साइबर सुरक्षा को मजबूत करना

प्रश्न पत्र- 3 (साइबर अपराध और सुरक्षा)

चर्चा में क्यों?

➤ लगभग 30 मिलियन रेल यात्रियों के निजी डेटा की बिक्री के लिए कथित अवैध प्रस्ताव, एक असुरक्षित किन्तु डिजिटल रूप से सक्षम अर्थव्यवस्था के खतरों को उजागर करने वाली नवीनतम घटना है।

पूर्व की घटनाएं :

➤ यह उल्लंघन का मामला देश के शीर्ष चिकित्सा संस्थान (AIIMS) पर साइबर-रैनसम हमले के बाद आया है।

हाल की चिंताएँ:

➤ भारत में बहुत अधिक संख्या में साइबर फिरौती के हमले दर्ज किए जाते हैं। साइबर अपराध की ये दो घटनाएं हिमशैल की सर्वोच्च चोटी के समान दृश्यमान हैं।

➤ भारत वैश्विक साइबर अपराध के लिए एक प्रमुख केंद्र बन गया है और साइबर अपराधों की बढ़ती संख्या इसे और अधिक संवेदनशील बनाते हैं।

➤ इसमें विधायी कमियां हैं कि भारत में व्यक्तिगत डेटा संरक्षण कानून नहीं है।

➤ व्यक्तिगत डेटा के बड़े डेटाबेस नियमित रूप से, कमोबेश खुले एवं सामान्य तौर पर बेचे जाते हैं।

➤ कई क्षेत्रों में छोटे पैमाने पर असंख्य डेटा लीक हुए हैं।इसके पीछे फ़िशिंग स्कैम और साइबरसेक्स ब्लैकमेल रैकेट चलाने वाले संगठित गिरोह शामिल हैं।

साइबर हमलों में वृद्धि के कारण

डेटा की सस्ती पहुंच:

➤ डेटा टैरिफ के मामले में भारत दुनिया का सबसे सस्ता स्थान है। यह उच्चतम प्रति व्यक्ति डेटा खपत वाला देश भी है।जैसे-जैसे 5जी और सैटेलाइट ब्रॉडबैंड जैसी नई उच्च-गति की इंटरनेट प्रौद्योगिकियां शुरू हो रही हैं,वैसे- वैसे डेटा उत्पादन तथासाइबर अपराध में भी में तेजी से वृद्धि होने की संभावना है।

प्रौद्योगिकी पर बढ़ती निर्भरता:

➤ जैसे-जैसे हम तेजी से आगे बढ़ रहे हैं, अधिक से अधिक सिस्टम्स को वर्चुअल स्पेस में स्थानांतरित किया जा रहा है, ताकि पहुंच और उपयोग में सुगमता को बढ़ावा दिया जा सके। हालाँकि, इस प्रवृत्ति का नकारात्मक पक्ष साइबर हमलों के लिए ऐसी प्रणालियों की बढ़ती भेद्यता है।

असममित और गुप्त युद्ध:

- जानमाल के नुकसान के साथ पारंपरिक युद्ध के विपरीत, साइबर युद्ध प्रशंसनीय खंडन के दायरे के साथ गुप्त युद्ध है, यानी पकड़े जाने पर भी सरकारें उनकी भागीदारी से इनकार कर सकती हैं। इसलिए, राष्ट्रों के बीच संघर्ष के लिए साइबर युद्ध तेजी से चुना गया स्थान बन गया है।

चीन के साथ प्रतिकूल संबंध:

- सूचना प्रौद्योगिकी में चीन को वैश्विक नेताओं में से एक माना जाता है। इसलिए, इसके पास किसी दूसरे देश में सूचना प्रौद्योगिकी सेवाओं को अक्षम या आंशिक रूप से बाधित करने की क्षमता होने की उम्मीद है।

साइबर सुरक्षा के साथ चुनौतियां

साइबर सुरक्षा के लिए जागरूकता की कमी:

- डिजिटल रूप से सक्षम अर्थव्यवस्था में, जहाँ लेन-देन का एक उच्च और बढ़ता अनुपात डिजिटल है, साइबर सुरक्षा की आवश्यकता के बारे में जागरूकता की कमी है।

सिस्टम में कमजोर बिंदु:

- सिस्टम में कमजोर बिंदुओं को खोजने और उनका पता लगाने की आवश्यकता है, जो सिस्टम में अनधिकृत प्रवेश की अनुमति दे सकते हैं। उदाहरण के लिए, यह उम्मीद की जाती है कि संवेदनशील परमाणु डेटा को भारी एन्क्रिप्शन द्वारा संरक्षित किया जाता है, लेकिन उपयोगकर्त्ता सिस्टम तक पहुँचने के दौरान मानवीय त्रुटियों के प्रति संवेदनशील हो सकते हैं।

राज्य प्रायोजित साइबर हमले:

- इस तरह के राज्य-प्रायोजित हमलों के साथ समस्या हैकर्स द्वारा विदेशी प्रणालियों में सेंध लगाने के लिए प्राप्त असीमित धन है। इसका मतलब यह है कि चीन या अन्य देशों से ऐसे खतरों का मुकाबला करने के लिए, भारत को पर्याप्त संसाधन आवंटित करने की आवश्यकता है, जो आनुपातिक रूप से सिस्टम को समझौता करने से रोक सके।

आम जनता के बीच कम डिजिटल साक्षरता:

- अक्सर यह बताया जाता है कि दिलचस्प सामग्री पर क्लिक करने के लिए लोगों को क्लिक-बेट करके आसानी से धोखा दिया जाता है, जिसमें अक्सर मैलवेयर जुड़ा होता है।

