वाहक नहीं रहा, बल्कि यह आधुनिक युद्ध का एक सक्रिय और प्रभावशाली घटक बन चुका है। यह न केवल सूचना के प्रवाह को नियंत्रित करता है, बल्कि युद्ध की दिशा, रणनीति और परिणाम को भी प्रभावित करने की क्षमता रखता है।

आधुनिक वैश्विक परिदृश्य में साइबर सुरक्षा, युद्ध और मीडिया के बीच एक गहरा, जटिल और परस्पर निर्भर त्रिकोणीय संबंध विकसित हो चुका है। यह संबंध केवल तीन अलग-अलग क्षेत्रों का संयोजन नहीं है, बल्कि एक ऐसी गतिशील संरचना है जिसमें प्रत्येक घटक अन्य दो को प्रभावित करता है और उनसे प्रभावित होता है। डिजिटल युग में सूचना, तकनीक और संचार के समन्वय ने इस त्रिकोण को और अधिक सशक्त तथा प्रभावशाली बना दिया है। इस संबंध को समझे बिना आधुनिक युद्ध, सुरक्षा रणनीतियों और वैश्विक शक्ति संरचना का समुचित विश्लेषण संभव नहीं है।

4.5 केस स्टडीज़ (Case Studies)

नीचे दो समकालीन एवं प्रासंगिक केस-स्टडीज़ दी जा रही हैं, जिनका समावेशन लेख को सिद्धांतात्मक विश्लेषण से वास्तविक दृष्टांतों तक ले जाता है और पाठक को यह स्पष्ट करने में मदद करेगा कि कैसे साइबर हमले, मीडिया-नैरेटिव और मनोवैज्ञानिक रणनीतियाँ वास्तविक संघर्षों में परस्पर जुड़ी हैं।

4.5.1 रूस-यूक्रेन संघर्ष

रूस-यूक्रेन संघर्ष में साइबर गतिविधियाँ और हैक्टिविज़्म युद्ध के सहायक आयाम बन गए हैं। 2022–2023 से शुरू हुई साइबरराजनीति में दोनों ओर सक्रिय हैक-ग्रुप्स, DDoS हमले, डेटा-लीक और डिजिटल सर्विसेज पर सीधी चोट जैसी रणनीतियाँ देखने को मिलीं। साथ ही, सोशल मीडिया और डिजिटल प्लेटफ़ॉर्म पर फैलने वाली सूचनाओं ने युद्ध-नैरेटिव को तेज़ी से आकार दिया,जहाँ कुछ मामलों में गलत सूचनाएँ और लीक किए गए दस्तावेज़ युद्ध के तुरन्त बाद के राजनैतिक और आर्थिक निर्णयों को प्रभावित कर गए। इस संघर्ष में हैक्टिविज़्म और राज्य-समर्थित/अनौपचारिक समूहों के क्रियाकलापों ने पारंपरिक सैन्य कार्रवाई के साथ-साथ डिजिटल फ्रंट को भी निर्णायक बनाया।

4.5.2 इज़राइल-हमास संघर्ष

अक्टूबर 2023 के बाद के इज़राइल-हमास वाक्यों में न केवल पारम्परिक सैन्य अभियानों बल्कि व्यापक सूचना-अभियानों और हाइब्रिड साइबर-गति-विधियों का भी प्रयोग हुआ। इस संघर्ष में सोशल मीडिया पर दुष्प्रचार और मिसइन्फ़ोर्मेशन का तीव्र प्रसार देखा गया,कई वायरल वीडियो/छवियों के मामलों में रिपोर्टिंग-फैक्ट-चेक से असहमति मिली और मीडिया-नैरेटिव ने त्वरित रूप से अंतरराष्ट्रीय विचार को प्रभावित किया। साथ ही कुछ रिपोर्टों में आरोप लगे कि मीडिया कर्मियों तथा समाचार सामग्री के खिलाफ लक्षित मानचित्रण और प्रचारात्मक रणनीतियाँ संचालित हुईं , यह बताता है कि किस तरह मीडिया-नैरेटिव को सैन्य वैधता और अंतरराष्ट्रीय समर्थन हेतु उपकरण के रूप में प्रयोग किया गया।

