International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

# साइबर सुरक्षा और वैश्विक राजनीतिक चुनौतियाँ

**कौशल कुमार सैन**

सह आचार्य

राजनीति विज्ञान, बाबू शोभाराम राजकीय कला महाविद्यालय, अलवर

**शोध सारांश (Abstract)**

वर्तमान डिजिटल युग में साइबर सुरक्षा केवल एक तकनीकी समस्या नहीं रह गई है, बल्कि यह वैश्विक राजनीति, अंतर्राष्ट्रीय संबंधों और राष्ट्रीय सुरक्षा का एक अनिवार्य अंग बन चुकी है। यह शोध पत्र साइबर सुरक्षा की बहुआयामी चुनौतियों और उनके वैश्विक राजनीतिक संदर्भ का विश्लेषण करता है।

इस शोध में यह समझने का प्रयास किया गया है कि किस प्रकार राष्ट्र-राज्य, गैर-राज्य अभिकर्ता, आतंकवादी संगठन और साइबर अपराधी, साइबर माध्यमों का प्रयोग करके न केवल आर्थिक हानि पहुँचाते हैं, बल्कि राजनीतिक अस्थिरता भी उत्पन्न करते हैं। इसके साथ ही यह पत्र यह भी विश्लेषण करता है कि भारत सहित अन्य देश किस प्रकार अपनी साइबर नीतियाँ विकसित कर रहे हैं।

शोध के प्रमुख निष्कर्षों में यह उभरकर आया है कि साइबर स्पेस अब पाँचवाँ युद्धक्षेत्र बन चुका है। अमेरिका-चीन, रूस-यूक्रेन जैसे संघर्षों में साइबर आक्रमण अहम भूमिका निभा रहे हैं। अंतर्राष्ट्रीय कानूनी ढाँचे की कमजोरी, सहयोग का अभाव और डिजिटल असमानता इस क्षेत्र की प्रमुख राजनीतिक चुनौतियाँ हैं। इस शोध में द्वितीयक स्रोतों — पुस्तकों, शोध पत्रिकाओं, सरकारी रिपोर्ट और अंतर्राष्ट्रीय संगठनों के दस्तावेजों — का उपयोग किया गया है।

आधुनिक युग में सूचना एवं संचार प्रौद्योगिकी के तीव्र विकास ने विश्व को डिजिटल रूप से जोड़ दिया है। इंटरनेट, कृत्रिम बुद्धिमत्ता, क्लाउड कंप्यूटिंग तथा डिजिटल नेटवर्क के बढ़ते उपयोग के साथ साइबर सुरक्षा वैश्विक राजनीति का महत्वपूर्ण विषय बन गई है। इस शोध का उद्देश्य साइबर सुरक्षा से उत्पन्न वैश्विक राजनीतिक चुनौतियों तथा उनके अंतरराष्ट्रीय संबंधों पर प्रभाव का अध्ययन करना है।

अध्ययन में पाया गया कि साइबर हमले, डेटा चोरी, हैकिंग, साइबर आतंकवाद और डिजिटल जासूसी जैसी गतिविधियाँ देशों की राष्ट्रीय सुरक्षा, अर्थव्यवस्था और लोकतांत्रिक संस्थाओं के लिए गंभीर खतरा बन चुकी हैं। कई राष्ट्र अब पारंपरिक सैन्य शक्ति के साथ-साथ साइबर शक्ति को भी अपनी सुरक्षा रणनीति का महत्वपूर्ण भाग मान रहे हैं।

शोध में यह स्पष्ट किया गया है कि साइबर क्षेत्र में बढ़ती प्रतिस्पर्धा ने अंतरराष्ट्रीय राजनीति में नए प्रकार के संघर्षों को जन्म दिया है। विकसित देश उन्नत तकनीकों और साइबर अवसंरचना के माध्यम से वैश्विक प्रभाव बढ़ाने का प्रयास कर रहे हैं, जबकि विकासशील देश साइबर सुरक्षा संसाधनों और तकनीकी क्षमता की कमी से जूझ रहे हैं। इसके परिणामस्वरूप डिजिटल असमानता और तकनीकी निर्भरता जैसी समस्याएँ सामने आ रही हैं।

