भारत की साइबर सुरक्षा चुनौतियाँ: खतरे और समाधान रणनीतियाँ

यह एडिटोरियल 26/12/2023 को 'इंडियन एक्सप्रेस' में प्रकाशित "We want a Digital India. Just not the one we are living in" लेख पर आधारित है। इसमें साइबर सुरक्षा के क्षेत्र में भारत के लिये व्याप्त चुनौतियों एवं अवसरों के बारे में चर्चा की गई है और तर्क दिया गया है कि भारत को एक नए दृष्टिकोण की आवश्यकता है जो आत्मनिर्भरता, नवाचार एवं सहकार्यता पर आधारित हो।

प्रिलिम्स के लिये:

SWIFT प्रणाली, राष्ट्रीय सूचना विज्ञान केंद्र (NIC), साइबर सुरक्षित भारत पहल, साइबर स्वच्छता केंद्र, भारतीय साइबर अपराध समन्वय केंद्र (I4C), राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC), डिफेंस साइबर एजेंसी (DCyA)।

मेन्स के लिये:

साइबर हमलों के प्रति भारत की संवेदनशीलता, साइबर हमलों से उत्पन्न चुनौतियाँ, सरकारी पहल और आगे की राह।

जैसे-जैसे दुनिया डिजिटलीकरण के क्षेत्र में आगे बढ़ रही है, साइबर हमलों का खतरा भी बढ़ता जा रहा है और भारत भी इससे अछूता नहीं है। अक्टूबर 2023 में अमेरिकी कंपनी 'रिसिक्योरिटी' (Resecurity) ने उजागर किया कि भारतीयों के निजी डेटा डार्क वेब (dark web) पर उपलब्ध हैं। ख़बरों की भीड़ में इसे नज़रअंदाज करना आसान होता, लेकिन डेटा के आकार और संवेदनशीलता ने तुरंत इस ओर ध्यान आकर्षित किया। इस डेटा सेट का विक्रेता 55% भारतीय आबादी (लगभग 81.5 करोड़ भारतीय नागरिक) की सत्यापन योग्य, संवेदनशील सूचना प्रदान करने का दावा कर रहा था।

इन सूचनाओं में लोगों के नाम, फोन नंबर, आधार नंबर, पासपोर्ट नंबर और पता जैसी व्यक्तिगत पहचान-योग्य जानकारी शामिल थी। मात्र 80,000 अमेरिकी डॉलर पर इस डेटा की बिक्री की जा रही थी। सक्रिय हुई दिल्ली पुलिस ने 18 दिसंबर को इस मामले में चार लोगों को गिरफ़्तार किया।

साइबर हमलों के प्रति भारत कितना संवेदनशील है?

- भारत में इंटरनेट उपयोगकर्ताओं की एक बड़ी और बढ़ती आबादी पाई जाती है, जहाँ **वर्ष 2022 में 52% से अधिक आबादी या 759 मिलियन लोग माह में कम से कम एक बार इंटरनेट का उपयोग** कर रहे थे।
  - चीन के बाद भारत **दुनिया का दूसरा सबसे बड़ा ऑनलाइन बाज़ार** है।
  - वर्ष 2025 तक यह संख्या **बढ़कर 900 मिलियन होने की उम्मीद** है।
- भारत में तेज़ी से बढ़ती डिजिटल अर्थव्यवस्था है, जहाँ स्वास्थ्य सेवा, शिक्षा, वित्त, खुदरा और कृषि जैसे क्षेत्र ऑनलाइन प्लेटफॉर्म एवं सेवाओं पर निर्भरता रखते हैं।
  - भारत की पुरानी पड़ चुकी या अपर्याप्त साइबर सुरक्षा अवसंरचना, नीतियाँ और जागरूकता हैकर्स के लिये सिस्टम में अंतराल एवं कमज़ोरियों का लाभ उठाना आसान बनाती है। यही कारण है कि भारत को राज्य-प्रायोजित और गैर-राज्य अभिकर्ताओं की ओर से परिष्कृत एवं नियमित रूप से साइबर खतरों का सामना करना पड़ता है, जो भारत के रणनीतिक, आर्थिक एवं राष्ट्रीय हित को निशाना बनाते हैं।

भारत पर साइबर हमलों से उत्पन्न चुनौतियाँ कौन-सी हैं?

