भारत की साइबर सुरक्षा पर पुनर्विचार

यह एडिटोरियल 04/12/2022 को 'हिंदुस्तान टाइम्स' में प्रकाशित "The AIIMS attack shows the importance of a robust cybersecurity framework" लेख पर आधारित है। इसमें एम्स के सर्वर पर रैनसमवेयर हमले और भारत के साइबरस्पेस से संबंधित चुनौतियों के बारे में चर्चा की गई है।

संदर्भ

आज इंटरनेट हमारे दैनिक जीवन के अभिन्न अंगों में से एक बन गया है। वह हमारे दैनिक जीवन के अधिकांश पहलुओं को प्रभावित कर रहा है। साइबरस्पेस हमें वर्चुअल रूप से दुनिया भर के करोड़ों ऑनलाइन उपयोगकर्त्ताओं से जोड़ता है।

- जैसे-जैसे भारत का इंटरनेट आधार बढ़ता जा रहा है (वर्ष 2025 तक 900 करोड़ से अधिक इंटरनेट उपयोगकर्त्ता होने के अनुमान के साथ), साइबर खतरों में भी चिंताजनक रूप से वृद्धि हो रही है। डिजिटल प्रौद्योगिकी की प्रगति के साथ साइबर अपराधों का परिष्करण भी बढ़ रहा है।
- इस परिदृश्य में यह अनिवार्य है कि भारत अपने साइबरस्पेस में विद्यमान खामियों पर सूक्ष्मता से विचार करे और एक अधिक व्यापक साइबर-सुरक्षा नीति के माध्यम से उन्हें समग्र रूप से संबोधित करे।

साइबर सुरक्षा क्या है?

- साइबर सुरक्षा (Cyber Security) या सूचना प्रौद्योगिकी सुरक्षा (Information Technology Security) कंप्यूटर, नेटवर्क, प्रोग्राम और डेटा को अनधिकृत पहुँच या हमलों से बचाने की तकनीकें हैं जो साइबर-भौतिक प्रणालियों (Cyber-Physical Systems) और महत्त्वपूर्ण सूचना अवसंरचना के दोहन पर लक्षित हैं।
  - **महत्त्वपूर्ण सूचना अवसंरचना (Critical Information Infrastructure):** सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70(1) महत्त्वपूर्ण सूचना अवसंरचना को एक कंप्यूटर संसाधन के रूप में परिभाषित करती है, जिसकी अक्षमता या विनाश का राष्ट्रीय सुरक्षा, अर्थव्यवस्था, सार्वजनिक स्वास्थ्य या सुरक्षा पर कारी प्रभाव पड़ेगा।

भारत में साइबर हमलों के हाल के कुछ उदाहरण

- वर्ष 2020 में लगभग 82% भारतीय कंपनियों को रैनसमवेयर हमलों का सामना करना पड़ा।
  - मई 2017 में भारत के पाँच प्रमुख शहर (कोलकाता, दिल्ली, भुवनेश्वर, पुणे और मुंबई) 'WannaCry' रैनसमवेयर हमले से प्रभावित हुए।
  - हाल में एम्स, दिल्ली पर रैनसमवेयर हमला हुआ है। देश के इस शीर्ष चिकित्सा संस्थान के सर्वर पर रैनसमवेयर हमले के बाद लाखों मरीजों का व्यक्तिगत डेटा खतरे में है।
- वर्ष 2021 में एक हाई-प्रोफाइल भारत-आधारित भुगतान कंपनी 'Juspay' को डेटा उल्लंघन का सामना करना पड़ा जिसमें 35 मिलियन ग्राहक प्रभावित हुए।
  - यह उल्लंघन अत्यंत चिंताजनक है क्योंकि 'Juspay' अमेज़न और कई अन्य बड़ी कंपनियों के ऑनलाइन मार्केटप्लेस के लिये भुगतान से संलग्न है।
- फरवरी 2022 में एयर इंडिया को एक बड़े साइबर हमले का सामना करना पड़ा जहाँ लगभग 4.5 मिलियन ग्राहक रिकॉर्ड के लिये खतरा उत्पन्न हुआ। यहाँ पासपोर्ट, टिकट और क्रेडिट कार्ड संबंधी सूचना की गुप्तता भंग हुई।

साइबर खतरों के प्रमुख प्रकार

- **रैनसमवेयर (Ransomware):** इस प्रकार का मैलवेयर कंप्यूटर डेटा को हाईजैक कर लेता है और फिर उसे पुनर्स्थापित करने के लिये भुगतान (आमतौर पर बिटकॉइन के रूप में) की मांग करता है।
- **ट्रोजन हॉर्सेज़ (Trojan Horses):** ट्रोजन हॉर्स अटैक एक दुर्भावनापूर्ण प्रोग्राम का उपयोग करता है जो एक वैध प्रतीत होने वाले प्रोग्राम के अंदर छिपा होता है।
  - जब उपयोगकर्त्ता संभवतः निर्दोष और वैध प्रोग्राम को निष्पादित करता है तो ट्रोजन के अंदर गुप्त रूप से शामिल मैलवेयर का उपयोग