साइबर सुरक्षा सुनिश्चित करने के लिए सरकार के कदम

नवीनतम पहलें:

- डिजिटल इंडिया पहल का उद्देश्य सरकारी सेवाओं के पूरे स्पेक्ट्रम को ऑनलाइन वितरित करना है। साथ ही इसका उद्देश्य निजी क्षेत्र द्वारा पेश किए जाने वाले उत्पादों और सेवाओं की पूरी श्रृंखला में कैशलेस डिजिटल अर्थव्यवस्था को संचालित करना भी है।
- यूनिफाइड पेमेंट्स इंटरफेस (UPI) कई अलग-अलग फिनटेक सेवा प्रदाताओं को एक साथ जोड़ता है और ये वित्तीय संस्थाएं प्रतिदिन अरबों का लेनदेन करती हैं।
- डिजिटल कॉमर्स के लिए ओपन नेटवर्क (ONDC) इस मायने में और भी अधिक महत्वाकांक्षी है कि यह रिटेल और ई-कॉमर्स स्पेस में एंड-टू-एंड सीमलेस लॉजिस्टिक्स और लेन-देन क्षमता की संकल्पना करता है।

संस्थागत संरचना:

- भारत में देश भर में राष्ट्रीय सूचना प्रौद्योगिकी प्रणालियों को विनियमित और मजबूत करने के लिए एक सुव्यवस्थित संरचना है। इसमें शामिल है राष्ट्रीय साइबर सुरक्षा परिषद के साथ-साथ कंप्यूटर इमरजेंसी रिस्पांस टीम - भारत (cert-in)।

व्यक्तिगत डेटा संरक्षण विधेयक:

- यह विधेयक निजी कंपनियों द्वारा व्यक्तियों के डेटा की सुरक्षा के लिए डेटा इन्फ्रास्ट्रक्चर को मजबूत करने का आदेश देता है। इसलिए, इसे केवल सरकार तक सीमित करने के बजाय डेटा संरक्षण के दायरे में निजी कंपनियों को शामिल करने पर ध्यान दिया जा रहा है।

संभावित रूप से असुरक्षित ऐप्स पर प्रतिबंध लगाना:

- भारत ने कई ऐप (ज्यादातर चीनी मूल के) पर प्रतिबंध लगा दिया था, जो भारतीय नागरिकों द्वारा उपयोग के लिए असुरक्षित पाए गए थे।ऐप्स कथित तौर पर डेटा को भारत के बाहर स्थित सर्वरों में स्थानांतरित कर रहे थे और यह सुनिश्चित करने के लिए उचित सुरक्षा उपाय नहीं थे कि भारतीय नागरिकों के निजी डेटा को अनधिकृत पहुंच से सुरक्षित रखा जाए।

आगामी साइबर सुरक्षा रणनीति:

- साइबर सुरक्षा रणनीति का उद्देश्य साइबर हमलों से निपटने और देश में साइबर स्पेस को सुरक्षित करने की तैयारी के लिए एक व्यापक दस्तावेज तैयार करना है।
- उदाहरण के लिए, यह रणनीति साइबर हमलों के क्षेत्र में तीन चरणों की पहचान करती है:

पूर्व हमला या प्रारंभिक चरण:

- इस चरण में, सिस्टम के अंतराल की पहचान की जाती है और उन्हें प्लग इन किया जाता है।
- इसका फोकस रक्षा तंत्र और फायरवॉल को मजबूत करने तथा सिस्टम को अद्यतित रखने पर है ताकि किसी भी संभावित खतरे को टाला जा सके एवं सिस्टम से समझौता न किया जा सके।

हमले के दौरान:

- हमले के समय, इसे जल्द से जल्द रोकने और सिस्टम को होने वाले नुकसान को कम करने पर ध्यान दिया जाता है।साथ ही, यह भी सुनिश्चित किया जाना चाहिए कि महत्वपूर्ण संपत्तियां और डेटा हमले में नष्ट न हों।
- जब हमलावरों को सिस्टम से बाहर कर दिया जाता है, तो फोकस सेवाओं को बहाल करने के लिए स्थानांतरित हो जाता है , ताकि उपभोक्ताओं को लंबे समय तक आउटेज का सामना न करना पड़े।

हमले के बाद का चरण:

- हमले के समाप्त होने के बाद सिस्टम को सामान्य स्थिति में बहाल कर दिया जाता है तथा सिस्टम में खामियों या अंतराल की पहचान करने पर ध्यान केंद्रित किया जाता है। यह समझने का प्रयास किया जाता है कि कैसे प्रतिक्रिया अधिक तेज हो सकती है और इस तरह के भविष्य के हमलों के मामले में कौन सी मानक संचालन प्रक्रिया (SOP) का निर्माण किया जा सकता है।

आगे की राह

- **नीतिगत पारिस्थितिकी तंत्र को मजबूत बनाना:** समय की आवश्यकता है कि हमें भावी राष्ट्रीय साइबर-सुरक्षा नीति के साथ आगे आना होगा जो पर्याप्त संसाधन आवंटित करती है और हितधारकों की चिंताओं को दूर करती है।
- साथ ही एक व्यक्तिगत डेटा संरक्षण कानून को शीघ्र लागू करने की आवश्यकता है।

मुख्य परीक्षा अभ्यास प्रश्न

प्रश्न- अधिक मजबूत साइबर सुरक्षा व्यवस्था सुनिश्चित करने के लिए भारत में जल्द से जल्द एक व्यक्तिगत डेटा संरक्षण कानून लागू करने की आवश्यकता है। चर्चा कीजिए।