साइबर सुरक्षा में सार्वजनिक-निजी तालमेल

यह एडिटोरियल 29/01/2025 को द हिंदू में प्रकाशित "Handling cybercrimes through public-private partnership model" पर आधारित है। यह लेख भारत में साइबर अपराध के बढ़ते खतरे और कानून प्रवर्तन के समक्ष आने वाली चुनौतियों को सामने लाता है। यद्यपि CCITR जैसी पहल सराहनीय हैं, फिर भी भारत को साइबर समुत्थानशक्ति बढ़ाने के लिये सुदृढ़ नीतियों, क्षमता निर्माण और सहयोग पर ध्यान केंद्रित करना चाहिये।

प्रिलिम्स के लिये:

साइबर अपराध, भारत के समक्ष प्रमुख साइबर खतरे, एडवांस्ड परसिस्टेंट थ्रेट (APT), रैनसमवेयर अटैक, क्रिप्टोकरेंसी, AI-संचालित गलत सूचना, डीपफेक, राष्ट्रीय साइबर सुरक्षा रणनीति, क्लाउड प्लेटफॉर्म, CERT-In द्वारा अनिवार्य ब्रीच रिपोर्टिंग

मेन्स के लिये:

भारत के साइबर सुरक्षा इंफ्रास्ट्रक्चर को बढ़ाने में निजी क्षेत्र की भूमिका, साइबर सुरक्षा परिदृश्य में निजी क्षेत्र को शामिल करने में प्रमुख चुनौतियाँ

साइबर अपराध एक बढ़ता हुआ वैश्विक खतरा है, जिसकी लागत वर्ष 2025 तक **सालाना 10.5 ट्रिलियन डॉलर तक पहुँचने का अनुमान** है। भारत में कानून प्रवर्तन को **धोखाधड़ी, हैकिंग, ऑनलाइन उत्पीड़न** और **निवेश घोटालों सहित साइबर खतरों में वृद्धि** का सामना करना पड़ता है। सामूहिक प्रयास की आवश्यकता का अभिनिर्धारण करते हुए, **कर्नाटक के CID ने इंफोसिस फाउंडेशन** और **DSCI** के साथ सार्वजनिक-निजी भागीदारी के माध्यम से वर्ष 2019 में साइबर अपराध जाँच प्रशिक्षण और अनुसंधान केंद्र (CCITR) की शुरुआत की। यद्यपि CCITR जैसी पहल सराहनीय हैं, फिर भी भारत को बेहतर **नीतियों, क्षमता निर्माण** और **सरकार, उद्योग एवं शिक्षाविदों के बीच सहयोग** के माध्यम से साइबर समुत्थानशक्ति बढ़ाने पर ध्यान केंद्रित करना चाहिये।

भारत के समक्ष प्रमुख साइबर खतरे क्या हैं?

