भारत का साइबर पारस्थितिकी तंत्र

यह एडटिोरियल 03/09/2022 को 'द हदिू' में प्रकाशति "India's Cyber Infrastructure Needs More Than Patches" लेख पर आधारति है। इसमें भारत के साइबर पारतिंत्र और देश के साइबर अवसंरचना में वद्यिमान अंतराल के बारे में चर्चा की गई है।

यदि मनुष्यों के पूर्वज सदयिों की लंबी नींद के बाद आज जागें तो वे समकालीन समय की क्रांतकिारी बदलावों और डजिटिलीकृत दुनयिा को देखकर चकति रह जाएँगे।

डजिटिलीकरण के आगमन ने मानव जीवन के हर पहलू को व्यापक स्तर तक प्रभावति कयिा है। हालाँकि सूचना प्रौद्योगकिी का उपयोग दोधारी तलवार भी सद्धि हो रहा है क्योंकि साइबर अपराध और इससे संबद्ध खतरे नाटकीय रूप से बढ़ गए हैं।

जैसे-जैसे भारत वभिन्नि क्षेत्रों में अधकिाधकि डजिटिलीकरण की ओर आगे बढ़ता जा रहा है, साइबरस्पेस राष्ट्रीय सुरक्षा के लयि एक गंभीर चति का वषिय भी बनता जा रहा है। राष्ट्रीय अपराध रकिॉर्ड ब्यूरो (NCRB) के आँकड़ों के अनुसार, वर्ष 2021 में भारत में साइबर अपराध के 52,974 मामले दर्ज कयि गए, जो वर्ष 2020 (50,035 मामले) की तुलना में से 5 प्रतशित से अधकि और वर्ष 2019 (44,735 मामले) की तुलना में 15 प्रतशित से अधकि की वृद्धि को दर्शाते हैं।

यद्यपि भारत सरकार ने साइबर सुरक्षा सुनश्चिति करने के लयि कई कदम उठाए हैं, जसिमें सभी प्रकार के साइबर अपराध से नपिटने के लयि गृह मंत्रालय के तहत भारतीय साइबर अपराध समन्वय केंद्र (Indian Cyber Crime Coordination Centre- I4C) की स्थापना करना भी शामलि है, लेकनि अवसंरचनागत कमयिों को दूर करने के लयि अभी भी बहुत कुछ कयिा जाना शेष है।

साइबर सुरक्षा (Cyber Security)