अध्ययन में साइबर युद्ध और राजनीतिक हस्तक्षेप के उदाहरणों का भी विश्लेषण किया गया है। चुनावी प्रक्रियाओं में हैकिंग, फेक न्यूज़ और सोशल मीडिया के माध्यम से जनमत को प्रभावित करने की घटनाओं ने लोकतांत्रिक व्यवस्था की विश्वसनीयता को चुनौती दी है। इसके अतिरिक्त साइबर आतंकवाद और महत्वपूर्ण सरकारी संस्थानों पर हमलों ने वैश्विक शांति और सुरक्षा को प्रभावित किया है।

शोध यह भी दर्शाता है कि साइबर सुरक्षा के लिए अंतरराष्ट्रीय सहयोग अत्यंत आवश्यक है। संयुक्त राष्ट्र, NATO तथा विभिन्न क्षेत्रीय संगठनों द्वारा साइबर अपराध नियंत्रण, डेटा संरक्षण और डिजिटल नियमों के निर्माण के प्रयास किए जा रहे हैं। भारत ने भी डिजिटल इंडिया, साइबर सुरक्षा नीति तथा CERT-In जैसी संस्थाओं के माध्यम से अपनी साइबर सुरक्षा व्यवस्था को मजबूत करने का प्रयास किया है।

अंततः शोध यह निष्कर्ष प्रस्तुत करता है कि साइबर सुरक्षा आज अंतरराष्ट्रीय राजनीति का एक केंद्रीय विषय बन चुकी है। वैश्विक स्तर पर साइबर खतरों से निपटने के लिए तकनीकी सहयोग, मजबूत कानूनी ढाँचे, डिजिटल

जागरूकता और अंतरराष्ट्रीय समन्वय की आवश्यकता है, ताकि विश्व शांति, सुरक्षा और डिजिटल संप्रभुता को सुरक्षित रखा जा सके।

**मुख्य शब्द:** साइबर सुरक्षा, साइबर युद्ध, डिजिटल संप्रभुता, वैश्विक राजनीति, साइबर आतंकवाद, साइबर कूटनीति, राष्ट्रीय सुरक्षा, अंतर्राष्ट्रीय संबंध।

## प्रस्तावना (Introduction)

### ऐतिहासिक पृष्ठभूमि

साइबर सुरक्षा की अवधारणा का उद्भव 1960-70 के दशक में हुआ जब अमेरिकी रक्षा विभाग ने ARPANET (Advanced Research Projects Agency Network) की स्थापना की। प्रारंभ में इंटरनेट को एक शैक्षणिक एवं सैन्य संचार माध्यम के रूप में विकसित किया गया था। किंतु धीरे-धीरे इसके व्यापक सामाजिक, आर्थिक और राजनीतिक प्रभाव सामने आने लगे।

1988 में 'मॉरिस वर्म' पहला प्रमुख साइबर आक्रमण था जिसने इंटरनेट से जुड़े हजारों कंप्यूटरों को प्रभावित किया। 1990 के दशक में इंटरनेट के व्यापक प्रसार के साथ-साथ साइबर अपराधों की संख्या भी बढ़ने लगी। 2007 में एस्टोनिया पर हुए साइबर हमले ने पहली बार यह स्पष्ट किया कि साइबर आक्रमण किसी देश की आधारभूत संरचना को पूरी तरह ध्वस्त कर सकते हैं। इस घटना को 'पहला साइबर युद्ध' भी कहा जाता है।

