

भारत में सुरक्षित साइबरस्पेस

यह एडिटरियल 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 विकासवस्था 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 डिजिटल 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 नयितरण रखना अनिवार्य होगा।

साइबर खतरों से संबंधित प्रमुख शब्दावली

- क्लिकजैकिंग (Clickjacking):** यह इंटरनेट उपयोगकर्ताओं को दुर्भावनापूर्ण सॉफ्टवेयर वाले लिंक पर क्लिक करने या अनजाने में सोशल मीडिया साइटों पर नज़ी जानकारी साझा करने के लिये लुभाने का कृत्य है।
- डनियल 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 मडिल 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 फरि इसे पुनर्स्थापित करने के लिये पैसे की मांग (आमतौर पर बटिकॉइन के रूप में) संबंधी संदेश पोस्ट किया जाता है।
- स्पाइवेयर (Spyware):** ऐसा मैलवेयर जो उपयोगकर्ता की कंप्यूटर गतिविधियों पर गुप्त रूप से नज़र रखता है।
- 'ज़ीरो डे वलनेरेबिलिटी' (Zero Day Vulnerability):** ज़ीरो डे वलनेरेबिलिटी 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 वनियमित करने वाले कोई सामान्य नियम और मानदंड मौजूद नहीं हैं, इसलिये यह वजिज़ापन-आधारित प्रौद्योगिकी के माध्यम से कुछ वेबसाइटों के अन्य के ऊपर अवैध ध्रुवीकरण को संभव बनाता है, दर्शकों को बराबर करने के लिये विविध 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।
 - डर्ग्स, 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 कथिा जा सकता है। दुनिया के सभी प्रमुख शक्ति केंद्र अपने साइबर स्पेस को युद्ध के लिये तैयार डोमेन में बदल रहे हैं।

◦ इंटरनेट संभावति रूप से खुफिया जानकारी एकत्र करने वाले एक मंच के रूप में दुरुपयोग कथिे जाने का उच्च जोखिम रखता है।

- **अंतर-नरिभर साइबरस्पेस:** आपूर्ति शृंखलाएँ तेज़ी से परस्पर संबद्ध होती जा रही हैं। व्यक्तिगत डेटा-आधारति 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 प्रगतति भारत की डिजिटल अवसंरचना पर क्वांटम साइबर हमले की संभावना का वसितार करती है, जो पहले से ही चीनी राज्य-प्रायोजति हैकरों के हमलों का सामना कर रही है।
 - वदिशी हार्डवेयर, वशिष रूप से चीनी हार्डवेयर पर भारत की नरिभरता एक अतरिक्रि भेद्यता का नरिमाण करती है।
- **इंटरनेट ऑफ थगिस (IoT) के लथिे कानूनी समर्थन का अभाव:** चूँकि इंटरनेट ऑफ थगिस अब आधुनकि उद्यमों, संगठनों और यहाँ तक कि जीने के बुनयादी तरीकों की रीढ़ बन गया है, यह चतिाजनक है कि भारत में IoT के लथिे कोई समरपति कानून नहीं है।
- **फेक न्यूज़ पर बढ़ती चतिा:** समाचार-आधारति ऐप्स एवं सेवाओं या सोशल मीडिया प्लेटफॉर्म (जनिहें इंटरनेट मध्यस्थों के रूप में भी जाना जाता है) द्वारा अग्रेषति संदेशों के माध्यम से ऑनलाइन नःशुल्क जानकारी तक पहुँच के साथ फेक न्यूज़ या भ्रामक सूचनाओं का भी उभार हुआ है जो प्रायः वास्तवकि दुनिया के लथिे गंभीर खतरा उत्पन्न करते हैं।
 - जागरूकता की कमी और डिजिटल अशकिषा उनहें और भी भेद्य बनाती है।

साइबर सुरक्षा के लथिे सरकार की प्रमुख पहलें

- [राष्ट्रीय साइबर सुरक्षा नीति, 2013](#)
- [राष्ट्रीय साइबर सुरक्षा समन्वय केंद्र \(NCCC\)](#)
- [साइबर स्वच्छता केंद्र](#)
- [इंडियन कंप्यूटर इमरजेंसी रसिपांस टीम \(CERT-In\)](#)