सिस्टम में बैकडोर को खोलने के लिये किया जा सकता है जिसके माध्यम से हैकर्स कंप्यूटर या नेटवर्क में प्रवेश कर सकते हैं।

- **क्लिकजैकिंग (Clickjacking):** यह इंटरनेट उपयोगकर्त्ताओं को दुर्भावनापूर्ण सॉफ्टवेयर वाले लिंक पर क्लिक करने या अनजाने में सोशल मीडिया साइटों पर निजी जानकारी साझा करने के लिये लुभाने का कृत्य है।
- **डिनायल ऑफ सर्विस (DOS) हमला:** यह किसी सेवा को बाधित करने के उद्देश्य से कई कंप्यूटरों और मार्गों से वेबसाइट जैसी किसी विशेष सेवा को ओवरलोड करने का जानबूझकर कर किया जाने वाला कृत्य है।
- **मैन इन मिड्ल अटैक' (Man in Middle Attack):** इस तरह के हमले में दो पक्षों के बीच संदेशों को पारगमन के दौरान 'इंटरसेप्ट' किया जाता है।
- **क्रिप्टोजैकिंग (Cryptojacking):** क्रिप्टोजैकिंग शब्द क्रिप्टोकरेंसी से निकटता से संबद्ध है। क्रिप्टोजैकिंग वह स्थिति है जब हमलावर क्रिप्टोकरेंसी माइनिंग के लिये किसी और के कंप्यूटर का उपयोग करते हैं।
- **'ज़ीरो डे वल्नेरेबिलिटी' (Zero Day Vulnerability):** ज़ीरो डे वल्नेरेबिलिटी मशीन/नेटवर्क के ऑपरेटिंग सिस्टम या ऐप्लीकेशन सॉफ्टवेयर में व्याप्त ऐसा दोष है जिसे डेवलपर द्वारा ठीक नहीं किया गया है और ऐसे हैकर द्वारा इसका दुरुपयोग किया जा सकता है जो इसके बारे में जानता है।

भारत के साइबरस्पेस से संबंधित चुनौतियाँ

- **क्षमता की वृद्धि, भेद्यता का विस्तार:** नागरिकों के डिजिटल एकीकरण के साथ भारत की डिजिटल अर्थव्यवस्था फली-फूली है, लेकिन इसने डेटा चोरी की भेद्यता भी पैदा की है।
  - सरकार विभिन्न क्षेत्रों में 'डेटा प्रवाह' के लिये सभी बाधाओं को दूर करने की अपेक्षा करती थी। इस आख्यान के परिणामस्वरूप टेक-उद्योग ने डेटा संरक्षण के प्रति केवल खानापूरी ही की है।
- **विदेशों में डेटा का संग्रहण:** लगभग प्रत्येक क्षेत्र में ही डिजिटलीकरण की ओर बढ़ने की होड़ ने भारत के बाहर एप्लीकेशन सेवा प्रदाताओं के साथ सहयोग को बल दिया है, ताकि ग्राहक शीघ्रातिशीघ्र सर्वोत्तम ऐप्स और सेवाओं तक पहुँच सकें।
  - विदेशी स्रोतों से प्राप्त हार्डवेयर एवं सॉफ्टवेयर या भारत के बाहर के सर्वरों पर भारी मात्रा में डेटा की पार्किंग हमारे राष्ट्रीय साइबरस्पेस के लिये खतरा पैदा करता है।
- **प्रॉक्सी साइबर अटैक:** कृत्रिम बुद्धिमत्ता (AI) स्वचालित घातक हथियार प्रणाली के निर्माण में सक्षम है जो मानव संलग्नता के बिना ही जीवन और लक्ष्य को नष्ट कर सकती है।
  - नकली डिजिटल मुद्रा और नवीनतम साइबर प्रौद्योगिकियों की सहायता से बौद्धिक संपदा की चोरी जैसी अवैध गतिविधियों की भेद्यता से भी राष्ट्रीय सुरक्षा के लिये खतरा उत्पन्न हुआ है।
- **चीन की क्वांटम बढ़त:** चीन की क्वांटम प्रगति भारत की डिजिटल अवसंरचना पर क्वांटम साइबर हमले की संभावना का विस्तार करती है, जो पहले से ही चीनी राज्य-प्रायोजित हैकरों के हमलों का सामना कर रही है।
  - विदेशी हार्डवेयर, विशेष रूप से चीनी हार्डवेयर पर भारत की निर्भरता एक अतिरिक्त भेद्यता का निर्माण करती है।

