भारत में सुरक्षित साइबरस्पेस

यह एडिटोरियल 17/10/2022 को 'इंडियन एक्सप्रेस' में प्रकाशित "Securing India's cyberspace from quantum techniques" लेख पर आधारित है। इसमें भारत के साइबरस्पेस से संबंधित मुद्दों और क्वांटम प्रौद्योगिकी के उभार के बारे में चर्चा की गई है।

संदर्भ

प्रौद्योगिकी के क्षेत्र में अभूतपूर्व विकास ने लोगों को एक-दूसरे से जोड़ने और शासन को रूपांतरित करने के रूप में सीमाओं को धुंधला कर दिया है। भारत सरकार द्वारा शुरू किया गया 'डिजिटल इंडिया' कार्यक्रम—जिसका उद्देश्य सरकारी सेवाओं को डिजिटल रूप में प्रदान करना और डिजिटल साक्षरता को बढ़ावा देना है—देश के लिये विश्वस्तरीय डिजिटल अवसंरचना के निर्माण के माध्यम से इस रूपांतरण को गति दे रहा है।

- हालाँकि अभी ऐसे अंतराल मौजूद हैं जिनका शत्रुओं द्वारा लाभ उठाया जा सकता है और हमें डिजिटल प्रौद्योगिकियों के लाभों से वंचित किया जा सकता है। साइबर शत्रु अधिक परिष्कृत और साधन संपन्न बनते जा रहे हैं। हाल में 'WannaCry' नामक एक उन्नत रैंसमवेयर हमले की चपेट में 100 से अधिक देश आए जिनमें भारत तीसरा सर्वाधिक प्रभावित देश रहा था।
- चूँकि टेक्नोलॉजी प्रोटोकॉल अभी भी विकासावस्था में हैं और धीमी गति से इनका उभार हो रहा है, ऐसे साइबर हमलों से बचना बेहद कठिन है। इस परिदृश्य में, चूँकि भारत एक डिजीटल जीवन की ओर आगे बढ़ रहा है जहाँ अस्तित्व क्लाउड कंप्यूटिंग, दूरसंचार क्षेत्र में 5G, ई-कॉमर्स और क्वांटम प्रौद्योगिकी आदि पर अत्यधिक निर्भर होगा, उसके लिये खामियों और अंतराल पर नियंत्रण रखना अनिवार्य होगा।

साइबर खतरों से संबंधित प्रमुख शब्दावली

- **क्लिकिजैकिंग (Clickjacking):** यह इंटरनेट उपयोगकर्ताओं 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:** 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।
- **'मैन इन मिडिल अटैक' (Man in Middle Attack):** इस तरह के हमले में दो पक्षों के बीच संदेशों को पारगमन के दौरान 'इंटरसेप्ट' किया जाता है।
- **रैंसमवेयर (Ransomware):** यह मैलवेयर का एक रूप है जहाँ हले कंप्यूटर के डेटा को हाईजैक किया जाता है और फिर इसे पुनर्स्थापित करने के लिये पैसे की मांग (आमतौर पर बिटिकॉइन के रूप में) संबंधी संदेश पोस्ट किया जाता है।
- सपाइवेयर (Spyware): ऐसा मैलवेयर जो उपयोगकर्ता की कंप्यूटर गतिविधियों पर गुप्त रूप से नज़र रखता है।
- **'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 साइबर स्पेस से संबंधित प्रमुख चुनौतियाँ