2010 में 'स्टक्सनेट' वायरस ने ईरान के परमाणु कार्यक्रम को निशाना बनाया, जो माना जाता है कि अमेरिका और इजराइल ने मिलकर विकसित किया था। इस घटना ने साइबर हथियारों की वास्तविकता को वैश्विक स्तर पर उजागर किया। 2013 में एडवर्ड स्नोडेन के खुलासों ने यह दर्शाया कि राष्ट्र-राज्य अपने ही नागरिकों और मित्र देशों की जासूसी भी साइबर माध्यमों से करते हैं।

### वर्तमान परिदृश्य

21वीं सदी के तीसरे दशक में साइबर सुरक्षा एक वैश्विक राजनीतिक प्राथमिकता बन चुकी है। आज विश्व के लगभग 5.4 अरब लोग इंटरनेट से जुड़े हैं और यह संख्या प्रतिवर्ष बढ़ती जा रही है। IoT (Internet of Things), Artificial Intelligence, क्लाउड कंप्यूटिंग और 5G तकनीक ने जहाँ एक ओर मानव जीवन को सुविधाजनक बनाया है, वहीं दूसरी ओर साइबर खतरों की संख्या और जटिलता भी बढ़ी है।

रूस-यूक्रेन युद्ध (2022 से अब तक) में साइबर आक्रमणों की अभूतपूर्व भूमिका देखी गई। यूक्रेन की सरकारी वेबसाइटें, बैंकिंग प्रणाली और ऊर्जा अवसंरचना पर लगातार साइबर हमले हुए। इसी प्रकार, चीन और अमेरिका के बीच चिप युद्ध और तकनीकी वर्चस्व की होड़ ने साइबर जासूसी को एक प्रमुख कूटनीतिक मुद्दे का रूप दे दिया है।

भारत में भी साइबर सुरक्षा चुनौतियाँ निरंतर बढ़ रही हैं। AIIMS दिल्ली (2022) पर रैंसमवेयर हमला, UPI और डिजिटल बैंकिंग पर साइबर धोखाधड़ी, तथा LAC (Line of Actual Control) पर भारत-चीन तनाव के दौरान साइबर घुसपैठ की घटनाएँ — ये सब इस बात के प्रमाण हैं कि साइबर सुरक्षा अब राष्ट्रीय सुरक्षा का अभिन्न अंग है।

वैश्विक स्तर पर संयुक्त राष्ट्र, NATO, G20 और BRICS जैसे बहुपक्षीय मंचों पर साइबर सुरक्षा विमर्श का हिस्सा बन चुकी है। किंतु एक सुसंगत और बाध्यकारी अंतर्राष्ट्रीय कानूनी ढाँचे का अभाव इस क्षेत्र की सबसे बड़ी राजनीतिक चुनौती बनी हुई है।

## उद्देश्य (Objectives)

प्रस्तुत शोध पत्र निम्नलिखित प्रमुख उद्देश्यों को ध्यान में रखकर तैयार किया गया है:

1. साइबर सुरक्षा की अवधारणा, इतिहास और वर्तमान स्वरूप का विस्तृत विश्लेषण करना।
2. साइबर खतरों के विभिन्न प्रकारों — साइबर युद्ध, साइबर जासूसी, साइबर आतंकवाद और साइबर अपराध — का राजनीतिक संदर्भ में अध्ययन करना।
3. राष्ट्र-राज्यों द्वारा साइबर माध्यमों के रणनीतिक उपयोग और उसके वैश्विक राजनीतिक प्रभावों को समझना।
4. भारत की साइबर सुरक्षा नीति, संस्थागत ढाँचे और चुनौतियों का परीक्षण करना।

5. अंतर्राष्ट्रीय साइबर कानून, संधियों और बहुपक्षीय सहयोग की वर्तमान स्थिति एवं सीमाओं का आकलन करना।
6. साइबर स्पेस में डिजिटल संप्रभुता, मानवाधिकार और अभिव्यक्ति की स्वतंत्रता जैसे राजनीतिक मुद्दों का विश्लेषण करना।
7. वैश्विक साइबर शासन के भविष्य की संभावनाओं और सुझावों को प्रस्तुत करना।

