साइबर सुरक्षा रणनीति की आवश्यकता

इस Editorial में The Hindu, The Indian Express, Business Line आदि में प्रकाशित लेखों का विश्लेषण किया गया है। इस लेख में साइबर सुरक्षा रणनीति की आवश्यकता व उससे संबंधित विभिन्न पहलुओं पर चर्चा की गई है। आवश्यकतानुसार, यथास्थान टीम दृष्टि के इनपुट भी शामिल किये गए हैं।

संदर्भ

हम जितनी तेज़ी से डिजिटल दुनिया की ओर बढ़ रहे हैं, ठीक उतनी ही तेज़ी से साइबर अपराध की संख्या में भी वृद्धि हो रही है। इसका एक ताजा उदाहरण ऑस्ट्रेलिया की संचार प्रणाली पर हुआ साइबर हमला है, जिसने शासन व्यवस्था की संचार प्रणाली को बाधित कर दिया है। साइबर विशेषज्ञों ने भारत में भी एक बड़े साइबर हमले की आशंका व्यक्त की है।

भारत में पूर्व में भी बढ़ती आवृत्ति के साथ साइबर हमले होते रहे हैं। उदाहरण के लिये वर्ष 2016 में बैंक खाताधारकों के 3.2 मिलियन डेबिट कार्ड की व्यक्तिगत जानकारी का लीक होना और उनका डेटा चोरी होना भारत में एक बड़ा साइबर हमला था। वर्तमान में साइबर सुरक्षा रणनीति, राष्ट्रीय सुरक्षा का एक अभिन्न अंग बन गया है। इसका प्रभाव क्षेत्र किसी देश के शासन, अर्थव्यवस्था और कल्याण के सभी पहलुओं को कवर करने में सैन्य प्रभाव व उसकी महत्ता से किसी भी प्रकार से कम नहीं है। आज के समय में इंटरनेट का उपयोग लगभग हर क्षेत्र में किया जाता है। इंटरनेट के विकास और इसके संबंधित लाभों के साथ साइबर अपराधों की अवधारणा भी विकसित हुई है।

इस आलेख में साइबर अपराध, साइबर सुरक्षा ढाँचे के अद्यतनीकरण की आवश्यकता, साइबर सुरक्षा दृष्टिकोण की चुनौतियाँ और सरकार के द्वारा किये गए प्रयासों पर विमर्श किया जाएगा।

साइबर अपराध क्या है?

- साइबर अपराध विभिन्न रूपों में किये जाते हैं। कुछ साल पहले, इंटरनेट के माध्यम से होने वाले अपराधों के बारे में जागरूकता का अभाव था। साइबर अपराधों के मामलों में भारत भी उन देशों से पीछे नहीं है, जहाँ साइबर अपराधों की घटनाओं की दर भी दिन-प्रतिदिन बढ़ती जा रही है।

- साइबर अपराध के मामलों में एक साइबर अपराधी, किसी उपकरण का उपयोग, उपयोगकर्ता की व्यक्तिगत जानकारी, गोपनीय व्यावसायिक जानकारी, सरकारी जानकारी या किसी डिवाइस को अक्षम करने के लिये कर सकता है। उपरोक्त सूचनाओं को ऑनलाइन बेचना या खरीदना भी एक साइबर अपराध है।
- इसमें कोई संशय नहीं है कि यह एक आपराधिक गतिविधि है, जिसे कंप्यूटर और इंटरनेट के उपयोग द्वारा अंजाम दिया जाता है। साइबर अपराध, जिसे 'इलेक्ट्रॉनिक अपराध' के रूप में भी जाना जाता है, एक ऐसा अपराध है जिसमें किसी भी अपराध को करने के लिये कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क का उपयोग, एक वस्तु या उपकरण के रूप में किया जाता है। जहाँ इनके (कंप्यूटर, नेटवर्क डिवाइस या नेटवर्क) ज़रिये ऐसे अपराधों को अंजाम दिया जाता है वहीँ इन्हें लक्षय बनाते हुए इनके विरुद्ध अपराध भी किया जाता है।

साइबर सुरक्षा ढाँचे के अद्यतनीकरण की आवश्यकता क्यों?