- **इंटरनेट ध्रुवीकरण (Internet Polarisation):** वर्तमान में इंटरनेट को विनियमित करने वाले कोई सामान्य नियम और मानदंड मौजूद नहीं हैं, इसलिये यह विज्ञापन-आधारित प्रौद्योगिकी के माध्यम से कुछ वेबसाइटों के अन्य के ऊपर अवैध ध्रुवीकरण को सक्षम बनाता है, दर्शकों को ब्राउज़ करने के लिये विवश करता है और इंटरनेट लोकतंत्र को कमज़ोर करता है।
- **क्षमता वृद्धि, भेद्यता वृद्धि:** नए संस्करण में प्रगति के साथ-साथ कृत्रिम बुद्धिमत्ता (AI) हमें जीवन को पुनर्परिभाषित और पुनर्गठित करने की अपार शक्ति प्रदान करती है।
    - AI स्वायत्त घातक हथियार प्रणालियों का उत्पादन करने में सक्षम है जो बिना किसी मानवीय हस्तक्षेप के जीवन और लक्ष्यों को नष्ट कर सकते हैं।
    - ड्रग्स, नकली करेंसी से लेकर बौद्धिक संपदा की चोरी तक विभिन्न अवैध गतिविधियों की भेद्यता राष्ट्रीय सुरक्षा के लिये भी प्रमुख चिंता का विषय है।
- **साइबर युद्ध और इंटरनेट युद्धक्षेत्र का वैश्विक खतरा:** डेटा दुनिया के लिये नया 'तेल' बन गया है, जिसका उपयोग किसी भी समय साइबर युद्ध

भड़काने के लिये किया जा सकता है। दुनिया के सभी प्रमुख शक्ति केंद्र अपने साइबर स्पेस को युद्ध के लिये तैयार डोमेन में बदल रहे हैं।
    - इंटरनेट संभावित रूप से खुफिया जानकारी एकत्र करने वाले एक मंच के रूप में दुरुपयोग किये जाने का उच्च जोखिम रखता है।
- **अंतर-निर्भर साइबरस्पेस:** आपूर्ति शृंखलाएँ तेज़ी से परस्पर संबद्ध होती जा रही हैं। व्यक्तिगत डेटा-आधारित प्लेटफॉर्म केंद्रीय मंच ग्रहण करते जा रहे हैं। इससे कंपनी की सुरक्षा दीवार कमज़ोर हो रही है और डेटा उल्लंघन अधिक आम होते जा रहे हैं।
- **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।
- **इंटरनेट ऑफ थिंग्स (IoT) के लिये कानूनी समर्थन का अभाव:** चूँकि इंटरनेट ऑफ थिंग्स अब आधुनिक उद्यमों, संगठनों और यहाँ तक कि जीने के बुनियादी तरीकों की रीढ़ बन गया है, यह चिंताजनक है कि भारत में IoT के लिये कोई समर्पित कानून नहीं है।
- **फेक न्यूज़ पर बढ़ती चिंता:** समाचार-आधारित ऐप्स एवं सेवाओं या सोशल मीडिया प्लेटफॉर्म (जिन्हें इंटरनेट मध्यस्थों के रूप में भी जाना जाता है) द्वारा अग्रेषित संदेशों के माध्यम से ऑनलाइन निःशुल्क जानकारी तक पहुँच में वृद्धि के साथ फेक न्यूज़ या भ्रामक सूचनाओं का भी उभार हुआ है जो प्रायः वास्तविक दुनिया के लिये गंभीर खतरा उत्पन्न करते हैं।
    - जागरूकता की कमी और डिजिटल अशिक्षा उन्हें और भी भेद्य बनाती है।

साइबर सुरक्षा के लिये सरकार की प्रमुख पहलें

- राष्ट्रीय साइबर सुरक्षा नीति, 2013
- राष्ट्रीय साइबर सुरक्षा समन्वय केंद्र (NCCC)
- साइबर स्वच्छता केंद्र
- इंडियन कंप्यूटर इमरजेंसी रिस्पांस टीम (CERT-In)