5.1 परस्पर निर्भरता (Interdependence)

साइबर सुरक्षा, युद्ध और मीडिया के बीच गहरी परस्पर निर्भरता विद्यमान है। साइबर हमले आधुनिक युद्ध की रणनीतियों का एक महत्वपूर्ण हिस्सा बन चुके हैं, जिनके माध्यम से विरोधी पक्ष की डिजिटल अवसंरचना को बाधित किया जाता है। इन हमलों का प्रभाव केवल तकनीकी स्तर तक सीमित नहीं रहता, बल्कि मीडिया के माध्यम से यह व्यापक सामाजिक और राजनीतिक स्तर पर भी प्रसारित होता है।

मीडिया इन साइबर घटनाओं को जनता तक पहुँचाता है, जिससे उनका प्रभाव कई गुना बढ़ जाता है। किसी साइबर हमले की सूचना जब व्यापक स्तर पर प्रसारित होती है, तो वह केवल एक तकनीकी घटना नहीं रह जाती, बल्कि वह जनचर्चा, राजनीतिक विमर्श और अंतरराष्ट्रीय संबंधों को प्रभावित करने वाली घटना बन जाती है(नासिर *et al.*, 2024)। दूसरी ओर, मीडिया के माध्यम से प्रसारित सूचनाएँ और नैरेटिव भी साइबर रणनीतियों को प्रभावित करते हैं, क्योंकि राज्य और अन्य तत्व इन सूचनाओं के आधार पर अपनी नीतियाँ और प्रतिक्रियाएँ निर्धारित करते हैं। इस प्रकार, यह स्पष्ट होता है कि ये तीनों घटक एक-दूसरे के साथ निरंतर अंतःक्रिया में रहते हैं।

5.2 सूचना युद्ध और दुष्प्रचार

आधुनिक युद्ध में सूचना सबसे शक्तिशाली हथियार के रूप में उभरी है। सूचना युद्ध (Information Warfare) के अंतर्गत केवल तथ्यात्मक जानकारी का आदान-प्रदान नहीं होता, बल्कि इसका उपयोग रणनीतिक उद्देश्यों की पूर्ति के लिए किया जाता है। दुष्प्रचार (Disinformation) इस प्रक्रिया का एक महत्वपूर्ण हिस्सा है, जिसमें जानबूझकर गलत या भ्रामक जानकारी फैलाकर विरोधी पक्ष को कमजोर करने और जनता की सोच को प्रभावित करने का प्रयास किया जाता है।

डिजिटल मीडिया, विशेष रूप से सोशल मीडिया प्लेटफॉर्म्स, इस प्रक्रिया को अत्यंत तीव्र और व्यापक बना देते हैं। यहाँ सूचना कुछ ही समय में लाखों लोगों तक पहुँच जाती है, और उसकी सत्यता की जाँच करना कठिन हो जाता है। इस स्थिति में दुष्प्रचार तेजी से फैलता है और लोगों की धारणाओं को प्रभावित करता है। परिणामस्वरूप, युद्ध केवल भौतिक स्तर पर नहीं, बल्कि विचारों और मानसिकता के स्तर पर भी लड़ा जाता है(बुखारी *et al.*, 2025)। यह एक ऐसा संघर्ष बन जाता है, जिसमें लक्ष्य विरोधी पक्ष के मनोबल, विश्वास और सामाजिक एकता को कमजोर करना होता है।

5.3 मनोवैज्ञानिक प्रभाव

साइबर गतिविधियों और मीडिया के संयुक्त प्रभाव से उत्पन्न मनोवैज्ञानिक प्रभाव आधुनिक युद्ध की एक महत्वपूर्ण विशेषता है। दुष्प्रचार, भावनात्मक सामग्री और चयनात्मक सूचना के माध्यम से लोगों में भय, भ्रम, असुरक्षा और अविश्वास की भावना उत्पन्न की जाती है। यह प्रक्रिया मनोवैज्ञानिक युद्ध (Psychological Warfare) का हिस्सा होती है, जिसका उद्देश्य समाज को भीतर से अस्थिर करना और उसकी सामूहिक चेतना को प्रभावित करना होता है।