- साइबर सुरक्षा या सूचना प्रौद्योगकिी सुरक्षा कंप्यूटर, नेटवर्क, प्रोग्राम और डेटा को अनधकिृत पहुँच या हमलों से बचाने की तकनीकें हैं जो साइबर-भौतकि प्रणालयिों (Cyber-Physical Systems) और महत्त्वपूर्ण सूचना अवसंरचना के दोहन पर लक्षति हैं।
  - साइबर-भौतकि प्रणालयिाँ भौतकि वस्तुओं और बुनयिादी ढाँचे में संवेदन (Sensing), संगणना (Computation), नयिंत्रण (Control) और नेटवर्कगि को एकीकृत करती हैं तथा उन्हें इंटरनेट से और परस्पर जोड़ती हैं।
    - **उदाहरण:** औद्योगकि नयिंत्रण प्रणाली, जल प्रणाली, रोबोटक्सि प्रणाली, स्मार्ट ग्रडि आदि।
  - **महत्त्वपूर्ण सूचना अवसंरचना (Critical Information Infrastructure):** सूचना प्रौद्योगकिी अधनियिम, 2000 महत्त्वपूर्ण सूचना अवसंरचना को एक कंप्यूटर संसाधन के रूप में परभिाषति करता है, जसिकी अक्षमता या वनिाश का राष्ट्रीय सुरक्षा, अर्थव्यवस्था, सार्वजनकि स्वास्थ्य या सुरक्षा पर कारी प्रभाव पड़ेगा।
- **साइबर खतरे:**
  - मैलवेयर, वायरस, ट्रोजन, स्पाइवेयर, बैकडोर आदि जो रमिोट एक्सेस की अनुमति देते हैं।
  - 'डस्टि्रब्यिूटेड डनियिल ऑफ सर्वसि' (DDoS), जो सर्वर एवं नेटवर्क पर फ्लडगि (Flooding) की स्थति उत्पन्न करता और उन्हें अनुपयोगी बना देता है।
  - 'डोमेन नेम्ड सस्टि्म पॉइजनगि अटैक' (DNS Poisoning Attacks) जो DNS को भेद्य बनाता और वेबसाइटों को धोखापूर्ण साइटों की ओर रीडायरेक्ट करता है।
- **साइबर सुरक्षा के दायरे में शामलि प्रमुख क्षेत्र:**
  - **ऐप्लीकेशन सुरक्षा (Application Security):** ऐप को उन खतरों से बचाने के लयि जो ऐप्लीकेशन डज़िाइन में मौजूद खामयिों के माध्यम से सामने आ सकते हैं।
  - **सूचना सुरक्षा (Information Security):** अनधकिृत पहुँच से सूचना की रक्षा के लयि ताकि पहचान की चोरी को टाला जा सके और नजिता की रक्षा हो सके।
  - **'डज़िास्टर रकिवरी' (Disaster Recovery):** यह ऐसी प्रक्रयिा है जसिमें साइबर आपदा के मामले में जोखमि मूल्यांकन, प्राथमकिताएँ तय करना, रकिवरी रणनीति वकिसति करना आदि शामलि हैं।
  - **नेटवर्क सुरक्षा (Network Security):** इसमें नेटवर्क की उपयोगति, वश्विसनीयता, अखंडता और सुरक्षा की रक्षा के लयि की जाने वाली गतविधियिाँ शामलि हैं।

- प्रभावी नेटवर्क सुरक्षा विभिन्न प्रकार के खतरों को लक्षित करती है और नेटवर्क में उनके प्रवेश या प्रसार को रोकती है।

साइबर-क्राइम, साइबर-टेररिज्म और साइबर-वार

- **साइबर-क्राइम (Cyber-Crime):** साइबर-क्राइम ऐसे गैरकानूनी कृत्य है जिसमें कंप्यूटर एक साधन के रूप में या लक्ष्य के रूप में या दोनों ही रूप में उपस्थित होता है।
  - साइबर-क्राइम या साइबर अपराधों में ऐसी आपराधिक गतिविधियाँ शामिल हो सकती हैं जो पारंपरिक प्रकृति की हैं, जैसे चोरी, धोखाधड़ी, जालसाजी, मानहानि, अनिष्ट या शरारत आदि।
- **साइबर-वार (Cyber-War):** साइबर-वार या साइबर युद्ध किसी राष्ट्र राज्य द्वारा विदेशी राष्ट्रों के विरुद्ध साइबर स्पेस में अभियानों के संचालन हेतु एक संगठित प्रयास है।
  - इसमें खुफिया जानकारी एकत्र करने के उद्देश्य से इंटरनेट का उपयोग शामिल है।
- **साइबर-टेररिज्म (Cyber-Terrorism):** साइबर-टेररिज्म या साइबर आतंकवाद साइबर स्पेस और आतंकवाद का अभिसरण है।
  - यह गैर-कानूनी हमलों, कंप्यूटर नेटवर्क और उसमें संग्रहीत सूचना के विरुद्ध हमलों की धमकी को संदर्भित करता है, जब ऐसा राजनीतिक या सामाजिक उद्देश्यों को आगे बढ़ाने के लिये सरकार या देश के लोगों को डराने या विवश करने के लिये किया जाता है।