- **महत्त्वपूर्ण अवसंरचना की भेद्यता/संवेदनशीलता:** भारत की महत्त्वपूर्ण अवसंरचना, जैसे कि पावर ग्रिड, परिवहन प्रणालियाँ एवं संचार नेटवर्क, साइबर हमलों के प्रति संवेदनशील हैं जो आवश्यक सेवाओं को बाधित कर सकते हैं और **सार्वजनिक संरक्षा एवं राष्ट्रीय सुरक्षा को खतरे** में डाल सकते हैं।
  - उदाहरण के लिये, अक्टूबर 2019 में कुडनकुलम परमाणु ऊर्जा संयंत्र पर साइबर हमले का प्रयास किया गया था।
- **वित्तीय क्षेत्र को खतरा:** भारत में वित्तीय क्षेत्र को उन साइबर अपराधियों की ओर से साइबर हमलों के उच्च जोखिम का सामना करना पड़ता है जो चोरी या जबरन वसूली से लाभ कमाना चाहते हैं। बैंकों, वित्तीय संस्थानों और ऑनलाइन भुगतान प्रणालियों पर साइबर हमलों से वित्तीय हानि, पहचान की चोरी और वित्तीय प्रणाली के प्रति भरोसे की कमी जैसी स्थिति उत्पन्न हो सकती है।
  - उदाहरण के लिये, मार्च 2020 में सिटी यूनियन बैंक के स्विफ्ट सिस्टम (SWIFT system) पर एक मैलवेयर हमले के कारण 2 मिलियन अमेरिकी डॉलर का अनधिकृत लेनदेन हुआ।

- **डेटा उल्लंघन और गोपनीयता संबंधी चिंताएँ:** जैसे-जैसे भारत डिजिटल अर्थव्यवस्था की ओर आगे बढ़ रहा है, ऑनलाइन संग्रहीत व्यक्तिगत एवं सरकारी डेटा की मात्रा भी बढ़ रही है। इससे डेटा उल्लंघनों का खतरा भी बढ़ गया है, जहाँ हैकर्स संवेदनशील जानकारी तक पहुँच बनाते हैं और उसे लीक करते हैं। डेटा उल्लंघनों से व्यक्तियों और संगठनों की गोपनीयता एवं सुरक्षा के लिये गंभीर परिणाम उत्पन्न हो सकते हैं।
    - उदाहरण के लिये, मई 2021 में कॉमन एडमिशन टेस्ट (CAT) 2020 (जिसका उपयोग IIMs में आवेदकों के चयन के लिये किया जाता है) के 190,000 उम्मीदवारों की व्यक्तिगत पहचान योग्य जानकारी (PII) एवं परीक्षा परिणाम को लीक कर दिया गया और साइबर क्राइम फोरम पर बिक्री के लिये उपलब्ध करा दिया गया।
- **साइबर जासूसी (Cyber Espionage):** साइबर जासूसी अन्य देशों या संस्थाओं की जासूसी करने या उनके हितों को नुक़सान पहुँचाने के लिये साइबर हमलों का उपयोग करने की प्रक्रिया है। अन्य देशों की तरह भारत भी साइबर जासूसी गतिविधियों के निशाने पर है, जो गोपनीय जानकारी चुराने और रणनीतिक बढ़त हासिल करने का उद्देश्य रखती है। साइबर जासूसी भारत की राष्ट्रीय सुरक्षा, विदेश नीति और आर्थिक विकास को प्रभावित कर सकती है।
    - उदाहरण के लिये, वर्ष 2020 में एक पाकिस्तानी थ्रेट एक्टर (threat actor) ऑपरेशन साइडकॉपी (Operation SideCopy) नामक साइबर जासूसी अभियान का पर्दाफाश हुआ जिसने मैलवेयर और फ़िशिंग ईमेल के साथ भारतीय सैन्य एवं राजनयिक कर्मियों को लक्षित किया था।
- **एडवांस्ड परसिस्टेंट थ्रेट्स (Advanced Persistent Threats- APTs):** APTs जटिल एवं दीर्घकालिक साइबर हमले हैं, जो आमतौर पर संसाधन-संपन्न और कुशल समूहों द्वारा किये अंजाम दिये जाते हैं। ये हमले लक्ष्य के नेटवर्क में घुसपैठ करने और लंबे समय तक छिपे रहने के लिये डिज़ाइन किये गए होते हैं, जिससे उन्हें डेटा चोरी करने या हेरफेर करने या क्षति पहुँचाने का अवसर मिलता है।
    - APTs का पता लगाना और उनका मुक़ाबला करना कठिन है, क्योंकि वे सुरक्षा उपायों से बचने के लिये उन्नत तकनीकों और उपकरणों का उपयोग करते हैं।
    - उदाहरण के लिये, फ़रवरी 2021 में RedEcho नामक साइबर सुरक्षा फर्म ने खुलासा किया कि चीन से जुड़े APT समूह ने भारत के बिजली क्षेत्र में 10 संस्थाओं को मैलवेयर से निशाना बनाया था, जो संभावित रूप से भारत में पावर आउटेज का कारण बन सकते थे।
- **आपूर्ति शृंखला की भेद्यताएँ:** आपूर्ति शृंखला संबंधी भेद्यताएँ उन सॉफ्टवेयर या हार्डवेयर घटकों में मौजूद कमज़ोरियों को संदर्भित करती हैं जिनका उपयोग सरकार और व्यवसायों द्वारा अपने संचालन के लिये किया जाता है। साइबर हमलावर इन घटकों पर निर्भर सिस्टम और सेवाओं को प्रभावित करने के लिये इन कमज़ोरियों का फायदा उठा सकते हैं और व्यापक क्षति पहुँचा सकते हैं।
    - उदाहरण के लिये, दिसंबर 2020 में नेटवर्क प्रबंधन उपकरण प्रदान करने वाली अमेरिका अवस्थित सॉफ्टवेयर कंपनी SolarWinds पर एक वैश्विक साइबर हमले ने कई भारतीय संगठनों को प्रभावित किया जिनमें **राष्ट्रीय सूचना विज्ञान केंद्र (NIC)**, इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (MeitY), भारत हेवी इलेक्ट्रिकल्स लिमिटेड (BHEL) आदि शामिल थे।