जब किसी समाज में लगातार नकारात्मक या भ्रामक सूचनाएँ प्रसारित होती हैं, तो लोगों के बीच असहमति, संदेह और तनाव बढ़ने लगता है। इससे सामाजिक एकता कमजोर होती है और निर्णय लेने की क्षमता प्रभावित होती है। इस प्रकार, बिना किसी प्रत्यक्ष सैन्य संघर्ष के भी समाज को कमजोर किया जा सकता है, जो आधुनिक युद्ध की एक महत्वपूर्ण रणनीति बन चुकी है।

5.4 शक्ति और नियंत्रण का नया स्वरूप

इस त्रिकोणीय संबंध के माध्यम से शक्ति और नियंत्रण की अवधारणा में भी महत्वपूर्ण परिवर्तन आया है। पारंपरिक रूप से शक्ति का संबंध सैन्य बल, संसाधनों और भौगोलिक नियंत्रण से जोड़ा जाता था, किन्तु डिजिटल युग में सूचना पर नियंत्रण ही वास्तविक शक्ति का प्रमुख आधार बन गया है(उस्मान *et al.*, 2023)।

जो पक्ष सूचना के प्रवाह, उसके स्वरूप और उसके प्रसार को नियंत्रित करता है, वही जनमत, नीतियों और रणनीतियों को प्रभावित करने में सक्षम होता है। साइबर क्षमताएँ इस नियंत्रण को तकनीकी आधार प्रदान करती हैं, जबकि मीडिया इसे सामाजिक और राजनीतिक स्तर पर प्रभावी बनाता है। इस प्रकार, साइबर सुरक्षा, युद्ध और मीडिया मिलकर शक्ति के एक नए ढाँचे का निर्माण करते हैं, जिसमें भौतिक शक्ति के साथ-साथ सूचनात्मक शक्ति (informational power) का महत्व अत्यधिक बढ़ गया है।

अतः यह कहा जा सकता है कि इस त्रिकोणीय संबंध ने आधुनिक युद्ध और वैश्विक राजनीति के स्वरूप को पुनर्परिभाषित कर दिया है, जहाँ सूचना, तकनीक और संचार ही शक्ति के प्रमुख स्रोत बन गए हैं।

6. चुनौतियाँ (Challenges)

साइबर सुरक्षा, युद्ध और मीडिया के बीच स्थापित त्रिकोणीय संबंध जहाँ एक ओर आधुनिक शक्ति संरचना को परिभाषित करता है, वहीं दूसरी ओर यह अनेक जटिल और गंभीर चुनौतियों को भी जन्म देता है। ये चुनौतियाँ केवल तकनीकी या सैन्य स्तर तक सीमित नहीं हैं, बल्कि इनका प्रभाव कानूनी, सामाजिक, राजनीतिक और अंतरराष्ट्रीय स्तर तक विस्तृत है। डिजिटल युग में इन तीनों क्षेत्रों की परस्पर निर्भरता के कारण किसी एक क्षेत्र में उत्पन्न समस्या अन्य क्षेत्रों को भी प्रभावित करती है, जिससे इन चुनौतियों की प्रकृति और अधिक जटिल हो जाती है(हारून *et al.*, 2024)।

सबसे पहले, तकनीकी स्तर पर तेजी से बदलती प्रौद्योगिकी एक प्रमुख चुनौती के रूप में सामने आती है। नई-नई डिजिटल तकनीकों के विकास के साथ-साथ साइबर हमलों के स्वरूप भी अधिक उन्नत और जटिल होते जा रहे हैं। हैकिंग, रैनसमवेयर, आर्टिफिशियल इंटेलिजेंस आधारित हमले और स्वचालित साइबर टूल्स सुरक्षा तंत्र के लिए निरंतर चुनौती उत्पन्न करते हैं। चूँकि तकनीक निरंतर विकसित हो रही है, इसलिए सुरक्षा उपायों को भी लगातार अद्यतन करना आवश्यक हो जाता है। इसके अभाव में डिजिटल अवसंरचनाएँ हमलों के प्रति अधिक संवेदनशील हो जाती हैं।