इन उद्देश्यों के माध्यम से यह शोध पत्र न केवल साइबर सुरक्षा की तकनीकी जटिलताओं को, बल्कि उसके गहरे राजनीतिक निहितार्थों को भी उजागर करने का प्रयास करता है।

## महत्व (Significance)

### राष्ट्रीय सुरक्षा के संदर्भ में महत्व -

साइबर सुरक्षा का अध्ययन आज इसलिए अत्यंत महत्वपूर्ण है क्योंकि इसने राष्ट्रीय सुरक्षा की परिभाषा ही बदल दी है। पारंपरिक सैन्य शक्ति के साथ-साथ अब साइबर क्षमता भी किसी राष्ट्र की शक्ति का मापदंड बन गई है। चीन, रूस, अमेरिका, इजराइल और उत्तर कोरिया जैसे देश साइबर युद्ध क्षमताओं में भारी निवेश कर रहे हैं।
भारत जैसे विकासशील देशों के लिए यह विषय और भी महत्वपूर्ण हो जाता है, क्योंकि डिजिटल इंडिया कार्यक्रम, UPI, आधार, और स्मार्ट सिटी परियोजनाओं ने जहाँ एक ओर शासन को पारदर्शी और सुलभ बनाया है, वहीं साइबर भेद्यता भी बढ़ी है।

### अंतर्राष्ट्रीय संबंधों के संदर्भ में महत्व

साइबर सुरक्षा अब कूटनीति का एक प्रमुख उपकरण बन चुकी है। देश एक-दूसरे पर साइबर हमलों का आरोप लगाते हैं और इसके चलते राजनयिक संबंध प्रभावित होते हैं। अमेरिकी राष्ट्रपति चुनाव (2016) में रूसी हस्तक्षेप के आरोप, सोलरविंड्स हैक (2020) और माइक्रोसॉफ्ट एक्सचेंज सर्वर हमले इसके स्पष्ट उदाहरण हैं।
साइबर सुरक्षा ने 'एट्रिब्यूशन' (Attribution) की समस्या उत्पन्न की है, अर्थात यह सिद्ध करना कि कोई हमला किसने किया — यह राजनीतिक रूप से अत्यंत जटिल है। इस समस्या ने अंतर्राष्ट्रीय कानून और राज्य उत्तरदायित्व के सिद्धांतों पर नए प्रश्न खड़े किए हैं।

### लोकतंत्र और मानवाधिकार के संदर्भ में महत्व

साइबर स्पेस लोकतांत्रिक विमर्श का एक महत्वपूर्ण मंच बन चुका है। किंतु इसी के साथ डिसइन्फॉर्मेशन (गलत सूचना), डीपफेक, सोशल मीडिया मैनिपुलेशन और चुनावी हस्तक्षेप जैसी चुनौतियाँ उभरी हैं। इससे लोकतांत्रिक प्रक्रियाओं की विश्वसनीयता पर खतरा मंडरा रहा है।
व्यक्तिगत डेटा की सुरक्षा, निजता का अधिकार, इंटरनेट पर अभिव्यक्ति की स्वतंत्रता — ये सभी मौलिक अधिकारों से जुड़े प्रश्न हैं जो साइबर सुरक्षा नीतियों से प्रत्यक्षतः प्रभावित होते हैं। सरकारें सुरक्षा के नाम पर नागरिकों की निगरानी करती हैं, जो मानवाधिकारों के संदर्भ में विवादास्पद है।

### आर्थिक और वाणिज्यिक संदर्भ में महत्व

साइबर अपराधों के कारण वैश्विक अर्थव्यवस्था को प्रतिवर्ष लगभग 8-10 ट्रिलियन डॉलर का नुकसान होता है (Cybersecurity Ventures, 2023)। रैंसमवेयर हमले, डेटा चोरी, बौद्धिक संपदा की चोरी और वित्तीय धोखाधड़ी — ये सब अंतर्राष्ट्रीय व्यापार और निवेश को प्रभावित करते हैं। इसलिए साइबर सुरक्षा वैश्विक आर्थिक नीति का भी अनिवार्य अंग बन चुकी है।