आगे की राह

- **क्वांटम-प्रतरिधी प्रणाली (Quantum-Resistant system):** पारंपरकि इंटरनेट मॉडल पर जोखिम और क्वांटम प्रौद्योगिकि के सैन्य अनुप्रयोगों की बढ़ती क्षमता को देखते हुए भारत में 'क्वांटम-प्रतरिधी' प्रणालियों की तैनाती समय की आवश्यकता है।
 - केंद्रीय बजट 2020-21 में हाल में घोषति 'क्वांटम टेक्नोलॉजीज और एप्लीकेशन पर राष्ट्रीय मशिन' पर 8,000 करोड़ रुपये खर्च करने का प्रस्ताव कथिा गया था, जो इस दशिा में एक स्वागतयोग्य कदम है।
- **'टेक्नो-डपिलोमेसी' की ओर: भारत** को अन्य 'टेक्नो-डेमोक्रेसी' देशों और उन्नत अर्थव्यवस्थाओं के साथ अपनी राजनयकि साझेदारी को मज़बूत करने की आवश्यकता है ताकि उभरते हुए सीमापारीय साइबर खतरों से नपिटने और सुरक्षति वैश्वकि साइबरस्पेस की ओर बढ़ने के लथिे वचिरों एवं संसाधनों को एकत्र कथिा जा सके।
- **सहकारी संघवाद को साइबर सुरक्षा से जोडना:** चूँकि पुलिस और लोक व्यवस्था राज्य सूची में शामिल है, राज्यों को यह सुनिश्चति करना चाहथि कि साइबर अपराध से नपिटने के लथिे पुलिस अचछी तरह से सुसज्जति है।
 - इसके अलावा, चूँकि आईटी अधिनियम और अन्य प्रमुख कानून केंद्र द्वारा अधिनियमति हैं, इसलथि केंद्र सरकार कानून प्रवर्तन एजेंसथियों के लथिे सार्वभौमकि वैधानकि प्रक्रथिा वकिसति करने का प्रयास कर सकती है।
 - इसके साथ ही, केंद्र और राज्यों को अत्यावश्यक साइबर अवसंरचना के वकिस के लथिे पर्याप्त प्रदान करना चाहथि।
- **साइबर फोरेंसकि प्रयोगशालाओं को उन्नत बनाना:** नई प्रौद्योगिकियों के साथ तालमेल रखने के लथिे साइबर फोरेंसकि प्रयोगशालाओं को अपग्रेड करने की आवश्यकता है।
 - राष्ट्रीय साइबर फोरेंसकि प्रयोगशाला (National Cyber Forensic Laboratory) और दलिली पुलिस की 'साइबर रोकथाम, जागरूकता और जाँच केंद्र' (Cyber Prevention, Awareness and Detection Centre- CYPAD) पहल इस दशिा में सकारात्मक कदम हैं।
- **साइबर सुरक्षा के साथ नैतिक मूल्यों का सममशिरण:** प्रौद्योगिकि एक ऐसे चरण में पहुँच गई है जहाँ हमें व्यक्तिगत और वैश्वकि भलाई के लथिे साइबर संसाधनों के अधिक वकिकपूर्ण उपयोग के लथिे नैतिकता एवं आचार की वैश्वकि समझ एवं समानता की आवश्यकता है।
- **अवसंरचनात्मक कमथियों को दूर करना:** भौतिक अवसंरचनात्मक कमथियों को दूर कर भारत के साइबर स्पेस का वसितार करने और साइबर सुरक्षा उपायों से लैस साइबर समावेशन की ओर आगे बढ़ने की आवश्यकता है।
- **साइबर-जागरूकता अभयान:** ई-गवर्नेंस की दुनिया में, जहाँ सरकार ई-सरकार में रूपांतरति हो रही है और नागरकि ई-नागरकि बन रहे हैं, नागरकिों के बीच साइबर-जागरूकता (जसिमें सुरक्षति ऑनलाइन लेनदेन और अनधिकृत वेबसाइटों के साथ सूचना साझा न करना शामिल है) को बढ़ावा देने के लथिे कदम उठाने की ज़रूरत है।

अभ्यास प्रश्न: प्रौद्योगिकि में अभूतपूर्व वृद्धतिने दुनिया भर में साइबर स्पेस की सीमाओं को धुंधला कर दथिा है। भारत के साइबर स्पेस से संबंधति प्रमुख चुनौतियों पर प्रकाश डालथिे।

यूपीएससी सविलि सेवा परीक्षा, वगित वर्ष के प्रश्न (PYQ)

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

Q.1 भारत में व्यक्तिथियों के लथिे साइबर बीमा के तहत धन की हानि और अन्य लाभों के भुगतान के अलावा आमतौर पर नमिनलखिति में से कौन से लाभ कवर कथिे जाते हैं? (वर्ष 2020)

1. कसीं के कंप्यूटर तक पहुँच को बाधति करने वाले मैलवेयर के मामले में कंप्यूटर सस्टिम की बहाली की लागत ।
2. एक नए कंप्यूटर की कीमत अगर कुछ हानिकारक तत्त्व जानबूझकर इसे नुकसान पहुँचाते हैं, अगर ऐसा साबति होता है ।
3. साइबर वसूली के मामले में नुकसान को कम करने के लिए एक वशिष सलाहकार को काम पर रखने की लागत ।
4. यदकि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव की लागत ।

नीचे दयि गए कूट का प्रयोग कर सही उत्तर चुनयि:

- (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 नमिनलखिति में से कसिके लयि साइबर सुरक्षा घटनाओं पर रपिर्ट करना कानूनी रूप से अनविर्य है? (वर्ष 2017)

1. सेवा प्रदाता
2. डेटा केंद्र
3. बॉडी कॉरपोरेट

नीचे दयि गए कूट का प्रयोग कर सही उत्तर चुनयि:

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

उत्तर: (D)

Q.3 साइबर सुरक्षा के वभिनिन तत्त्व क्या हैं? साइबर सुरक्षा में चुनौतयिों को ध्यान में रखते हुए, जाँच करें कभिारत ने एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीतको कसि हद तक सफलतापूर्वक वकिसति कयि है। (वर्ष 2022)