दूसरी महत्वपूर्ण चुनौती कानूनी और नीतिगत स्तर पर देखने को मिलती है। साइबर स्पेस की सीमा-रहित प्रकृति के कारण विभिन्न देशों के कानूनों और नीतियों में असमानता एक बड़ी समस्या बन जाती है। साइबर अपराध अक्सर एक देश में बैठकर दूसरे देश को प्रभावित करते हैं, जिससे अपराधियों की पहचान और उनके खिलाफ कार्रवाई करना कठिन हो जाता है। इसके अतिरिक्त, साइबर हमलों की जिम्मेदारी तय करना (attribution) भी एक जटिल प्रक्रिया है, क्योंकि हमलावर अपनी पहचान छिपाने के लिए उन्नत तकनीकों का उपयोग करते हैं। इस प्रकार, एक सुसंगत और प्रभावी अंतरराष्ट्रीय कानूनी ढाँचे का अभाव इन चुनौतियों को और बढ़ा देता है।

मीडिया के स्तर पर दुष्प्रचार (disinformation) और फेक न्यूज एक गंभीर समस्या के रूप में उभरे हैं (मट्टीला *et al.*, 2022)। डिजिटल मीडिया प्लेटफॉर्म्स पर जानकारी का तीव्र प्रसार जहाँ एक ओर संचार को सशक्त बनाता है,

वहीं दूसरी ओर गलत और भ्रामक सूचनाओं के प्रसार को भी बढ़ावा देता है। दुष्प्रचार के माध्यम से जनमत को प्रभावित किया जाता है, जिससे लोकतांत्रिक प्रक्रियाएँ, जैसे चुनाव और नीति-निर्माण, प्रभावित हो सकते हैं। इसके परिणामस्वरूप समाज में अविश्वास, ध्रुवीकरण और अस्थिरता की स्थिति उत्पन्न होती है।

इसके अतिरिक्त, मनोवैज्ञानिक और सामाजिक स्तर पर भी अनेक चुनौतियाँ सामने आती हैं। लगातार नकारात्मक और भ्रामक सूचनाओं के संपर्क में रहने से लोगों में भय, भ्रम और असुरक्षा की भावना उत्पन्न होती है। इससे सामाजिक एकता कमजोर होती है और संस्थाओं पर विश्वास कम होता है। यह स्थिति किसी भी समाज की स्थिरता के लिए गंभीर खतरा बन सकती है।

अंतरराष्ट्रीय स्तर पर सहयोग की कमी भी एक महत्वपूर्ण चुनौती है। साइबर सुरक्षा, युद्ध और मीडिया की समस्याएँ वैश्विक प्रकृति की हैं, जिन्हें किसी एक देश द्वारा अकेले हल नहीं किया जा सकता। इसके लिए विभिन्न देशों के बीच सूचना साझा करने, संयुक्त रणनीतियाँ बनाने और सहयोगात्मक तंत्र विकसित करने की आवश्यकता होती है(रोमानोव्स *et al.*, 2024)। किन्तु राजनीतिक मतभेद, रणनीतिक प्रतिस्पर्धा और विश्वास की कमी इस सहयोग में बाधा उत्पन्न करते हैं।

इसके अलावा, निजी कंपनियों और तकनीकी प्लेटफॉर्म्स की भूमिका भी इस संदर्भ में महत्वपूर्ण हो जाती है। सोशल मीडिया कंपनियाँ और डिजिटल सेवा प्रदाता सूचना के प्रवाह को नियंत्रित करने में महत्वपूर्ण भूमिका निभाते हैं, किन्तु इनके लिए स्पष्ट नियामक ढाँचे का अभाव कई बार दुष्प्रचार और साइबर खतरों को बढ़ावा देता है। इस स्थिति में सरकारों, संस्थानों और निजी क्षेत्र के बीच संतुलन स्थापित करना एक चुनौतीपूर्ण कार्य बन जाता है।

अतः यह स्पष्ट है कि साइबर सुरक्षा, युद्ध और मीडिया के इस त्रिकोणीय संबंध से उत्पन्न चुनौतियाँ बहुआयामी और जटिल हैं। इनका प्रभाव केवल सुरक्षा तक सीमित नहीं है, बल्कि यह समाज, राजनीति और वैश्विक स्थिरता को भी प्रभावित करता है(फिरदौस *et al.*, 2022)। इसलिए इन चुनौतियों का समाधान एक समन्वित, बहुस्तरीय और अंतरराष्ट्रीय दृष्टिकोण के माध्यम से ही संभव है, अन्यथा यह संबंध वैश्विक सुरक्षा के लिए एक गंभीर और स्थायी चिंता का विषय बना रहेगा।