- **सरकारी तत्त्वों द्वारा बढ़ती साइबर जासूसी:** भारत को रक्षा, ऊर्जा और सरकारी संस्थानों जैसे महत्त्वपूर्ण क्षेत्रों को निशाना बनाने वाले विदेशी राज्य प्रायोजित समूहों से बढ़ते खतरों का सामना करना पड़ रहा है।
  - **चीन और पाकिस्तान से** एडवांस्ड परसिस्टेंट थ्रेट (APT) निगरानी करते हैं, संवेदनशील डेटा चुराते हैं और रणनीतिक परियोजनाओं को बाधित करते हैं।
  - सुदृढ़ स्वदेशी साइबर सुरक्षा इंफ्रास्ट्रक्चर की कमी के कारण भारत ऐसे हमलों के प्रति संवेदनशील है।
    - वर्ष 2021 की एक **रिपोर्ट में सुझाव** दिया गया है कि **चीनी राज्य प्रायोजित अभिकर्त्ताओं** ने LAC पर बढ़ते तनाव के बीच मैलवेयर के साथ भारतीय विद्युत ग्रिड और बंदरगाहों को निशाना बनाने का प्रयास किया है।
- **महत्त्वपूर्ण बुनियादी अवसंरचना पर बढ़ते रैनसमवेयर हमले: रैनसमवेयर समूह** तेज़ी से भारत के वित्तीय, स्वास्थ्य सेवा और IT क्षेत्रों को निशाना बना रहे हैं, जिससे आवश्यक सेवाएँ बाधित हो रही हैं।
  - हैकर्स सिस्टम को लॉक करने के लिये परिष्कृत मैलवेयर का प्रयोग करते हैं और **फिरौती की मांग** करते हैं, जो **प्रायः क्रिप्टोकरेंसी में** होती है, जिससे **ट्रैकिंग मुश्किल** हो जाती है।
  - भारतीय उद्यमों में प्रायः **आवश्यक साइबर सुरक्षा का अभाव** रहता है**,** जिसके कारण वे इन हमलों का आसान शिकार बन जाते हैं।
    - नवंबर 2022 में एम्स दिल्ली के सर्वर से छेड़छाड़ की गई थी, रिपोर्टों में **विदेशी अभिकर्त्ताओं से जुड़े संभावित साइबर हमले** का सुझाव दिया गया था।
    - एक हालिया रिपोर्ट के अनुसार, भारत रैनसमवेयर हमलों के लिये एक प्रमुख लक्ष्य के रूप में उभरा है,**जो एशिया प्रशांत और जापान (APJ) क्षेत्र में दूसरे स्थान पर है।**
- **वित्तीय क्षेत्र को लक्षित करने वाले साइबर अपराध में वृद्धि:** भारत के तेज़ी से डिजिटल बैंकिंग विस्तार के कारण **फिशिंग, UPI धोखाधड़ी** और **डिजिटल भुगतान घोटालों में वृद्धि** हुई है।
  - धोखेबाज **डिजिटल भुगतान गेटवे की कमियों का फायदा** उठाते हैं और सोशल इंजीनियरिंग रणनीति के माध्यम से अनजान **उपयोगकर्त्ताओं का शोषण** करते हैं।
  - साइबर सुरक्षा के प्रति कम जागरूकता और बैंकिंग नेटवर्क में पुराने सॉफ्टवेयर का उपयोग वित्तीय संस्थाओं को असुरक्षित बनाता है।
  - RBI की वार्षिक रिपोर्ट के अनुसार, **400 मिलियन से अधिक विशिष्ट उपयोगकर्त्ताओं के साथ UPI** में **वित्तीय धोखाधड़ी में**

वृद्धि देखी गई है, जो सत्र 2022-23 की तुलना में **2023-24 में 166%** बढ़ गई।

- **डीपफेक और AI-संचालित गलत सूचना:** **AI-संचालित गलत सूचना** और **डीपफेक** **वीडियो** के बढ़ने से भारत की **चुनावी प्रक्रिया, सामाजिक सद्भाव और सार्वजनिक धारणा को खतरा** है।
  - **राजनीतिक दल, विदेशी अभिकर्त्ता** और **दुर्भावनापूर्ण समूह** दुष्प्रचार फैलाने, जनता की भावनाओं से छेड़छाड़ करने तथा विरोधियों को बदनाम करने के लिये AI का हथियार बना रहे हैं।
  - उदाहरण के लिये, वर्ष 2023 में **अभिनेत्री रश्मिका मंदाना का एक डीपफेक वायरल** हुआ, जिसमें तकनीक के खतरों पर प्रकाश डाला गया।
  - **विश्व आर्थिक मंच की ग्लोबल रिस्क रिपोर्ट- 2024** के लिये सर्वेक्षण किये गए विशेषज्ञों के अनुसार, **गलत सूचना और भ्रामक सूचना** के जोखिम के मामले में भारत को सर्वोच्च स्थान दिया गया है।
- **भारतीय उद्यमों पर आपूर्ति शृंखला साइबर हमले:** हैकर्स बड़े भारतीय निगमों में प्रवेश पाने के लिये **तृतीय पक्ष के विक्रेताओं और सॉफ्टवेयर आपूर्ति शृंखलाओं को तेज़ी से निशाना** बना रहे हैं।
  - डिजिटल इको-सिस्टम की परस्पर संबद्ध प्रकृति का अर्थ है कि एक कमज़ोर कड़ी कई कंपनियों के लिये खतरा बन सकती है।
    - MSME (जो बड़ी कंपनियों के लिये विक्रेता के रूप में काम करते हैं) **के बीच सख्त साइबर सुरक्षा नीतियों का अभाव** जोखिम को और भी बढ़ा देता है।
  - विदेशी सॉफ्टवेयर और क्लाउड सॉल्यूशन्स पर भारत की बढ़ती निर्भरता भी उसे गुप्त शोषण के प्रति संवेदनशील बनाती है।
  - इसका एक उदाहरण दिसंबर 2020 में पाया गया **सोलरविंड्स सप्लाई चेन अटैक** है, जहाँ हैकरों ने **सोलरविंड्स के ओरियन सॉफ्टवेयर** (एक व्यापक रूप से इस्तेमाल किया जाने वाला IT प्रबंधन उपकरण) को निशाना बनाया।
- **साइबर आतंकवाद और डार्क वेब गतिविधियाँ:** आतंकवादी समूह अपने अभियानों के वित्तपोषण और हमलों के समन्वय के लिये **डार्क वेब, एन्क्रिप्टेड मैसेजिंग प्लेटफॉर्म** और **क्रिप्टोकरेंसी लेन-देन** का लाभ उठा रहे हैं।
  - **सोशल मीडिया** और **ऑनलाइन हेट ग्रुप्स के माध्यम से कट्टरपंथ** राष्ट्रीय सुरक्षा के लिये बढ़ता खतरा है।
  - **साइबर आतंकवादी गुमनाम रहने के लिये भारत के सुभेद्य निगरानी तंत्र** और VPN नेटवर्क का फायदा उठाते हैं। कई स्लीपर सेल इन प्लेटफॉर्म का इस्तेमाल बिना संसूचन **भर्ती और योजना बनाने के लिये** कर रहे हैं।
    - सुरक्षा एजेंसियों ने बताया है कि **ISIS से संबद्ध समूह भारतीय युवाओं की भर्ती के लिये टेलीग्राम और डार्क वेब फोरम का उपयोग** करते हैं।
      - NIA ने वर्ष 2016 में 35 से अधिक ISIS आतंकवादियों को गिरफ्तार किया और **एन्क्रिप्टेड चरमपंथ का पर्दाफाश** किया, जहाँ भारतीय युवाओं को टेलीग्राम व सिग्नल जैसे संचार ऐप पर भर्ती किया जा रहा था।
- **IoT और स्मार्ट सिटी कमज़ोरियाँ: निगरानी कैमरे, यातायात प्रबंधन** और **सार्वजनिक उपयोगिताओं** सहित **स्मार्ट सिटी प्रौद्योगिकी** को तेज़ी से अपनाने से नए साइबर सुरक्षा जोखिम उत्पन्न हो गए हैं।
  - भारत में तैनात कई IoT उपकरणों में उचित एन्क्रिप्शन का अभाव है और वे हैकिंग के प्रति संवेदनशील हैं।
  - समझौता किये गए IoT नेटवर्क से बड़े पैमाने पर व्यवधान उत्पन्न हो सकते हैं, जिनमें ब्लैकआउट, यातायात जाम और गोपनीयता का उल्लंघन शामिल है।
  - हैकर समूह और शत्रु राष्ट्र पहले से ही इन कमज़ोरियों की जाँच कर रहे हैं।
    - उदाहरण के लिये, वर्ष 2020 में **मुंबई की बिजली कटौती** को चीन के साइबर हमले से जोड़ा गया था।