## अध्ययन की विधि (Research Methodology)

### शोध का स्वरूप

प्रस्तुत शोध पत्र प्रकृति में गुणात्मक (Qualitative) और वर्णनात्मक-विश्लेषणात्मक (Descriptive-Analytical) है। इसमें साइबर सुरक्षा और वैश्विक राजनीति के संबंधों को समझने के लिए ऐतिहासिक विश्लेषण (Historical

Analysis), केस स्टडी पद्धति (Case Study Method), तुलनात्मक राजनीतिक विश्लेषण (Comparative Political Analysis) और सामग्री विश्लेषण (Content Analysis) का सम्मिलित उपयोग किया गया है।

### प्राथमिक स्रोत (Primary Sources)

यद्यपि यह शोध पत्र मुख्यतः द्वितीयक स्रोतों पर आधारित है, तथापि कुछ प्राथमिक स्रोतों का भी संदर्भ लिया गया है:

- भारत सरकार के IT मंत्रालय और CERT-In (Computer Emergency Response Team - India) की वार्षिक रिपोर्टें।
- संयुक्त राष्ट्र के GGE (Group of Governmental Experts) और OEWG (Open-Ended Working Group) के दस्तावेज।
- NATO साइबर रक्षा नीति दस्तावेज।
- विभिन्न देशों की राष्ट्रीय साइबर सुरक्षा नीतियाँ (National Cyber Security Policies)।
- अंतर्राष्ट्रीय दूरसंचार संघ (ITU) की वैश्विक साइबर सुरक्षा सूचकांक रिपोर्टें।

### द्वितीयक स्रोत (Secondary Sources)

इस शोध में निम्नलिखित प्रकार के द्वितीयक स्रोतों का व्यापक उपयोग किया गया है:

- अकादमिक पुस्तकें और विद्वत्तापूर्ण ग्रंथ (जैसे — Cyber War by Richard A. Clarke, The Perfect Weapon by David Sanger आदि)
- शोध पत्रिकाएँ — Journal of Cybersecurity, International Security, Security Dialogue, India Quarterly आदि।
- थिंक टैंक रिपोर्टें — Brookings Institution, RAND Corporation, Observer Research Foundation (ORF), Institute for Defence Studies and Analyses (IDSA)।
- समाचार पत्र और डिजिटल मीडिया — The Hindu, Indian Express, Reuters, BBC, The Guardian।
- अंतर्राष्ट्रीय संगठनों की रिपोर्टें — UN, WEF (World Economic Forum), Interpol, Kaspersky Lab, Mandiant आदि।

### डेटा संग्रह और विश्लेषण पद्धति

डेटा संग्रह के लिए पुस्तकालय अनुसंधान, ऑनलाइन डेटाबेस (जैसे JSTOR, Google Scholar, ResearchGate) और आधिकारिक सरकारी वेबसाइटों का उपयोग किया गया। विश्लेषण में आगमनात्मक (Inductive) और निगमनात्मक (Deductive) दोनों पद्धतियों का सम्मिश्रण किया गया। सामग्री विश्लेषण के लिए विषय-आधारित कोडिंग (Thematic Coding) का प्रयोग किया गया जिससे प्रमुख विषयों की पहचान की जा सके।

## विस्तृत विश्लेषण

### साइबर खतरों के प्रकार और राजनीतिक आयाम

साइबर खतरे अनेक रूपों में प्रकट होते हैं। इन्हें मुख्यतः चार श्रेणियों में विभाजित किया जा सकता है:

