साइबर हमले का बढ़ता खतरा

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

संदर्भ

भारत सरकार ने **राष्ट्रीय साइबर सुरक्षा समन्वयक के दिशा-निर्देशन में एक विशेषज्ञ समिति** का गठन किया है जिसका उद्देश्य चीन की सरकार से संबंधित उन चीनी प्रौद्योगिकी कंपनियों के संबंध में जानकारी एकत्र करना है जिन पर भारतीय नागरिकों और संगठनों की निगरानी करने का आरोप लगा है। भारत एकमात्र ऐसा देश नहीं है जो इस तरह के साइबर हमले के खतरे से चिंतित है। हाल ही में **संयुक्त राज्य अमेरिका के रक्षा विभाग** (Department of Defence-DoD) ने लोगों और संगठनों की निज़ी एवं गुप्त सूचनाओं को चोरी करने वाले मालवेयर (वायरस) **स्लॉथफुलमीडिया (SlothfulMedia)** की पहचान उजागर की, जिसमें यह बताया गया कि इस मालवेयर का प्रयोग भारत, कज़ाकिस्तान, किर्गिस्तान, मलेशिया, रूस और यूक्रेन में नागरिकों और संवेदनशील रक्षा प्रतिष्ठानों को लक्षय बनाकर साइबर हमले प्रारंभ करने के लिये किया जा रहा था।

यद्यपि संयुक्त राज्य अमेरिका के रक्षा विभाग ने अभी तक इस मालवेयर के स्रोत की जानकारी नहीं दी है, परंतु पूर्व में चीन, रूस, उत्तरी अमेरिका एवं ईरान द्वारा इस तरह के साइबर हमलों को अंजाम दिया गया था। इसका एक ताज़ा उदाहरण वर्ष 2016 में अमेरिकी राष्ट्रपति चुनाव को प्रभावित करने के रूप में देखा जा सकता है।

साइबर हमले से तात्पर्य?

- **'साइबर हमला'** वाक्यांश का प्रयोग आतंकवादी गतिविधियों में इंटरनेट के माध्यम से किये जाने वाले हमलों को संबोधित करने के लिये किया जाता है। इनमें कंप्यूटर वायरस जैसे साधनों के माध्यम से कंप्यूटर नेटवर्क में जान-बूझकर बड़े पैमाने पर किया गया व्यवधान शामिल है, विशेष रूप से इंटरनेट से जुड़े किसी निजी कंप्यूटर में।
- साइबर हमले साइबर जगत में विरोधियों के बीच होने वाली एक रणनीतिक प्रतियोगिता है। इसके माध्यम से विभिन्न देश व्यापक स्तर पर अपने देश के नागरिकों या अन्य देशों के नागरिकों या रक्षा प्रतिष्ठानों की गोपनीय सूचनाएँ एकत्र करने में सक्षम हो जाते हैं।

- साइबर हमले को किसी कंप्यूटर अपराध के रूप में और अधिक सामान्य तरीके से इस प्रकार परिभाषित किया जा सकता है..."**वास्तविक दुनिया के बुनियादी ढाँचे, संपत्ति तथा किसी के जीवन को हानि पहुँचाए बिना किसी कंप्यूटर नेटवर्क को लक्षित कर उसे क्षति पहुँचाना ।**"

साइबर हमले की व्यापकता

- साइबर हमले का क्षेत्र अति व्यापक है, यह सामाजिक, आर्थिक, राजनीतिक, सांस्कृतिक/बौद्धिक तथा सैन्य क्षेत्रों को काफी हानि पहुँचा सकता है। संयुक्त राज्य अमेरिका में 85 प्रतिशत साइबर हमले आर्थिक क्षेत्र से संबंध रखने वाले प्रतिष्ठानों जैसे- छोटे बैंक और गैर बैंकिंग वित्तीय कंपनियों में हुए।
- संयुक्त राज्य अमेरिका ने एक एडवाइज़री जारी करते हुए बताया कि उत्तर कोरिया का एक हैकिंग ग्रुप **बीगल बॉयज़** (BeagleBoyz) भारत समेत विभिन्न देशों की बैंकिंग प्रणाली को **हैक** करने का प्रयास कर रहा है।