6.1 अंतरराष्ट्रीय कानून और 'ग्लोबल साइबर ट्रीटी' हेतु ठोस सिफारिशें

आधुनिक साइबर-जोखिमों के समाधान के लिए राष्ट्रीय प्रयास पर्याप्त नहीं हैं; इसलिए यह आवश्यक है कि बहुपक्षीय कानूनी तंत्र और सामूहिक संस्थागत तंत्र विकसित किए जाएँ। निम्नलिखित ठोस सुझाव दस्तावेज़ में जोड़े जाएँ:

1. **UN-आधारित नियमित और स्थायी मंच:** 2021–2025 के OEWG (Open-ended Working Group) ने स्थायी और संस्थागत संवाद की आवश्यकता पर जोर दिया है; लेख में यह उल्लेख करें और प्रस्ताव रखें कि भारत समेत सभी राज्यों के लिए एक पारदर्शी, समावेशी और तकनीकी-विशिष्ट UN-माध्यमिक मंच स्थायी होना चाहिए।
2. **वैश्विक साइबर-आपराधिकता संधि का समर्थन और ह्युमन-राइट्स-गाइडलाइंस:** हाल की UN Cybercrime Treaty पहल (UN Convention against Cybercrime) को संदर्भित करते हुए सुझाव दें कि किसी भी वैश्विक संधि में मानवाधिकारों, प्रेस-स्वतंत्रता और नागरिक गोपनीयता की स्पष्ट सुरक्षा व्यवस्था हो।

3. **State-Peer Review और Attribution-मेकैनिज़्म का प्रस्ताव:** एक पारदर्शी 'स्टेट साइबर-पियर-रिव्यू' तंत्र और स्वतंत्र तकनीकी attribution-फ्रेमवर्क की वकालत करें जिससे साइबर हमलों की जिम्मेदारी तय करने में सहायता मिले और गलत आरोपों/प्रचार से रक्षा हो सके। (इस अवधारणा पर कई NGO/विशेषज्ञों ने चर्चा की है।)

4. **Confidence-Building Measures (CBMs) और Crisis-Hotline:** राज्यों के बीच त्वरित सूचना-विनिमय हेतु तकनीकी CBMs और डिजिटल 'क्राइसिस-हॉटलाइन' जैसी प्रक्रियाओं को स्थापित करने का सुझाव दें ताकि प्रारंभिक मिसअट्रिब्यूशन और गलती से वृद्धि वाली तनाव-स्थितियों को रोका जा सके।

5. **निजी-क्षेत्र भागीदारी और प्लेटफ़ॉर्म जवाबदेही:** सोशल मीडिया प्लेटफ़ॉर्म और टेक कंपनियों को नियामक मानकों के अनुरूप पारदर्शी रिपोर्टिंग और फेक न्यूज़/दुष्प्रचार के खिलाफ जवाबदेही का दायित्व देते हुए उनके साथ साझेदारी की सलाह दें।

7. निष्कर्ष

साइबर सुरक्षा, युद्ध और मीडिया के बीच स्थापित त्रिकोणीय संबंध आधुनिक विश्व की एक महत्वपूर्ण वास्तविकता है। यह संबंध केवल तकनीकी या सैन्य नहीं, बल्कि सामाजिक, राजनीतिक और मनोवैज्ञानिक आयामों से भी जुड़ा हुआ है।

आधुनिक युद्ध में साइबर हमले, सूचना युद्ध और मीडिया रणनीतियाँ एक साथ मिलकर कार्य करती हैं, जिससे शक्ति संतुलन और जनमत दोनों प्रभावित होते हैं। मीडिया इस प्रक्रिया में एक केंद्रीय भूमिका निभाता है, जो सूचना को न केवल प्रसारित करता है, बल्कि उसे दिशा भी देता है।