भारत के साइबर सुरक्षा इंफ्रास्ट्रक्चर को बढ़ाने में निजी क्षेत्र क्या भूमिका निभा सकता है?

- **साइबर सुरक्षा अनुसंधान एवं विकास तथा स्वदेशी समाधानों को सुदृढ़ बनाना:** निजी क्षेत्र स्वदेशी अनुसंधान में निवेश करके तथा भारत की आवश्यकताओं के अनुरूप **उन्नत सुरक्षा समाधान विकसित करके साइबर सुरक्षा में नवाचार** को बढ़ावा दे सकता है।
  - **विदेशी साइबर सुरक्षा फर्मों पर निर्भरता** से भू-राजनीतिक जोखिमों और आयातित प्रौद्योगिकियों में संभावित गुप्त खतरों के प्रति संवेदनशीलता बढ़ जाती है।
  - **निजी भागीदारों द्वारा समर्थित स्वदेशी समाधान** डेटा इंटीग्रिटी सुनिश्चित कर सकते हैं और बाहरी निर्भरता से होने वाले जोखिम को कम कर सकते हैं।
  - उदाहरण के लिये, IIT कानपुर में साइबर सुरक्षा प्रौद्योगिकी नवाचार केंद्र **C3iHub** ने साइबर सुरक्षा सॉल्यूशन को आगे बढ़ाने के लिये **टाटा एडवांस्ड सिस्टम्स के साथ साझेदारी** की है।
- **साइबर खतरे की खुफिया जानकारी पर सरकार के साथ सहयोग:** निजी कंपनियाँ **ठीक समय की खतरे की खुफिया जानकारी साझा करने** और राष्ट्रीय बुनियादी अवसंरचना पर **साइबर हमलों को रोकने के लिये सरकारी एजेंसियों के साथ काम** कर सकती हैं।
  - यद्यपि **CERT-In ने अनिवार्य ब्रीच रिपोर्टिंग** जैसे उपायों को लागू किया है, फिर भी खुफिया जानकारी साझा करने का काम अभी भी सीमित है तथा कानून प्रवर्तन और वाणिज्यिक कंपनियों के बीच बहुत कम सहयोग है।
  - एक सुदृढ़ सार्वजनिक-निजी खतरा खुफिया नेटवर्क सक्रिय खतरे का पता लगाने और घटना पर प्रतिक्रिया को बढ़ा सकता है।
    - राज्य प्रायोजित तत्त्वों से साइबर खतरों का मुकाबला करने के लिये यह अत्यंत आवश्यक है।
    - उदाहरण के लिये, **IBM की एक्स-फोर्स थ्रेट इंटेलिजेंस** साइबर खतरों की पहचान करने और उन्हें कम करने के लिये भारतीय प्राधिकारियों के साथ सहयोग करती है।
- **वित्तीय क्षेत्र में साइबर सुरक्षा को बढ़ाना: बैंकिंग, फिनटेक** और **UPI भुगतान** के तेज़ी से डिजिटलीकरण के साथ, निजी भागीदारों को धोखाधड़ी और वित्तीय साइबर अपराध को रोकने के लिये सुरक्षा कार्यढाँचे को मज़बूत करना आवश्यक है।
  - निजी क्षेत्र द्वारा संचालित नवाचार जैसे कि **AI-संचालित धोखाधड़ी का पता लगाना** और **ब्लॉकचेन-आधारित सुरक्षा,** वित्तीय लेन-देन को सुरक्षित करने में मदद कर सकते हैं।
    - उदाहरण के लिये, कंप्लीएडवांटेज वित्तीय संस्थानों को **AI-संचालित धोखाधड़ी और AML जोखिम** का पता लगाने की सुविधा प्रदान करता है।