आगे की राह

- **क्वांटम-प्रतिरोधी प्रणाली (Quantum-Resistant system):** पारंपरिक इंटरनेट मॉडल पर जोखिम और क्वांटम प्रौद्योगिकी के सैन्य अनुप्रयोगों की बढ़ती क्षमता को देखते हुए भारत में 'क्वांटम-प्रतिरोधी' प्रणालियों की तैनाती समय की आवश्यकता है।
    - केंद्रीय बजट 2020-21 में हाल में घोषित 'क्वांटम टेक्नोलॉजीज और एप्लीकेशन पर राष्ट्रीय मिशन' पर 8,000 करोड़ रुपये खर्च करने का प्रस्ताव किया गया था, जो इस दिशा में एक स्वागतयोग्य कदम है।
- **'टेक्नो-डिप्लोमेसी' की ओर: भारत** को अन्य 'टेक्नो-डेमोक्रेसी' देशों और उन्नत अर्थव्यवस्थाओं के साथ अपनी राजनयिक साझेदारी को मज़बूत करने की आवश्यकता है ताकि उभरते हुए सीमापारीय साइबर खतरों से निपटने और सुरक्षित वैश्विक साइबरस्पेस की ओर बढ़ने के लिये विचारों एवं संसाधनों को एकत्र किया जा सके।
- **सहकारी संघवाद को साइबर सुरक्षा से जोड़ना:** चूँकि पुलिस और लोक व्यवस्था राज्य सूची में शामिल है, राज्यों को यह सुनिश्चित करना चाहिये कि साइबर अपराध से निपटने के लिये पुलिस अच्छी तरह से सुसज्जित है।
    - इसके अलावा, चूँकि आईटी अधिनियम और अन्य प्रमुख कानून केंद्र द्वारा अधिनियमित हैं, इसलिये केंद्र सरकार कानून प्रवर्तन एजेंसियों के लिये सार्वभौमिक वैधानिक प्रक्रिया विकसित करने का प्रयास कर सकती है।
    - इसके साथ ही, केंद्र और राज्यों को अत्यावश्यक साइबर अवसंरचना के विकास के लिये पर्याप्त प्रदान करना चाहिये।
- **साइबर फोरेंसिक प्रयोगशालाओं को उन्नत बनाना:** नई प्रौद्योगिकियों के साथ तालमेल रखने के लिये साइबर फोरेंसिक प्रयोगशालाओं को अपग्रेड करने की आवश्यकता है।
    - राष्ट्रीय साइबर फोरेंसिक प्रयोगशाला (National Cyber Forensic Laboratory) और दिल्ली पुलिस की 'साइबर रोकथाम, जागरूकता और जाँच केंद्र' (Cyber Prevention, Awareness and Detection Centre- CYPAD) पहल इस दिशा में सकारात्मक कदम हैं।
- **साइबर सुरक्षा के साथ नैतिक मूल्यों का सम्मिश्रण:** प्रौद्योगिकी एक ऐसे चरण में पहुँच गई है जहाँ हमें व्यक्तिगत और वैश्विक भलाई के लिये साइबर संसाधनों के अधिक विवेकपूर्ण उपयोग के लिये नैतिकता एवं आचार की वैश्विक समझ एवं समानता की आवश्यकता है।
- **अवसंरचनात्मक कमियों को दूर करना:** भौतिक अवसंरचनात्मक कमियों को दूर कर भारत के साइबर स्पेस का विस्तार करने और साइबर सुरक्षा उपायों से लैस साइबर समावेशन की ओर आगे बढ़ने की आवश्यकता है।
- **साइबर-जागरूकता अभियान:** ई-गवर्नेंस की दुनिया में, जहाँ सरकार ई-सरकार में रूपांतरित हो रही है और नागरिक ई-नागरिक बन रहे हैं, नागरिकों के बीच साइबर-जागरूकता (जिसमें सुरक्षित ऑनलाइन लेनदेन और अनधिकृत वेबसाइटों के साथ सूचना साझा न करना शामिल है) को बढ़ावा देने के लिये कदम उठाने की ज़रूरत है।

अभ्यास प्रश्न: प्रौद्योगिकी में अभूतपूर्व वृद्धि ने दुनिया भर में साइबर स्पेस की सीमाओं को धुंधला कर दिया है। भारत के साइबर स्पेस से संबंधित प्रमुख चुनौतियों पर प्रकाश डालिये।

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 आमतौर पर निम्नलिखित में से कौन से लाभ 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 कीमत अगर कुछ हानिकारक तत्त्व जानबूझकर इसे नुकसान पहुँचाते हैं, अगर ऐसा साबित होता है।
3. साइबर 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 चुनिए:

(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. बॉडी कॉरपोरेट

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 तत्त्व क्या हैं? साइबर सुरक्षा में चुनौतियों को ध्यान में रखते हुए, जाँच करें कि भारत ने एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति को किस हद तक सफलतापूर्वक विकसित किया है। (वर्ष 2022)