भारत में साइबर सुरक्षा से संबंधित चुनौतियाँ

- **लाभ-उन्मुख अवसंरचना की मानसिकता:** उदारीकरण के बाद से सूचना प्रौद्योगिकी (IT), बिजली और दूरसंचार क्षेत्र में निजी क्षेत्र द्वारा वृहत निवेश किया गया है। लेकिन साइबर हमले से बचाव हेतु तैयारी और नियामक ढाँचे में सुधार पर उनका अपर्याप्त ध्यान रहा है जो चिंता का कारण है।
  - सभी ऑपरेटर लाभ पर अधिक केंद्रित हैं और अवसंरचना में निवेश नहीं करना चाहते क्योंकि वहाँ उनके लिये लाभ के अवसर नहीं हैं।
- **पृथक प्रक्रियात्मक संहिता का अभाव:** साइबर या कंप्यूटर संबंधी अपराधों की जाँच के लिये कोई पृथक प्रक्रियात्मक संहिता मौजूद नहीं है।
- **साइबर हमलों की अंतर्राष्ट्रीय (ट्रांस-नेशनल) प्रकृति:** अधिकांश साइबर अपराध प्रकृति में ट्रांस-नेशनल होते हैं। विदेशी क्षेत्रों से साक्ष्य एकत्र करना न केवल एक कठिन बल्कि एक धीमी प्रक्रिया भी है।
- **डिजिटल पारितंत्र का विस्तार:** पिछले कुछ वर्षों से भारत अपने विभिन्न आर्थिक घटकों के डिजिटलीकरण के मार्ग पर आगे बढ़ा है और सफलतापूर्वक अपने लिये एक जगह बनाई है।
  - 5G और इंटरनेट ऑफ थिंग्स जैसी नवीनतम प्रौद्योगिकियाँ इंटरनेट से जुड़े पारितंत्र के कवरेज में वृद्धि करेंगी।
  - डिजिटलीकरण के आगमन के साथ उपभोक्ता एवं नागरिक डेटा को डिजिटल प्रारूप में संग्रहीत किया जाएगा और लेनदेन ऑनलाइन माध्यम से संपन्न होगा, जो भारत को हैकर्स और साइबर अपराधियों के लिये एक सक्षम ब्रीडिंग ग्राउंड बना सकता है।
- **सीमित विशेषज्ञता और प्राधिकार:** क्रिप्टोकरेंसी से संबंधित अपराधों की कम रिपोर्टिंग की जाती है क्योंकि ऐसे अपराधों को हल करने की क्षमता सीमित रहती है
  - यद्यपि अधिकांश राज्यस्तरीय साइबर लैब हार्ड डिस्क और मोबाइल फोन का विश्लेषण करने में सक्षम हैं, फिर भी उन्हें केंद्र सरकार द्वारा 'इलेक्ट्रॉनिक साक्ष्य के परीक्षक' (Examiners of Electronic Evidence) के रूप में मान्यता दिया जाना अभी शेष है। जब तक उन्हें मान्यता प्राप्त नहीं होगी, वे इलेक्ट्रॉनिक डेटा पर विशेषज्ञ राय नहीं दे सकते।

भारत में साइबर सुरक्षा के लिये वर्तमान उपबंध

- **भारतीय राष्ट्रीय सुरक्षा परिषद (Indian National Security Council):** साइबर नीति से संबंधित पारितंत्र को आकार देने के लिये।
- **राष्ट्रीय साइबर सुरक्षा रणनीति (National Cyber Security Strategy):** सभी डिजिटलीकरण पहलों में डिज़ाइन के प्रारंभिक चरण में सुरक्षा पर ध्यान केंद्रित करने के लिये।
- **कंप्यूटर इमरजेंसी रिस्पांस टीम (Computer Emergency Response Team- CERT-In):** साइबर सुरक्षा उल्लंघनों और अन्य मुद्दों के संबंध में सतर्कता/चेतावनी के लिये।
- **भारतीय साइबर अपराध समन्वय केंद्र (Indian Cyber Crime Coordination Centre- I4C):** साइबर अपराध से संबंधित कई मुद्दों को व्यापक और समन्वित तरीके से संभालने के लिये।
- **साइबर स्वच्छता केंद्र:** भारत में बॉटनेट संक्रमणों का पता लगाकर एक सुरक्षित साइबर स्पेस का निर्माण करने के लिये।