अतः यह स्पष्ट है कि इस त्रिकोणीय संबंध को समझे बिना आधुनिक युद्ध और वैश्विक सुरक्षा को पूरी तरह समझा नहीं जा सकता। यह क्षेत्र भविष्य में और अधिक महत्वपूर्ण होता जाएगा, जहाँ सूचना, तकनीक और शक्ति का संबंध और गहरा होता जाएगा।

Reference list

1. इमरान, एल. और अली, आर.एफ., 2023. सैन्य-जनसंपर्क: क्लॉज़विट्ज़ की त्रिमूर्ति के संदर्भ में समकालीन सूचना युद्ध का अध्ययन। लाहौर इंस्टिट्यूट फॉर रिसर्च एंड एनालिसिस जर्नल, 1।
2. अशरफ, एन., 2025. साइबर युद्ध का विरोधाभास और क्लॉज़विट्ज़ की युद्ध की अवधारणा। NUST जर्नल ऑफ इंटरनेशनल पीस एंड स्टेबिलिटी, पृ. 17-29।
3. बेरोज़ाशविली, टी. तृतीय विश्व युद्ध: डिजिटल युग में सूचना युद्ध के नैतिक आयाम।
4. औरंगज़ेब, एम., उद्दीन, एस.एस., इरफान, एम., अज़ीज़, ज़ेड. और इक़्तिदार, ए., 2024. साइबर युद्ध और राष्ट्रीय सुरक्षा: यथार्थवाद के दृष्टिकोण से अमेरिका-चीन साइबर प्रतिद्वंद्विता का विश्लेषण और वैश्विक साइबर सुरक्षा शासन पर इसके प्रभाव। जर्नल ऑफ पॉलिटिकल स्टेबिलिटी आर्काइव, 2(4), पृ. 293-303।
5. वेंगर, ए. और कैवेल्टी, एम.डी., 2022. निष्कर्ष: बहुआयामी अनिश्चितता के संदर्भ में साइबर सुरक्षा राजनीति की अस्पष्टता। In: साइबर सिक्योरिटी पॉलिटिक्स (पृ. 239-266). Routledge।

