संसद टीवी विशेष: सुरक्षित साइबर स्पेस

प्रलिम्सि के लिये:

भारतीय साइबर अपराध समन्वय केंद्र (I4C), साइबर अपराध, सॉफ्टवेयर, इंटरनेट, दूरसंचार नेटवर्क, वायरस, रैनसमवेयर, स्पाइवेयर, ट्रोजन, राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (NCRB) रिपोर्ट, फिशिंग, आईपी एड्रेस, आतंकवादी संगठन, महत्त्वपूर्ण बुनियादी ढाँचा, **वित्तीय अपराध, सहकारी संघवाद**, CERT-In, साइबर सुरक्षित भारत, डिजिटल इंडिया, मैलवेयर।

मेन्स के लिये:

साइबर अपराध के निहितार्थ और भारत में सुरक्षित साइबरस्पेस का महत्त्व।

चर्चा में क्यों?

हाल ही में भारतीय साइबर अपराध समन्वय केंद्र **(Indian Cyber Crime Coordination Centre- I4C)** के प्रथम स्थापना दिवस के अवसर पर **नई दिल्ली** में एक कार्यक्रम आयोजित किया गया , जिसमें कई प्रमुख पहलों की शुरुआत के साथ साइबर अपराध की रोकथाम में महत्त्वपूर्ण प्रगति को प्रदर्शित किया गया।

साइबर सुरक्षा क्या है?

- **साइबर सुरक्षा: यह हार्डवेयर,** सॉफ्टवेयर और डेटा सहित **सूचना प्रणालियों को साइबर खतरों से सुरक्षा** प्रदान करता है। इसका उद्देश्य **अनधिकृत पहुँच**, चोरी, क्षति तथा अन्य दुर्भावनापूर्ण गतिविधियों से बचाव करना है जो डिजिटल जानकारी की अखंडता, गोपनीयता एवं उपलब्धता से समझौता कर सकती हैं।
- **साइबर स्पेस :** इंटरनेट, दूरसंचार नेटवर्क और कंप्यूटर प्रणालियों सहित **परस्पर जुड़ी सूचना प्रौद्योगिकी अवसंरचनाओं** का वैश्विक नेटवर्क, जहाँ डेटा और संचार होते हैं।
- क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर **(CII):** सूचना प्रौद्योगिकी अधिनियम **की धारा 70(1)** द्वारा परिभाषित, **क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर (Critical Information Infrastructure- CII)** में कंप्यूटर संसाधन शामिल हैं जिनकी अक्षमता या खंडन राष्ट्रीय सुरक्षा**, आर्थिक स्थिरता, सार्वजनिक स्वास्थ्य या सुरक्षा को गंभीर रूप से प्रभावित कर सकता है।**
- साइबर अटैक: व्यक्तियों या संगठनों द्वारा सूचना प्रणालियों में सेंध लगाने का **जानबूझकर और दुर्भावनापूर्ण प्रयास**, जिसका उद्देश्य वित्तीय लाभ से लेकर राजनीतिक सक्रियता या जासूसी तक हो सकता है।

साइबर हमलों के प्रकार:

- **मैलवेयर**: दुर्भावनापूर्ण सॉफ्टवेयर, जिसमें वायरस, वर्म्स, रैनसमवेयर, स्पाइवेयर और ट्रोजन शामिल हैं , जो सिस्टम को नुकसान पहुँचाने या बाधित करने, जानकारी चुराने या अनधिकृत पहुँच प्राप्त करने के लिये डिज़ाइन किये गए हैं।
- **फिशिंग: भ्रामक ईमेल या वेबसाइट** जो व्यक्तियों को धोखा देकर उनसे व्यक्तिगत जानकारी, जैसे लॉगिन क्रेडेंशियल या वित्तीय विवरण, प्रकट करवाती हैं।
- **सेवा अस्वीकार (DoS) हमले : इन हमलों का उद्देश्य किसी मशीन या नेटवर्क पर अत्यधिक ट्रैफिक** डालकर उसे बंद करना होता है, जिससे वह वैध उपयोगकर्त्ताओं के लिये दुर्गम हो जाता है।
- **मैन इन मिडिल (MitM) अटैक**: दो पक्षों के बीच उनकी जानकारी के बिना संचार को बाधित करना और बदलना, जिससे डेटा चोरी या हेर-फेर संभव हो सके।
- **SQL इंजेक्शन**: डेटा तक पहुँचने या उसमें हेर-फेर करने के लिये क्वेरीज़ (Queries) में गलत कोड डालकर डेटाबेस की कमजोरियों का फायदा उठाना।
- **क्रॉस-साइट स्क्रिप्टिंग (XSS)**: उपयोगकर्त्ताओं के ब्राउज़रों में चलाने के लिये वेबसाइटों में **दुर्भावनापूर्ण स्क्रिप्ट डालना**, संभावित रूप से व्यक्तिगत जानकारी चुराना या अनधिकृत कार्य करना।
- **सामाजिक इंजीनियरिंग**: मनोवैज्ञानिक चालों के माध्यम से व्यक्तियों को सुरक्षा प्रोटोकॉल का उल्लंघन करने या गोपनीय जानकारी का खुलासा