साइबर सुरक्षा को लेकर कौन-सी प्रमुख पहलें की गई हैं?

- **राष्ट्रीय साइबर सुरक्षा नीति (National Cyber Security Policy):** इस नीति का लक्ष्य नागरिकों, व्यवसायों और सरकार के लिये एक सुरक्षित एवं प्रत्यास्थी साइबरस्पेस का निर्माण करना है। यह साइबरस्पेस सूचना एवं अवसंरचना की रक्षा करने, साइबर हमलों को रोकने एवं जवाबी कार्रवाई के लिये क्षमताओं का निर्माण करने और संस्थागत संरचनाओं, व्यक्तियों, प्रक्रियाओं एवं प्रौद्योगिकी के समन्वित प्रयासों के माध्यम से क्षति को न्यूनतम करने के लिये विभिन्न उद्देश्यों एवं रणनीतियों की रूपरेखा तैयार करता है।
- **'साइबर सुरक्षित भारत' पहल:** यह पहल साइबर अपराधों के बारे में जागरूकता बढ़ाने और सभी सरकारी विभागों में मुख्य सूचना सुरक्षा अधिकारियों (CISOs) एवं अग्रिम पंक्ति के आईटी कर्मचारियों के लिये सुरक्षा उपाय का सृजन करने के लिये शुरू की गई थी।
- **भारतीय साइबर अपराध समन्वय केंद्र (Indian Cyber Crime Coordination Centre- I4C):** इस केंद्र की स्थापना कानून प्रवर्तन एजेंसियों को व्यापक एवं समन्वित तरीके से साइबर अपराधों से निपटने के लिये एक रूपरेखा एवं पारितंत्र प्रदान करने के लिये की गई थी। इसके सात घटक हैं:
    - नेशनल साइबरक्राइम थ्रेट एनालिटिक्स यूनिट
(National Cybercrime Threat Analytics Unit)
    - नेशनल साइबर क्राइम रिपोर्टिंग पोर्टल
(National Cyber Crime Reporting Portal)
    - संयुक्त साइबर अपराध जाँच दल के लिये मंच
(Platform for Joint Cyber Crime Investigation Team)
    - राष्ट्रीय साइबर अपराध फोरेंसिक प्रयोगशाला पारिस्थितिकी तंत्र
(National Cyber Crime Forensic Laboratory Ecosystem)
    - राष्ट्रीय साइबर क्राइम प्रशिक्षण केंद्र
(National Cyber Crime Training Centre)
    - साइबर क्राइम इकोसिस्टम मैनेजमेंट यूनिट
(Cyber Crime Ecosystem Management Unit)
    - राष्ट्रीय साइबर अनुसंधान और नवाचार केंद्र
(National Cyber Research and Innovation Centre.)
- **साइबर स्वच्छता केंद्र (Botnet Cleaning and Malware Analysis Centre):** इस केंद्र को भारत में बॉटनेट संक्रमणों का पता लगाकर एक सुरक्षित साइबरस्पेस का निर्माण करने और आगे के संक्रमण को रोकने के लिये अंतिम उपयोगकर्त्ताओं को सूचित करने तथा बॉटनेट शोधन एवं सुरक्षा प्रणालियों को सक्षम करने के लिये वर्ष 2017 में लॉन्च किया गया था।
- **कंप्यूटर इमरजेंसी रिस्पांस टीम - इंडिया (CERT-In):** यह MeitY का एक संगठन है जो साइबर घटनाओं पर सूचना का संग्रहण, विश्लेषण एवं प्रसारण करता है और साइबर सुरक्षा घटनाओं पर अलर्ट भी जारी करता है।
- **महत्त्वपूर्ण सूचना अवसंरचना (Critical information infrastructure- CII):** इसे एक कंप्यूटर संसाधन के रूप में परिभाषित किया गया है,