प्रथम, साइबर युद्ध (Cyber Warfare): जब कोई राष्ट्र-राज्य दूसरे देश की आधारभूत संरचना, सैन्य प्रणाली या सरकारी नेटवर्क को निशाना बनाता है। 2007 में एस्टोनिया पर रूसी हमला, 2010 में ईरान पर स्टक्सनेट हमला और 2022 में रूस-यूक्रेन साइबर युद्ध इसके प्रमुख उदाहरण हैं।

द्वितीय, साइबर जासूसी (Cyber Espionage): दूसरे देशों की गोपनीय सूचनाएँ चुराना। चीन के APT (Advanced Persistent Threat) समूहों पर अमेरिकी सरकारी एजेंसियों और कंपनियों से डेटा चोरी का आरोप है। भारत के रक्षा, अंतरिक्ष और परमाणु प्रतिष्ठानों पर भी इस प्रकार के हमले हो चुके हैं।

तृतीय, साइबर आतंकवाद (Cyber Terrorism): आतंकवादी संगठनों द्वारा साइबर माध्यमों का उपयोग भर्ती, प्रचार-प्रसार, धनराशि संग्रह और संचार के लिए किया जाता है। ISIS ने डार्क वेब और एन्क्रिप्टेड संदेश सेवाओं का व्यापक उपयोग किया।

चतुर्थ, साइबर अपराध (Cybercrime): यह सबसे व्यापक और सामान्य रूप है जिसमें बैंकिंग धोखाधड़ी, रैंसमवेयर, फिशिंग, पहचान चोरी आदि शामिल हैं। इसके पीछे अक्सर संगठित अपराधी गिरोह होते हैं जो कभी-कभी राज्य-संरक्षित भी होते हैं।

## प्रमुख केस स्टडी

रूस-यूक्रेन साइबर युद्ध (2022-अब): 24 फरवरी 2022 को रूस के सैन्य आक्रमण से पहले ही यूक्रेन पर साइबर हमले शुरू हो गए थे। 'वाइपर मैलवेयर' ने यूक्रेनी सरकारी कंप्यूटर नष्ट किए, बैंकिंग सेवाएँ बाधित हुईं और सरकारी वेबसाइटें ध्वस्त हुईं। इसके जवाब में यूक्रेन ने 'IT Army of Ukraine' बनाई जिसने रूसी वेबसाइटों पर जवाबी हमले किए।

सोलरविंड्स हैक (2020): अमेरिकी सरकारी एजेंसियों, रक्षा विभाग और शीर्ष कंपनियों की आपूर्ति श्रृंखला को हैक किया गया। इसे रूस के SVR (Foreign Intelligence Service) से जोड़ा गया। इस हमले ने 'सप्लाई चेन अटैक' की भयावहता को उजागर किया।

चीन का साइबर अभियान: China's APT10, APT40 और APT41 समूहों पर अमेरिका, ऑस्ट्रेलिया, भारत और यूरोपीय देशों की सरकारी एजेंसियों और विश्वविद्यालयों से डेटा चोरी का आरोप है। 2021 में माइक्रोसॉफ्ट एक्सचेंज सर्वर हमले में चीनी समूह शामिल था।

## डिजिटल संप्रभुता और इंटरनेट शासन

डिजिटल संप्रभुता (Digital Sovereignty) की अवधारणा ने हाल के वर्षों में अंतर्राष्ट्रीय राजनीति में महत्वपूर्ण स्थान प्राप्त किया है। रूस और चीन जैसे देश 'साइबरस्पेस की संप्रभुता' की माँग करते हैं अर्थात अपने देश के इंटरनेट को नियंत्रित करने का अधिकार। चीन का 'ग्रेट फायरवॉल' और रूस का RuNet इसके उदाहरण हैं।

दूसरी ओर, अमेरिका और पश्चिमी देश 'मुक्त और खुले इंटरनेट' की वकालत करते हैं। यह वैचारिक विभाजन — मल्टीस्टेकहोल्डर बनाम मल्टीलेटरल इंटरनेट शासन — वैश्विक राजनीतिक संघर्ष का एक प्रमुख आयाम बन गया है। ITU में इस पर गहरे मतभेद हैं।