करने के लिये प्रेरित करना।

साइबर अपराध से निपटने हेतु सरकार की क्या पहल हैं?

- **हालिया पहल:**
    - **साइबर धोखाधड़ी शमन केंद्र (CFMC)**: यह केंद्र **प्रमुख बैंकों, वित्तीय मध्यस्थों, दूरसंचार सेवा प्रदाताओं, IT मध्यस्थों और कानून प्रवर्तन एजेंसियों के प्रतिनिधियों को एक साथ लाता है।**
        - यह ऑनलाइन **वित्तीय अपराधों से** निपटने के लिये एक सहकारी मंच के रूप में कार्य करता है और कानून प्रवर्तन में**सहकारी संघवाद का उदाहरण प्रस्तुत करता है।**
    - **समन्वय प्लेटफॉर्म**: एक **वेब-आधारित मॉड्यूल** जिसे साइबर अपराध डेटा के लिये एक केंद्रीय भंडार के रूप में डिज़ाइन किया गया है, जो पूरे भारत में कानून प्रवर्तन एजेंसियों के बीच डेटा साझाकरण, अपराध मानचित्रण और समन्वय की सुविधा प्रदान करता है।
    - **साइबर कमांडो कार्यक्रम**: अगले पाँच वर्षों में लगभग **5,000 साइबर कमांडो को प्रशिक्षित करने के उद्देश्य से** यह कार्यक्रम डिजिटल स्पेस को सुरक्षित करने में राज्य और केंद्रीय एजेंसियों की सहायता के लिये साइबर सुरक्षा पेशेवरों का एक विशेष कैडर विकसित करने पर केंद्रित है।
    - **संदिग्ध रजिस्ट्री**: यह राष्ट्रीय स्तर की रजिस्ट्री साइबर अपराध संदिग्धों के बारे में जानकारी एकत्रित करती है तथा**वित्तीय पारिस्थितिकी तंत्र के भीतर धोखाधड़ी जोखिम प्रबंधन को बढ़ाती है।**
- **पिछली पहल:**
    - **सूचना प्रौद्योगिकी अधिनियम, 2000**: यह अधिनियम इलेक्ट्रॉनिक प्रारूपों में कंप्यूटर, नेटवर्क और डेटा के उपयोग को नियंत्रित करता है, जिसमें **हैकिंग, साइबर आतंकवाद तथा डेटा चोरी जैसे अपराधों के लिये प्रावधान शामिल हैं।**
    - **भारतीय साइबर अपराध समन्वय केंद्र (I4C): गृह मंत्रालय** द्वारा स्थापित, **I4C का** उद्देश्य समन्वित प्रयासों के माध्यम से भारत में साइबर अपराध को संबोधित करना है।
        - 5 अक्तूबर, 2018 को स्वीकृत I4C कानून प्रवर्तन और हितधारकों के बीच**समन्वय को बढ़ाता है, राष्ट्रीय क्षमताओं को बढ़ाता है और साइबर अपराध से निपटने में नागरिक संतुष्टि में सुधार करता है।**
    - **भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In):** CERT-In साइबर सुरक्षा घटनाओं के प्रबंधन और प्रतिक्रिया प्रयासों के समन्वय में महत्त्वपूर्ण भूमिका निभाता है। यह भारत के डिजिटल परिदृश्य में घटना प्रबंधन, भेद्यता मूल्यांकन तथा सुरक्षा निरीक्षण के लिये केंद्रीय प्राधिकरण के रूप में कार्य करता है।
    - **साइबर सुरक्षित भारत: इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY) द्वारा राष्ट्रीय इलेक्ट्रॉनिक गवर्नेंस प्रभाग (National Electronic Governance Division- NeGD)** के सहयोग से शुरू किया गया, **साइबर सुरक्षित भारत का** उद्देश्य वर्तमान साइबर खतरों तथा चुनौतियों के बारे में जागरूकता बढ़ाकर **"डिजिटल इंडिया" दृष्टिकोण का समर्थन करना है।**
    - **साइबर स्वच्छता केंद्र:** यह पहल कंप्यूटर और डिवाइस से दुर्भावनापूर्ण बॉटनेट प्रोग्राम की पहचान करने और उन्हें खत्म करने पर केंद्रित है। यह **मैलवेयर** विश्लेषण के लिये निःशुल्क उपकरण प्रदान करता है तथा सिस्टम एवं डिवाइस सुरक्षा को बढ़ाता है।
    - **राष्ट्रीय साइबर सुरक्षा रणनीति, 2020: इसका उद्देश्य** अधिक कठोर ऑडिट लागू करके साइबर जागरूकता बढ़ाना **और साइबर सुरक्षा को मज़बूत करना है।**
        - **साइबर ऑडिटर** वर्तमान कानूनी आवश्यकताओं से परे संगठनात्मक सुरक्षा उपायों का अधिक गहन मूल्यांकन करेंगे।
- **अंतर्राष्ट्रीय पहल:**
    - **साइबर अपराध पर बुडापेस्ट कन्वेंशन:** साइबर अपराध पर कानूनों को सुसंगत बनाने और सहयोग बढ़ाने के लिये एक अंतर्राष्ट्रीय संधि है। यह 1 जुलाई, 2004 से प्रभावी है। भारत इसका हस्ताक्षरकर्त्ता नहीं है।
    - **इंटरनेट गवर्नेंस फोरम (IGF):** इंटरनेट गवर्नेंस पर सरकारों, निजी क्षेत्र और नागरिक समाज के बीच संवाद के लिये एक मंच।
    - **UNGA संकल्प:** ICT सुरक्षा के लिये दो प्रक्रियाएँ स्थापित की गईं, अर्थात्**ओपन-एंडेड वर्किंग ग्रुप (Open-ended Working Group- OEWG) और सरकारी विशेषज्ञों का समूह (GGE)।**