हैकिंग

हैकिंग एक ऐसी प्रक्रिया है जिसमें हैकिंग करने वाला किसी अन्य व्यक्ति की जानकारी को बिना उसकी इजाज़त के चोरी करता है। ऐसा करने के लिये वह उस व्यक्ति की निजी जानकारियों में सेंध लगाकर उन्हें हैक करता है। हैकिंग को गैर-कानूनीमाना गया है, लेकिन कई बार हैकिंग अच्छे काम के लिये भी की जाती है। इसके माध्यम से साइबर अपराधियों द्वारा कई प्रकार के अपराध किये जाते हैं।

- अमेरिकी न्याय प्रशासन ने पाँच चीनी सैन्य अधिकारियों पर अभियोग चलाया जिन पर यूएस स्टील (US Steel), जे.पी. मॉर्गन (JP Morgan), वेस्टिंगहाउस इलेक्ट्रिकल (Westinghouse Electrical), सोलर वर्ल्ड (SolarWorld) और यूनाइटेड स्टीलवर्कर्स (United Steelworkers) जैसी कंपनियों के डेटा चोरी का आरोप था।
- सैन्य क्षेत्र में साइबर हमले साइबर वॉरफेयर के सर्वाधिक संवेदनशील क्षेत्रों में से एक हैं। कुछ समय पूर्व ही रूस की इंटेलीजेंस एजेंसी से संबंधित **सैंडवर्म टीम** (Sandworm Team) ने संयुक्त राज्य अमेरिका, पोलैंड, यूक्रेन, यूरोपियन यूनियन और नाटो से संबंधित सैन्य प्रतिष्ठानों पर साइबर हमले किये थे।

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 के रूप 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-IoTs) 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**
  - 21वीं सदी में डेटा, मुद्रा के समान महत्त्वपूर्ण हो गया है। भारत की विशाल जनसंख्या के कारण कई अंतर्राष्ट्रीय कंपनियाँ (जैसे-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 के समक्ष चुनौतियाँ

- **मानव संसाधन 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-IoTs) 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।
- **साइबर सक्रिय डिफेंस का अभाव**

  भारत में यूरोपीय संघ की तरह, सामान्य डेटा संरक्षण विनियमन (General Data Protection Regulation-GDPR) या अमेरिका के 'क्लेरिफाइंग लॉ फुल ओवरसीज़ यूज़ ऑफ 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, ब्रिटेन और सिंगापुर में साइबर स्पेस के क्षेत्र में कार्य करने वाला एक ही संगठन है। जबकि भारत में कई केंद्रीय संगठन हैं जो साइबर मुद्दों से निपटते हैं, इसलिये प्रत्येक संगठन में रिपोर्टिंग की प्रक्रिया अलग-अलग होती है, यही कारण है कि इन संगठनों की कार्यप्रणाली में एकरूपता का अभाव है।
- **फेक न्यूज़**

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

साइबर सुरक्षा को मज़बूत करने की दिशा में 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, 43A, 66, 66B, 66C, 66D, 66E, 66F, 67, 67A, 67B, 70, 72, 72A 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 अति-संवेदनशील सूचना अवसंरचना संरक्षण केंद्र** (National Critical Information Infrastructure protection centre-NCIIPC) का गठन किया गया।
- इसके अंतर्गत 2 वर्ष की 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।

आगे की राह

- वित्तीय 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।
- **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 मज़बूत करने की आवश्यकता है।
- 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- 'वर्तमान डिजिटल युग के दौर में साइबर सुरक्षा एक महत्त्वपूर्ण डोमेन बनकर उभरा है।' साइबर सुरक्षा से संबंधित चुनौतियों का उल्लेख करते हुए इसके समाधान की दिशा में किये जा रहे प्रयासों का वर्णन कीजिये।