साइबर सुरक्षा से संबंधित सरकार की वर्तमान पहलें

- भारतीय साइबर अपराध समन्वय केंद्र (I4C)
- भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In)
- साइबर सुरक्षित भारत
- साइबर स्वच्छता केंद्र
- राष्ट्रीय साइबर सुरक्षा समन्वय केंद्र (NCCC)

आगे की राह

- **साइबर-जागरूकता:** शिक्षा साइबर-अपराधों की रोकथाम के बारे में सूचना के प्रसार के लिये महत्त्वपूर्ण क्षेत्रों में से एक है और युवा आबादी साइबरस्पेस में अपनी भागीदारी के बारे में जागरूक होने तथा साइबर सुरक्षा के लिये और साइबर अपराध रोकने के लिये एक पारिस्थितिकी तंत्र का निर्माण करने के लिये बल गुणक के रूप में कार्य कर सकती है।
- **सुरक्षित वैश्विक साइबरस्पेस के लिये टेक-डिप्लोमेसी:** उभरते सीमा-पार साइबर खतरों से निपटने के लिये और एक सुरक्षित वैश्विक साइबरस्पेस की ओर आगे बढ़ने के लिये भारत को उन्नत अर्थव्यवस्थाओं तथा प्रौद्योगिकी-उन्मुख लोकतंत्रों (Techno-) के साथ अपनी राजनयिक साझेदारी को सुदृढ़ करना चाहिये।
- **सहकारी संघवाद और साइबर सुरक्षा:** पुलिस और लोक व्यवस्था राज्य सूची के विषय हैं, इसलिये राज्यों को यह सुनिश्चित करना चाहिये कि साइबर अपराध से निपटने के लिये विधि प्रवर्तन पूर्ण सक्षम है।
  - आईटी अधिनियम और अन्य प्रमुख कानून केंद्रीय रूप से अधिनियमित किये जाते हैं, इसलिये केंद्र सरकार कानून प्रवर्तन के लिये सार्वभौमिक वैधानिक प्रक्रियाएँ विकसित कर सकती है।
  - इसके साथ ही, केंद्र और राज्यों को आवश्यक साइबर अवसंरचना विकसित करने के लिये पर्याप्त धन का निवेश करना चाहिये।
- **अनिवार्य डेटा संरक्षण मानदंड:** व्यक्तिगत डेटा से संलग्न सभी सरकारी और निजी एजेंसियों के लिये अनिवार्य डेटा सुरक्षा मानदंडों का पालन करना आवश्यक होना चाहिये।
  - मानदंडों का अनुपालन सुनिश्चित करने के लिये संबंधित प्राधिकारों को नियमित रूप से डेटा सुरक्षा ऑडिट करना चाहिये।

अभ्यास प्रश्न: जैसे-जैसे आधुनिक साइबर प्रौद्योगिकी विभिन्न क्षेत्रों में भारत की क्षमता को कई गुना बढ़ा रही है, वैसे-वैसे यह इसकी भेद्यताओं में भी वृद्धि कर रही है। टिप्पणी कीजिये।

यूपीएससी सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न (PYQ)

??????????? ????????

Q.1 भारत में, व्यक्तियों के लिए साइबर बीमा के तहत, धन की हानि और अन्य लाभों के भुगतान के अलावा, निम्नलिखित में से कौन से लाभ आम तौर पर कवर किये जाते हैं? (वर्ष 2020)

1. किसी के कंप्यूटर तक पहुँच को बाधित करने वाले मैलवेयर के मामले में कंप्यूटर सिस्टम की बहाली की लागत।
2. एक नए कंप्यूटर की लागत अगर ऐसा साबित हो जाता है कि कुछ असामाजिक तत्त्वों ने जानबूझकर इसे नुकसान पहुँचाया है।
3. साइबर जबरन वसूली के मामले में नुकसान को कम करने के लिए एक विशेष सलाहकार को काम पर रखने की लागत
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव की लागत

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(A) केवल 1, 2 और 4
(B) केवल 1, 3 और 4
(C) केवल 2 और 3
(D) 1, 2, 3 और 4

उत्तर: (B)

Q.2 भारत में निम्नलिखित में से किसके लिये साइबर सुरक्षा घटनाओं पर रिपोर्ट करना कानूनी रूप से अनिवार्य है? (वर्ष 2017)

1. सेवा प्रदाता
2. डेटा केंद्र
3. निगमित निकाय

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(A) केवल 1
(B) केवल 1 और 2
(C) केवल 3
(D) 1, 2 और 3

उत्तर: (D)

????? ????????

Q. साइबर सुरक्षा के विभिन्न घटक क्या हैं? साइबर सुरक्षा में चुनौतियों को ध्यान में रखते हुए जाँच करें कि भारत ने व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति को किस हद तक सफलतापूर्वक विकसित किया है। (वर्ष 2022)