साइबर खतरों की आधुनिक समस्याओं के लिये आधुनिक समाधान

- **सुरक्षित साइबरस्पेस के लिये केंद्र-राज्य सहयोग:** चूँकि पुलिस और लोक व्यवस्था राज्य सूची में शामिल है, अपराध की जाँच करने और आवश्यक साइबर अवसंरचना का निर्माण करने का प्राथमिक दायित्व राज्यों पर है।
  - लेकिन इसके साथ ही चूँकि आईटी अधिनियम और अन्य प्रमुख कानून केंद्रीय अधिनियम हैं, केंद्र सरकार को कानून प्रवर्तन एजेंसियों के लिये सार्वभौमिक वैधानिक प्रक्रियाओं के विकास के लिये आगे बढ़ना चाहिये।
  - केंद्र और राज्यों को साइबर अपराध की जाँच की सुविधा के लिये न केवल मिलकर काम करना चाहिये और वैधानिक दिशानिर्देश तैयार करना चाहिये, बल्कि बहुप्रतीक्षित और आवश्यक साइबर अवसंरचना के विकास के लिये पर्याप्त धन भी प्रदान करना चाहिये।
- **साइबर प्रयोगशालाओं का उन्नयन:** नई प्रौद्योगिकियों के आगमन के साथ साइबर फोरेंसिक प्रयोगशालाओं का उन्नयन किया जाना चाहिये।

- राष्ट्रीय साइबर फोरेंसिक लैब (National Cyber Forensic Lab) और दिल्ली पुलिस की 'साइबर रोकथाम, जागरूकता और जाँच केंद्र' (Cyber Prevention, Awareness and Detection Centre- CYPAD) इस दिशा में एक अच्छा कदम है।

- **क्षमता निर्माण:** साइबर अपराध से निपटने के लिये पर्याप्त क्षमता का निर्माण करना आवश्यक है। इसके लिये या तो प्रत्येक ज़िले या रेंज में एक अलग साइबर पुलिस स्टेशन स्थापित करना होगा या मौजूदा प्रत्येक पुलिस स्टेशन में तकनीकी रूप से योग्य कर्मचारियों की नियुक्ति करनी होगी।
- **न्याय वितरण प्रणाली में सुधार:** चूँकि निजता उल्लंघन के मामले में इलेक्ट्रॉनिक साक्ष्य पारंपरिक अपराधों के साक्ष्य से बहुत भिन्न होते हैं, इलेक्ट्रॉनिक साक्ष्य के लिये मानक और समान प्रक्रियाएँ विकसित करना आवश्यक है ताकि समयबद्ध न्याय सुनिश्चित हो। यह नागरिकों की सुरक्षा के साथ-साथ अवसंरचना को बनाए रखने के लिये आवश्यक है।
- **साइबर रक्षा तंत्र विकसित करना:** साइबर संघर्ष से निपटने के लिये एक समग्र दृष्टिकोण आवश्यक है, चाहे वह साइबर सर्च अभियान के संबंध में हो या साइबर हमलों के विरुद्ध जवाबी कार्रवाई का दायरा बढ़ाने के संबंध में हो।
    - साइबर रक्षा एवं युद्ध पर एक स्पष्ट सार्वजनिक रुख नागरिकों के विश्वास को बढ़ाती है और इस प्रकार एक अधिक आकर्षक, स्थिर और सुरक्षित साइबर पारितंत्र को सक्षम बनाती है।

अभ्यास प्रश्न: जैसे-जैसे भारत डिजिटलीकृत पारितंत्र की ओर बढ़ रहा है, साइबरस्पेस राष्ट्रीय सुरक्षा के लिये एक गंभीर चिंता का विषय भी बनता जा रहा है। टिप्पणी कीजिये।