- **राष्ट्रीय सुरक्षा का अभिन्न अंग**
  - साइबर कमांड को बढ़ाने की आवश्यकता के पक्ष में सैन्य सिद्धांतों में हो रहा परिवर्तन साइबर सुरक्षा रणनीति में बदलाव के महत्त्व को प्रतिबिंबित करता है।
  - राष्ट्रीय सुरक्षा के अभिन्न अंग के रूप में एक सक्षम साइबर सुरक्षा बुनियादी ढाँचे की आवश्यकता पर पहली बार **कारगिल समीक्षा समिति (Kargil Review Committee), 1999** द्वारा ज़ोर दिया गया था।
- **डिजिटल अर्थव्यवस्था का बढ़ता महत्त्व**

  वर्तमान में भारत की कुल अर्थव्यवस्था के आकार का 14-15 प्रतिशत भाग डिजिटल अर्थव्यवस्था में शामिल है और वर्ष 2024 तक इसे 20 प्रतिशत तक पहुँचाने का लक्षय है।
- **एक जटिल डोमेन**

  कृत्रिम बुद्धिमत्ता (Artificial Intelligence-AI), मशीन लर्निंग (Machine Learning -ML), डेटा एनालिटिक्स, क्लाउड कंप्यूटिंग और इंटरनेट ऑफ थिंग्स (Internet of Things-IoT) की अधिक समावेशी प्रकृति के कारण साइबर स्पेस एक जटिल डोमेन बन गया है, जो तकनीकी व कानूनी प्रकृति की समस्याओं को जन्म देगा।
- **डेटा संरक्षण की चुनौती**
  - 21 वीं सदी में डेटा, मुद्रा के समान महत्त्वपूर्ण है। भारत की विशाल जनसंख्या के कारण कई अंतरराष्ट्रीय कंपनियाँ (गूगल, अमेज़न) यहाँ अपनी पहुँच बनाने की कोशिश कर रही हैं।
  - इसलिये डेटा संप्रभुता (Data Sovereignty), **डेटा स्थानीयकरण** (Data Localisation) और इंटरनेट गवर्नेंस (Internet Governance) आदि से संबंधित मुद्दों का समाधान आवश्यक है।

साइबर सुरक्षा दृष्टिकोण की चुनौतियाँ

- **मानव संशाधन की कमी**
    - इस क्षेत्र के लिये आवश्यक विभिन्न सॉफ्टवेयर और हार्डवेयर से संबंधित तकनीकी पहलुओं को समझने के लिये भारतीय सैन्य बलों, केंद्रीय पुलिस संगठनों, कानून प्रवर्तन एजेंसियों में कुशल लोगों का अभाव है।
    - इसके अलावा कृत्रिम बुद्धिमत्ता (Artificial Intelligence-AI), ब्लॉकचेन टेक्नोलॉजी (BlockChain Technology-BCT), मशीन लर्निंग (Machine Learning -ML), डेटा एनालिटिक्स, क्लाउड कंप्यूटिंग और इंटरनेट ऑफ थिंग्स (Internet of Things-IoT) जैसी अत्याधुनिक तकनीकी की समझ रखने वाले पेशेवरों की कमी है।
    - कई विशेषज्ञों के अनुसार, वर्तमान में कम से कम तीन मिलियन साइबर सुरक्षा पेशेवरों की आवश्यकता है।
- **सक्रिय साइबर डिफेंस का अभाव**

    भारत में यूरोपीय संघ की तरह, सामान्य डेटा संरक्षण विनियमन (General Data Protection Regulation-GDPR) या अमेरिका के 'क्लैरीफाइंग लॉ फुल ओवरसीज़ यूज़ ऑफ़ डेटा (Clarifying Lawful Overseas Use of Data-CLOUD) अधिनियम की तरह सक्रिय साइबर डिफेंस का अभाव है।
- **विनियामक संगठनों की कार्यप्रणाली में एकरूपता का अभाव**

    संयुक्त राज्य अमेरिका, सिंगापुर और ब्रिटेन में साइबर स्पेस के क्षेत्र में कार्य करने वाला एक ही संगठन है जबकि भारत में कई केंद्रीय निकाय हैं जो साइबर मुद्दों से निपटते हैं। इसलिये प्रत्येक निकाय में एक अलग रिपोर्टिंग संरचना होती है, जिससे विनियामक संगठनों की कार्यप्रणाली में एकरूपता का अभाव नज़र आता है।
- **साइबर सुरक्षा उपकरणों के लिये अन्य देशों पर निर्भरता**
    - भारत में हार्डवेयर के साथ-साथ सॉफ्टवेयर साइबर सुरक्षा उपकरणों में स्वदेशीकरण का अभाव है।
    - यह भारत के साइबर स्पेस को राज्य अभिकर्ताओं और गैर-राज्य अभिकर्ताओं से प्रेरित साइबर हमले से निपटने में दुर्बल कर देता है।
- **वाह्य चुनौतियाँ**

    सोशल मीडिया 'सूचना' के प्रसार का एक शक्तिशाली उपकरण बन रहा है, जिससे भ्रामक समाचार तेज़ी से फैलते हैं, जो साइबर सुरक्षा को खतरा उत्पन्न करते रहते हैं।