भारत में साइबर सुरक्षा से जुड़ी चुनौतियाँ क्या हैं?

- **साइबर अपराध दर में वृद्धि: राष्ट्रीय अपराध रिकॉर्ड ब्यूरो (National Crime Records Bureau- NCRB) की रिपोर्ट से** पता चलता है कि वर्ष 2022 में **साइबर अपराध के मामलों में 24.4% की वृद्धि** होगी। वर्ष 2022 में साइबर अपराध श्रेणी के तहत अपराध दर (प्रति लाख जनसंख्या) 2021 में 3.9 से बढ़कर 4.8 हो गई है।
    - वर्ष 2022 में साइबर अपराध के 64.8% मामले धोखाधड़ी से संबंधित थे, 5.5% जबरन वसूली से संबंधित थे और 5.2% यौन शोषण से संबंधित थे।
    - **भारतीय साइबर अपराध समन्वय केंद्र (I4C)** के अनुसार, मई 2024 में प्रतिदिन औसतन **7,000 साइबर अपराध शिकायतें** दर्ज की गईं।
- **मोबाइल प्रौद्योगिकी और इंटरनेट का बढ़ता उपयोग**: भारत में **1 बिलियन से अधिक** स्मार्टफोन उपयोगकर्त्ता हैं और कई मोबाइल ऐप्स में मज़बूत सुरक्षा सुविधाओं का अभाव है, जिससे डेटा उल्लंघन का खतरा बढ़ जाता है।
- **इंटरनेट ऑफ थिंग्स (IoT) का प्रसार : स्मार्ट होम गैजेट्स और पहनने योग्य उपकरणों जैसे IoT** उपकरणों का व्यापक उपयोग अक्सर कमज़ोर सुरक्षा सुविधाओं के कारण हमलों के लिये उन्हें उजागर करता है, जिससे वे साइबर घुसपैठ हेतु आसान लक्ष्य बन जाते हैं।
- **जटिल सॉफ्टवेयर प्रणालियाँ: आधुनिक सॉफ्टवेयर प्रणालियों** की बढ़ती जटिलता, जिसमें उनके अनेक घटक और अंतर्क्रियाएँ शामिल हैं, कमजोरियाँ पैदा कर सकती हैं जिनका हमलावर फायदा उठा सकते हैं।
    - इस जटिलता के कारण अक्सर सुरक्षा संबंधी खामियाँ पैदा हो जाती हैं, जिन्हें पहचानना और उनका समाधान करना कठिन होता है, जिससे ये प्रणालियाँ साइबर हमलों के प्रति अधिक संवेदनशील हो जाती हैं।