## भारत की साइबर सुरक्षा नीति

भारत ने 2013 में अपनी पहली राष्ट्रीय साइबर सुरक्षा नीति (National Cyber Security Policy) जारी की। 2020 में नई साइबर सुरक्षा रणनीति का मसौदा तैयार हुआ। CERT-In, NCIIPC (National Critical Information Infrastructure Protection Centre) और DRDO की साइबर शाखा इस क्षेत्र में सक्रिय हैं।

भारत के लिए प्रमुख चुनौतियाँ हैं: चीन और पाकिस्तान से साइबर खतरे, डिजिटल अवसंरचना की सुरक्षा, डेटा संरक्षण कानून (DPDP Act 2023) का प्रभावी क्रियान्वयन, और साइबर सुरक्षा विशेषज्ञों की कमी। भारत ने 'डेटा लोकलाइजेशन' की नीति अपनाई है और 59 चीनी ऐप्स पर प्रतिबंध लगाकर डिजिटल संप्रभुता का संदेश दिया है।

## निष्कर्ष (Conclusion)

इस शोध पत्र के अध्ययन से यह स्पष्ट होता है कि साइबर सुरक्षा अब केवल एक तकनीकी चुनौती नहीं, बल्कि 21वीं सदी की राजनीति, कूटनीति और अंतर्राष्ट्रीय संबंधों का केंद्रीय विषय बन चुकी है। इसके निम्नलिखित प्रमुख निष्कर्ष उभरे हैं:

प्रथम: साइबर स्पेस पाँचवाँ युद्धक्षेत्र — भूमि, समुद्र, वायु और अंतरिक्ष के बाद साइबर स्पेस अब युद्ध का पाँचवाँ आयाम बन चुका है। NATO ने 2016 में साइबर स्पेस को आधिकारिक रूप से परिचालन क्षेत्र (Operational Domain) घोषित किया।

द्वितीय: अंतर्राष्ट्रीय कानूनी शून्य — साइबर हमलों से निपटने के लिए कोई सार्वभौमिक बाध्यकारी अंतर्राष्ट्रीय संधि नहीं है। 'Tallinn Manual' जैसे दस्तावेज मार्गदर्शक हैं किंतु बाध्यकारी नहीं। इस शून्य का लाभ उठाकर राष्ट्र-राज्य एक-दूसरे पर साइबर हमले करते हैं और जवाबदेही से बचते हैं।

तृतीय: डिजिटल असमानता एक चुनौती — विकसित और विकासशील देशों के बीच साइबर क्षमताओं में भारी असमानता है। कम संसाधन वाले देश साइबर हमलों का आसान शिकार बनते हैं। यह 'डिजिटल डिवाइड' वैश्विक सुरक्षा के लिए खतरा है।
चतुर्थ: बहुपक्षीय सहयोग की आवश्यकता — साइबर सुरक्षा की चुनौती किसी एक देश की क्षमता से परे है। इसके लिए राष्ट्रों के बीच सूचना साझाकरण, संयुक्त प्रशिक्षण और क्षमता निर्माण आवश्यक है। भारत ने QUAD और SCO जैसे मंचों पर इस दिशा में प्रयास किए हैं।
पंचम: प्रौद्योगिकी और नीति का समन्वय — AI, क्वांटम कंप्यूटिंग और 5G जैसी नई प्रौद्योगिकियाँ साइबर खतरों को और जटिल बना रही हैं। सरकारों को तकनीकी विकास के साथ-साथ नीतिगत ढाँचों को भी अद्यतन करना होगा।
अंततः, यह कहा जा सकता है कि साइबर सुरक्षा वैश्विक राजनीतिक व्यवस्था में एक नई शक्ति की गतिशीलता ला रही है। जो देश साइबर क्षमताओं में आगे होंगे, वे 21वीं सदी की वैश्विक राजनीति में भी आगे रहेंगे। भारत के लिए आवश्यक है कि वह अपनी साइबर क्षमताओं को मजबूत करे, एक समग्र साइबर रणनीति बनाए और वैश्विक साइबर शासन में नेतृत्वकारी भूमिका निभाए।