साइबर सुरक्षा की दिशा में किये गए सरकार के प्रयास

- भारत में 'सूचना प्रौद्योगिकी अधिनियम, 2000' पारित किया गया जिसके प्रावधानों के साथ-साथ भारतीय दंड संहिता के प्रावधान सम्मिलित रूप से साइबर हमलों के प्रभाव से निपटने के लिये पर्याप्त हैं।
- सूचना प्रौद्योगिकी अधिनियम 2000 की धाराएँ 43, 43ए, 66, 66बी, 66सी, 66डी, 66ई, 66एफ, 67, 67ए, 67बी, 70, 72, 72ए और 74 हैकिंग और साइबर अपराधों से संबंधित हैं।
- सरकार द्वारा **'राष्ट्रीय साइबर सुरक्षा नीति, 2013'** जारी की गई जिसके तहत अति-संवेदनशील सूचनाओं के संरक्षण के लिये **'राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure protection centre-NCIIPC)** का गठन किया।
- इसके अंतर्गत 2 वर्ष से लेकर उम्रकैद तथा दंड अथवा जुर्माने का भी प्रावधान है।

- विभिन्न स्तरों पर सूचना सुरक्षा के क्षेत्र में मानव संसाधन विकसित करने के उद्देश्य से सरकार ने **'सूचना सुरक्षा शिक्षा और जागरूकता'** (Information Security Education and Awareness: ISEA) परियोजना प्रारंभ की है।
- साइबर सुरक्षा के खतरों का विश्लेषण करने, अनुमान लगाने और चेतावनी देने के लिये **भारतीय कंप्यूटर आपात प्रतिक्रिया टीम** (CERT-IN) को नोडल एजेंसी बनाया गया।
- देश में साइबर अपराधों से समन्वित और प्रभावी तरीके से निपटने के लिये 'साइबर स्वच्छता केंद्र' भी स्थापित किया गया है। यह इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय (Ministry of Electronics and Information Technology-MeitY) के तहत भारत सरकार की डिजिटल इंडिया मुहिम का एक हिस्सा है।
- भारत सूचना साझा करने और साइबर सुरक्षा के संदर्भ में सर्वोत्तम कार्य प्रणाली अपनाने के लिये अमेरिका, ब्रिटेन और चीन जैसे देशों के साथ समन्वय कर रहा है।
- सरकार ने साइबर सुरक्षा से संबंधित फ्रेमवर्क का अनुमोदन किया है। इसके लिये **राष्ट्रीय सुरक्षा परिषद सचिवालय** को नोडल एजेंसी बनाया गया है।

आगे की राह

- **जागरूकता में वृद्धि: व्यापारिक संगठनों और सरकारी प्रक्रियाओं को लक्षित करने वाले डिजिटल वारफेयर और हैकर्स के विरुद्ध ठोस उपाय करने के लिये भारत को अन्य देशों के साथ साझा उपाय करने होंगे और इस संदर्भ में जागरूकता में वृद्धि करनी होगी कि कोई भी व्यक्ति या संस्था अकेले डिजिटल वारफेयर के प्रति प्रतिरक्षित नहीं है।**
- मौजूदा साइबर सुरक्षा ढाँचे को मजबूत करना: राष्ट्रीय साइबर समन्वय केंद्र (National Cyber Coordination Centre-NCCC), नेशनल क्रिटिकल इन्फॉर्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर (National Critical Information Infrastructure Protection Centre-NCIIPC) और कंप्यूटर इमरजेंसी रिस्पांस टीम (Computer Emergency Response Team-CERT) जैसी राष्ट्रीय साइबर सुरक्षा परियोजनाओं को कई गुना मजबूत करने की आवश्यकता है।
- शैक्षिक पाठ्यक्रमों में साइबर सुरक्षा को शामिल करना: केंद्रीय विश्वविद्यालयों, निजी विश्वविद्यालयों, उद्योग संघों, औद्योगिक प्रशिक्षण संस्थानों सहित अन्य शैक्षिक संस्थानों को साइबर सुरक्षा को पाठ्यक्रमों को शामिल करना चाहिये।
- **एकीकृत दृष्टिकोण:** मोबाइल फोन और दूरसंचार के बढ़ते प्रभाव को देखते हुए राष्ट्रीय साइबर सुरक्षा नीति और राष्ट्रीय दूरसंचार नीति को वर्ष 2030 तक एक व्यापक समग्र नीति के निर्माण हेतु प्रभावी रूप से सहयोग करना होगा।

प्रश्न- भारत को साइबर सुरक्षा ढाँचे के अद्यतनीकरण की आवश्यकता क्यों है? साइबर सुरक्षा के क्षेत्र में विभिन्न चुनौतियों का उल्लेख करते हुए इसके समाधान हेतु किये जा रहे प्रयासों पर चर्चा कीजिये।