- **मानवीय त्रुटि:** सुरक्षा प्रथाओं में गलतियाँ जैसे **सेटिंग्स को गलत तरीके से कॉन्फिगर करना** या [फिशिंग](#) योजनाओं के झाँसे में आना, हमलावरों के लिये संभावित प्रवेश बिंदु बनाते हैं।
    - उदाहरण के लिये, कोई कर्मचारी गलती से एक्सेस नियंत्रण को गलत तरीके से कॉन्फ़िगर करके या किसी **दुर्भावनापूर्ण लिंक पर क्लिक करके संवेदनशील डेटा को उजागर कर सकता है**, जिससे डेटा चोरी हो सकती है।
    - ये त्रुटियाँ प्रायः जागरूकता या प्रशिक्षण की कमी के कारण होती हैं, जिससे जोखिमों को कम करने और समग्र सुरक्षा को मज़बूत करने के लिये निरंतर शिक्षा तथा कड़े प्रोटोकॉल की आवश्यकता पर बल मिलता है।
- **प्रॉक्सी सर्वर और VPN का उपयोग** : हमलावर अक्सर अपने [आईपी एड्रेस](#) को छिपा देते हैं , जिससे उनके मूल का पता लगाने के प्रयास जटिल हो जाते हैं।
- **तकनीकी विलंब**: आक्रमण तकनीकें तेजी से विकसित होती हैं, जो प्रायः प्रत्युत्तर उपायों के विकास से भी आगे निकल जाती हैं।
    - उदाहरण के लिये जबकि उन्नत एन्क्रिप्शन विधियों के साथ नए प्रकार के **रैनसमवेयर** सामने आ सकते हैं, मौजूदा एंटीवायरस सॉफ्टवेयर अभी तक इन खतरों का पता लगाने या उन्हें बेअसर करने में सक्षम नहीं हो सकते हैं।
- **अपर्याप्त प्रशिक्षण**: कई व्यक्तियों और कर्मचारियों को साइबर सुरक्षा प्रथाओं में **पर्याप्त प्रशिक्षण का अभाव है।**
    - **नैसकॉम के** एक हालिया अध्ययन में पूर्वानुमान लगाया है कि वर्ष 2027 तक **1 मिलियन** नई **साइबर सुरक्षा नौकरियाँ** उत्पन्न होंगी, जिनमें **कुशल प्रतिभा की कमी** के कारण से **30% मौजूदा पद** खाली रह जाएंगे ।
- **खतरों को कम आँकना**: कुछ संगठन और व्यक्ति साइबर खतरों की गंभीरता को पूरी तरह से नहीं समझ पाते, जिसके परिणामस्वरूप अपर्याप्त सुरक्षा मिलती है।
    - जागरूकता की कमी के कारण **अपर्याप्त सुरक्षा और तैयारी हो सकती** है, जिससे सिस्टम हमलों के प्रति असुरक्षित हो सकता है, जिसे साइबर सुरक्षा के प्रति अधिक व्यापक दृष्टिकोण से कम किया जा सकता था।
- **साइबर सुरक्षा विशेषज्ञों की कमी: कुशल साइबर सुरक्षा पेशेवरों** की मांग आपूर्ति से अधिक है, जिसके कारण नियुक्ति प्रतिस्पर्द्धी है और कर्मचारियों का टर्नओवर अधिक है।
    - अपर्याप्त प्रशिक्षण कार्यक्रमों के कारण योग्य विशेषज्ञों की कमी हो जाती है।
- **आतंकवादियों द्वारा साइबरस्पेस का बढ़ता उपयोग: आतंकवादी संगठन भर्ती और प्रचार** के लिये इंटरनेट का उपयोग करते हैं। साथ ही आतंकवादियों द्वारा साइबर हमलों का उपयोग करके [महत्तत्वपूर्ण बुनियादी ढाँचे](#) को निशाना बनाने का जोखिम भी है।
    - उदाहरण के लिये **इस्लामिक स्टेट (ISIS) ने फाइटरों की भर्ती करने और वैश्विक स्तर पर चरमपंथी सामग्री का प्रसार करने के लिये सोशल मीडिया का इस्तेमाल किया है। इसके अलावा** साइबर हमलों के माध्यम **महत्तत्वपूर्ण बुनियादी ढाँचे को निशाना बनाने वाले** आतंकवादियों का जोखिम बढ़ रहा है ।