6. खान, ज़ेड.एफ., 2025. साइबर युद्ध और अंतरराष्ट्रीय सुरक्षा: एक नया भू-राजनीतिक क्षितिज। द क्रिटिकल रिव्यू ऑफ सोशल साइंसेज स्टडीज, 3(2), पृ. 513-527।
7. त्रिथारा, डी., 2024. डिजिटल नीति की गतिशीलता: अंतरराष्ट्रीय संबंध सिद्धांत और वैश्विक प्लेटफॉर्म राजनीति की चुनौती।
8. शैंडलर, आर. और कैनेटी, डी., 2024. परिचय: साइबर-संघर्ष,अटकलों से जांच की ओर। जर्नल ऑफ पीस रिसर्च, 61(1), पृ. 3-9।
9. मेस्किटा, आर. और ब्रिटो, आर.एल., 2024. युद्ध, शब्द और संपत्ति: साइबर, डिजिटल और तकनीकी कूटनीति के बीच अंतर का अन्वेषण। OSF प्रीप्रिंट्स।
10. क्लार, एच.टी., 2025. साइबर कूटनीति और साइबर युद्ध के बीच संतुलन की खोज। In: द पालग्रेव हैंडबुक ऑन साइबर डिप्लोमेसी (पृ. 231-251). स्प्रिंगर नेचर स्विट्ज़रलैंड।
11. बाकीरोव, ए. और सुलेइमेनोव, आई., 2025. आधुनिक सूचना युद्ध के प्रतिरोध के तरीकों के सैद्धांतिक आधार। Computers, 14(10), पृ. 410।
12. नगुएन, एम.क्यू. वियतनाम के साइबर सुरक्षा कानून का औचित्य: राज्य मीडिया में शक्तिहीनता, राजनीतिक निष्ठा और अलगाव।
13. लिंडसे, जे.आर., 2025. स्टक्सनेट पुनर्परीक्षण: साइबर युद्ध से गुप्त राज्यकला तक। जर्नल ऑफ स्ट्रैटेजिक स्टडीज, 48(4), पृ. 834-873।
14. रोमानोव्स, ए. और किक्कास, के., 2024. आधुनिक साइबर युद्ध का विकास और विश्लेषण: बाल्टिक देशों पर केंद्रित अध्ययन।
15. खान, डी., महमूद, डब्ल्यू. और शाह, एच., 2025. भारत और पाकिस्तान के बीच हाइब्रिड युद्ध: साइबर खतरे, दुष्प्रचार और रणनीतिक स्थिरता (2019–2024)। रिसर्च कंसोर्टियम आर्काइव, 3(2), पृ. 634-653।
16. ज्यू, एस., वांग, डब्ल्यू. और सुलिवन, जे., 2025. साइबर सुरक्षा, साइबर संप्रभुता और साइबर शासन। Routledge Handbook of Chinese Media।
17. नासिर, एन.एफ.एम., रऊफ, यू.एफ.ए., ज़ैनोल, ज़ेड. और ग़नी, के.ए., 2024. साइबर सुरक्षा में अंदरूनी खतरों के बहु-दृष्टिकोण कारकों का विश्लेषण। जर्नल ऑफ मीडिया एंड इन्फॉर्मेशन वारफेयर, 17(1), पृ. 65-82।
18. टोलमच, एम., ट्राच, वाई., चाइकोव्स्का, ओ., वोलिन्ेट्स, वी., ख्रुश्च, एस. और कोत्सियुबिव्स्का, के., 2023. यूक्रेन पर रूस के सशस्त्र आक्रमण के संदर्भ में दुष्प्रचार और शत्रु प्रचार का मुकाबला करने में कृत्रिम बुद्धिमत्ता। स्प्रिंगर, सिंगापुर।
19. बुखारी, एस.आर.एच., हमायून, एम.के. और खान, एच.ए., 2025. नया वैश्विक अव्यवस्था: कैसे वैश्विक संकट 21वीं सदी की शक्ति संरचना को पुनर्लेखित कर रहे हैं। जर्नल ऑफ रीजनल स्टडीज रिव्यू, 4(4), पृ. 73-88।
20. उस्मान, एच. और मीर, एस.ए., 2023. पारंपरिक युद्ध से परे: साइबर हमले और संयुक्त राष्ट्र चार्टर के अनुच्छेद 2(4) की व्याख्या। ग्लोबल लीगल स्टडीज रिव्यू, 8(2), पृ. 16-26।

21. हारून, ए., 2024. इजराइल-ईरान संघर्ष में एआई और साइबर संचालित युद्ध तथा खाड़ी देशों की सुरक्षा पर प्रभाव। जर्नल ऑफ पॉलिटिक्स एंड इंटरनेशनल स्टडीज, 10(2), पृ. 145-163।

22. सुलझित्स्की, आई., मातवेइएवा, ओ., नवुमाउ, वी. और खुट्की, डी., 2024. युद्ध के दौरान रूसी और यूक्रेनी मीडिया फ्रेम्स की तुलना: एक मिश्रित-विधि दृष्टिकोण। स्टडीज इन कम्युनिकेशन साइंसेज, 24(3), पृ. 303-321।

23. मट्टीला, जे.के., 2022. राज्य साइबर शक्ति का मॉडल: रूसी व्यवहार का अध्ययन। ECCWS 2022।

24. मट्टीएलो, एच., 2024. 'मुफ्त' की छिपी हुई लागतों का अनावरण: डिजिटल अर्थव्यवस्था में व्यक्तिगत डेटा का वस्तुकरण। जर्नल ऑफ पॉलिसी एंड सोसाइटी, 2(2)।

25. फिरदौस, आर., शुए, वाई., गैंग, एल. और सिब्त-ए-अली, एम., 2022. ऑनलाइन लेन-देन धोखाधड़ी में कृत्रिम बुद्धिमत्ता और मानव मनोविज्ञान। फ्रंटियर्स इन साइकोलॉजी, 13, पृ. 947234।

26. बेड़ेर्ना, ज़ेड. और रज़्ज़ाई, ज़ेड., 2022. **यूरोपीय संघ में साइबर सुरक्षा पारिस्थितिकी तंत्र का विश्लेषण।** इंटरनेशनल साइबरसिक्योरिटी लॉ रिव्यू, 3(1), पृ. 35-49।