जसिके नष्ट होने से राष्ट्रीय सुरक्षा, अर्थव्यवस्था, सार्वजनिक स्वास्थ्य या सुरक्षा पर अस्थिरताकारी प्रभाव पड़ेगा।

- सरकार ने बिजली, बैंकिंग, दूरसंचार, परिवहन, शासन और रणनीतिक उद्यमों जैसे विभिन्न क्षेत्रों के CII की सुरक्षा के लिये राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure Protection Centre-NCIIPC) की स्थापना की है।

- **रक्षा साइबर एजेंसी (Defence Cyber Agency- DCyA):** DCyA भारतीय सशस्त्र बलों की एक त्रि-सेवा कमान है जो साइबर सुरक्षा खतरों से निपटने के लिये ज़िम्मेदार है। इसमें विभिन्न साइबर थ्रेट एक्टर्स के विरुद्ध हैकिंग, सर्विलांस, डेटा रिकवरी, एन्क्रिप्शन और जवाबी कार्रवाई जैसे साइबर ऑपरेशन संचालित करने की क्षमता है।

साइबर हमलों से बचने के लिये भारत को आगे क्या करना चाहिये?

- **मौजूद विधिक ढाँचे को सुदृढ़ करना:** सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000, साइबर अपराधों को नियंत्रित करने वाला भारत का प्राथमिक कानून है, जिसे नई चुनौतियों और खतरों से निपटने के लिये कई बार संशोधित किया गया है।
  - हालाँकि, आईटी अधिनियम में अभी भी कुछ कमियाँ और सीमाएँ मौजूद हैं, जैसे विभिन्न साइबर अपराधों के लिये स्पष्ट परिभाषाओं, प्रक्रियाओं एवं दंडों की कमी और साइबर अपराधियों की निम्न दोषसिद्धि दर (conviction rate)।
  - भारत को **व्यापक और अद्यतन कानून बनाने की आवश्यकता है जो साइबर सुरक्षा के सभी पहलुओं** , जैसे साइबर आतंकवाद, साइबर युद्ध, साइबर जासूसी और साइबर धोखाधड़ी को दायरे में ले।
- **साइबर सुरक्षा क्षमताओं को बढ़ाना:** साइबर सुरक्षा परिदृश्य में सुधार के लिये भारत में कई पहलें और नीतियाँ अपनाई गई हैं, जैसे राष्ट्रीय साइबर सुरक्षा नीति, साइबर सेल एवं साइबर अपराध जाँच इकाइयाँ, साइबर क्राइम रिपोर्टिंग प्लेटफॉर्म और क्षमता निर्माण एवं प्रशिक्षण कार्यक्रम।
  - हालाँकि, ये प्रयास अभी भी अपर्याप्त और खंडित हैं, क्योंकि भारत को तकनीकी कर्मचारियों, साइबर फोरेंसिक सुविधाओं, साइबर सुरक्षा मानकों और विभिन्न हितधारकों के बीच समन्वय की कमी का सामना करना पड़ रहा है।
  - भारत को अपने मानव एवं तकनीकी संसाधनों को विकसित करने, साइबर सुरक्षा के उत्कृष्टता केंद्र स्थापित करने, सर्वोत्तम अभ्यासों एवं मानकों को अपनाने और विभिन्न एजेंसियों एवं क्षेत्रों के बीच सहयोग एवं सूचना साझेदारी को बढ़ावा देने में अधिक निवेश करने की आवश्यकता है।
- **एक साइबर सुरक्षा बोर्ड की स्थापना करना:** भारत को सरकारी और निजी क्षेत्र के प्रतिभागियों के साथ एक साइबर सुरक्षा बोर्ड की स्थापना करनी चाहिये, जिसके पास किसी महत्त्वपूर्ण साइबर घटना के बाद उसका विश्लेषण करने और साइबर सुरक्षा में सुधार के लिये ठोस अनुशंसाएँ करने के लिये बैठक करने का अधिकार हो।