## संदर्भ सूची (Bibliography)

### पुस्तकें (Books)

1. Clarke, Richard A. & Knake, Robert K. (2010). Cyber War: The Next Threat to National Security and What to Do About It. New York: Ecco Press.
2. Sanger, David E. (2018). The Perfect Weapon: War, Sabotage, and Fear in the Cyber Age. New York: Crown Publishers.
3. Kaplan, Fred (2016). Dark Territory: The Secret History of Cyber War. New York: Simon & Schuster.
4. Rid, Thomas (2016). Rise of the Machines: A Cybernetic History. New York: W.W. Norton & Company.
5. Sharma, Arvind & Gupta, R.K. (2021). Bharat ki Cyber Suraksha: Chunautiyan aur Sambhavnayein (भारत की साइबर सुरक्षा: चुनौतियाँ और संभावनाएँ). New Delhi: Pentagon Press.
6. Singh, Manpreet (2020). Digital India aur Cyber Khatra (डिजिटल इंडिया और साइबर खतरा). New Delhi: Vani Prakashan.

### शोध पत्रिकाएँ (Research Journals)

7. Nye, Joseph S. Jr. (2017). 'Deterrence and Dissuasion in Cyberspace.' International Security, 41(3), pp. 44-71.
8. Valeriano, Brandon & Maness, Ryan C. (2014). 'The Dynamics of Cyber Conflict Between Rival Antagonists.' Journal of Peace Research, 51(3), pp. 347-360.
9. Sharma, Rajeev & Mishra, Anand (2022). 'India's Cyber Security Challenges: A Policy Perspective.' India Quarterly, 78(2), pp. 112-134.
10. Dixit, Prashant (2023). 'Cyber Yuddh aur Vaishvik Rajniti' (साइबर युद्ध और वैश्विक राजनीति). Rajniti Vigyan Sameeksha, 15(1), pp. 45-67.

### सरकारी और संस्थागत रिपोर्टें (Government & Institutional Reports)

11. CERT-In (2023). Annual Report on Cyber Security Incidents in India 2022-23. New Delhi: Ministry of Electronics & Information Technology, Government of India.
12. United Nations (2021). Report of the Group of Governmental Experts on Advancing Responsible State Behaviour in Cyberspace. New York: United Nations General Assembly.
13. WEF (2023). Global Cybersecurity Outlook 2023. Geneva: World Economic Forum.
14. NATO (2022). NATO Cyber Defence Policy. Brussels: North Atlantic Treaty Organization.
15. ITU (2022). Global Cybersecurity Index 2022. Geneva: International Telecommunication Union.

## थिंक टैंक और अन्य स्रोत (Think Tanks & Other Sources)

16. Observer Research Foundation (ORF) (2023). India's Cyber Security Architecture. New Delhi: ORF Special Reports.
17. Institute for Defence Studies and Analyses (IDSA) (2022). Cyber Security and India's National Security. New Delhi: IDSA Monograph.
18. Mandiant (2023). M-Trends 2023: A View from the Frontlines. Reston, VA: Mandiant Inc.
19. Cybersecurity Ventures (2023). Cybercrime Report 2023. Sausalito, CA: Cybersecurity Ventures.
20. RAND Corporation (2021). Cybersecurity and the Future of Warfare. Santa Monica, CA: RAND Corporation.

## वेबसाइटें और ऑनलाइन स्रोत (Websites & Online Sources)

21. Ministry of Electronics & Information Technology, Government of India: https://meity.gov.in
22. CERT-In Official Website: https://www.cert-in.org.in
23. NCIIPC Official Website: https://nciipc.gov.in
24. United Nations Institute for Disarmament Research (UNIDIR) Cyber Policy Portal: https://unidir.org/cyber-policy-portal