आगे की राह

- **जन जागरूकता अभियान**: विविध मीडिया के माध्यम से लोगों तक पहुँच बढ़ाना और साइबर सुरक्षा शिक्षा को स्कूली पाठ्यक्रम में शामिल करना। **I4C के स्थापना दिवस समारोह में हाल ही में घोषित नई पहलों में साइबर अपराध तथा साइबर अपराध हेल्पलाइन 1930** के बारे में लोगों को शिक्षित करने के लिये टीवी, रेडियो और अन्य मीडिया का उपयोग किया जाएगा। राज्य सरकारों से जागरूकता फैलाने में भाग लेने का आग्रह किया जाता है।
- **तकनीकी उपायों को मज़बूत करना**: उन्नत प्रौद्योगिकियों में निवेश करना तथा सरकार, निजी क्षेत्र और अंतर्राष्ट्रीय साझेदारों के बीच **सहयोग बढ़ाना।**
- **साइबर सुरक्षा प्रतिभा का विकास करना**: प्रशिक्षण कार्यक्रमों का विस्तार करना और साइबर सुरक्षा में कॅरियर विकास के अवसर पैदा करना। यह अनुमान है कि वर्ष 2026 तक वैश्विक साइबर सुरक्षा बाज़ार का **352.25 बिलियन अमेरिकी डॉलर तक बढ़ना** भारत के लिये महत्त्वपूर्ण अवसर प्रस्तुत करता है, जिसमें इसके साइबर सुरक्षा उद्योग का विस्तार **तथा रोज़गार सृजन में वृद्धि शामिल है।**
- **निगरानी और मूल्यांकन**: साइबर सुरक्षा पहलों का नियमित मूल्यांकन करना तथा निरंतर सुधार के लिये फीडबैक तंत्र स्थापित करना।
- **व्यापक प्रशिक्षण कार्यक्रम**: **साइबर खतरों** और रोकथाम के सर्वोत्तम तरीकों के बारे में जागरूकता बढ़ाने के लिये व्यक्तियों और संगठनों हेतु प्रशिक्षण पहल का विस्तार करना।
- **उन्नत सुरक्षा प्रौद्योगिकियों में निवेश**: उभरते खतरों का मुकाबला करने के लिये अत्याधुनिक सुरक्षा समाधानों के विकास और तैनाती को प्राथमिकता देना। यह सुनिश्चित करना कि ज्ञात कमजोरियों को दूर करने तथा समग्र सुरक्षा में सुधार करने हेतु सॉफ्टवेयर एवं सिस्टम **नियमित रूप से अपडेट किये जाते हैं।**
- **अंतर-एजेंसी समन्वय**: साइबर अपराध से निपटने के लिये सूचना और रणनीतियों को साझा करने हेतु **सरकारी एजेंसियों, निजी क्षेत्र की संस्थाओं तथा अंतर्राष्ट्रीय भागीदारों के बीच सहयोग को बढ़ावा देना।**

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

प्रिलिम्स:

Q. 'वानाक्राई, पेट्या और इटर्नलब्लू' पद जो हाल ही में समाचारों में उल्लिखित थे निम्नलिखित में से किसके साथ संबंधित हैं: (2018)

(a) एक्सोप्लैनेट्स
(b) प्रच्छन्न मुद्रा (क्रिप्टोकरेंसी)
(c) साइबर आक्रमण
(d) लघु उपग्रह

उत्तर: (c)

प्रश्न. भारत में, किसी व्यक्ति के साइबर बीमा कराने पर, निधि की हानि के भरपाई एवं अन्य लाभों के अतिरिक्त, सामान्यतः निम्नलिखित में से कौन-कौन से लाभ दिये जाते हैं? (2020)

1. यदि कोई मैलवेयर कंप्यूटर तक उसकी पहुँच बाधित कर देता है, तो कंप्यूटर प्रणाली को पुनः प्रचलित करने में लगने वाली लागत
2. यदि यह प्रमाणित हो जाता है कि किसी शरारती तत्त्व द्वारा जान-बूझकर कंप्यूटर को नुकसान पहुँचाता गया है, तो नए कंप्यूटर की लागत
3. यदि साइबर बलात्-ग्रहण होता है तो इस हानि को न्यूनतम करने के लिये विशेषज्ञ परामर्शदाता की सेवाएँ लेने पर लगने वाली लागत
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव करने में लगने वाली लागत

नीचे दिये गए कूट का प्रयोग करके 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. भारत की आंतरिक सुरक्षा को ध्यान में रखते हुए सीमा-पार से होने वाले साइबर हमलों के प्रभाव का विश्लेषण कीजिये। साथ ही इन परिष्कृत हमलों के विरुद्ध रक्षात्मक उपायों की चर्चा कीजिये। (2021)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/sansad-tv-vishesh-safe-cyberspace