  - एक ज़ीरो-ट्रस्ट आर्किटेक्चर (zero-trust architecture) अपनाया जाए और साइबर सुरक्षा संबंधी भेद्यताओं एवं घटनाओं पर प्रतिक्रिया देने के लिये एक मानकीकृत 'प्लेबुक' (playbook) को अनिवार्य किया जाए। राज्य नेटवर्क की रक्षा एवं आधुनिकीकरण और इसकी घटना प्रतिक्रिया नीति (incident response policy) को अद्यतन करने के लिये तत्काल एक योजना को क्रियान्वित किया जाए।
- **अंतर्राष्ट्रीय सहयोग का विस्तार:** भारत अकेला देश नहीं है जो साइबर सुरक्षा की चुनौतियों का सामना कर रहा है, क्योंकि साइबर हमले राष्ट्रीय सीमाओं तक सीमित नहीं हैं और पूरे वैश्विक समुदाय को प्रभावित कर रहे हैं।
  - भारत को अन्य देशों और संयुक्त राष्ट्र, अंतर्राष्ट्रीय दूरसंचार संघ, इंटरपोल एवं साइबर विशेषज्ञता पर वैश्विक मंच (Global Forum on Cyber Expertise) जैसे अंतर्राष्ट्रीय संगठनों के साथ और अधिक संलग्न होने की ज़रूरत है ताकि सर्वोत्तम अभ्यासों के लेनदेन, खुफिया सूचनाओं की साझेदारी, साइबर कानूनों एवं मानकों के सामंजस्य और साइबर अन्वेषण एवं अभियोजन में सहयोग का लाभ प्राप्त हो सके।
  - भारत को आसियान क्षेत्रीय फोरम, ब्रिक्स (BRICS) **एवं भारत-अमेरिका साइबर सुरक्षा फोरम** जैसे क्षेत्रीय और द्विपक्षीय संवादों एवं पहलों में अधिक सक्रिय रूप से भाग लेने की ज़रूरत है ताकि विश्वास एवं भरोसे का निर्माण किया जा सके और साझा साइबर सुरक्षा मुद्दों एवं हितों को संबोधित किया जा सके।

अभ्यास प्रश्न: भारत पर साइबर हमलों से उत्पन्न प्रमुख चुनौतियों पर प्रकाश डालिये। सरकार साइबर हमलों से उत्पन्न जोखिमों को कम करने के लिये किस प्रकार प्रभावी रणनीति का निर्माण कर सकती है?

UPSC सिविल सेवा परीक्षा विगत वर्ष के प्रश्न

_??????????:_

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

1. यदि कोई किसी मैलवेयर कंप्यूटर तक उसकी पहुँच को बाधित कर देता है तो कंप्यूटर प्रणाली को पुनः प्रचालित करने में लगने वाली लागत
2. यदि यह प्रमाणित हो जाता है कि किसी शरारती तत्त्व द्वारा जानबूझ कर कंप्यूटर को नुकसान पहुँचाया गया है तो एक नए कंप्यूटर की लागत
3. यदि साइबर बलात्-ग्रहण होता है तो इस हानि को न्यूनतम करने के लिये विशेष परामर्शदाता की की सेवाएँ 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 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)

प्रश्न. भारत में साइबर सुरक्षा घटनाओं पर रपिोर्ट करना नम्निलखिति में से कसिके/कनिके लयि वधितिः अधदिशात्मक है? (2017)

1. सेवा प्रदाता
2. डेटा सेंटर
3. कॉर्पोरेट नकािय

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)

?????:

प्रश्न. साइबर सुरक्षा के वभिन्नि तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतयिों को ध्यान में रखते हुए समीक्षा कीजयि कि भारत ने कसि हद तक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक वकिसति की है। (2022)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/india-s-cyber-security-challenges-threats-and-strategies