- **कुशल साइबर सुरक्षा कार्यबल का निर्माण:** भारत में प्रशिक्षित साइबर सुरक्षा पेशेवरों की तीव्र कमी को दूर करने के लिये साइबर सुरक्षा शिक्षा और कौशल विकास में निजी क्षेत्र का निवेश आवश्यक है।
    - कई **भारतीय कंपनियों को कुशल विशेषज्ञ की खोज़ में कठिनाई** हो रही है, जिसके कारण उद्यमों और सरकारी संस्थानों में साइबर सुरक्षा की स्थिति सुभेद्य होती जा रही है।
        - मई 2023 में, प्रतिभा की कमी के कारण भारत में लगभग **40000 साइबर सुरक्षा पेशेवर नौकरी रिक्तियाँ** भरी नहीं गईं।
    - कॉर्पोरेट संस्थाएँ विश्वविद्यालयों के साथ साझेदारी कर सकती हैं, **साइबर सुरक्षा बूट कैंप की पेशकश** कर सकती हैं, और इस **कौशल अंतर को समाप्त करने के लिये इन-हाउस प्रशिक्षण** प्रदान कर सकती हैं। निजी क्षेत्र भी IT पेशेवरों को बेहतर कौशल प्रदान करने के लिये वैश्विक प्रमाणन कार्यक्रम स्थापित करने में मदद कर सकता है।
- **सुरक्षित क्लाउड और डेटा संरक्षण अवसंरचना का विकास:** जैसे-जैसे भारत **डेटा स्थानीयकरण** की ओर बढ़ रहा है, निजी कंपनियाँ राष्ट्रीय डेटा परिसंपत्तियों की सुरक्षा के लिये सुरक्षित क्लाउड और डेटा स्टोरेज सॉल्यूशन बनाने में मदद कर सकती हैं।
    - वर्तमान में, **भारतीय डेटा का एक बहुत बड़ा हिस्सा विदेशी क्लाउड प्लेटफॉर्मों पर होस्ट** किया जाता है, जिससे निगरानी और अनधिकृत अभिगम का खतरा बना रहता है।
        - निजी कंपनियाँ डेटा सुरक्षा को मज़बूत करने के लिये AI-संचालित एन्क्रिप्शन और **शून्य-विश्वास सुरक्षा कार्यढाँचे में निवेश** कर सकती हैं।
        - उदाहरण के लिये, रिलायंस जियो ने सुरक्षित क्लाउड स्टोरेज समाधान प्रदान करने के लिये **अपना स्वदेशी जियोक्लाउड प्लेटफॉर्म** लॉन्च किया।
- **डीपफेक** और **AI-संचालित साइबर खतरों को विनियमित करना:** AI-जनित **डीपफेक घोटाले, गलत सूचना और साइबर धोखाधड़ी** बढ़ने के साथ, निजी फर्म इन खतरों का मुकाबला करने के लिये पहचान उपकरण विकसित करने में मदद कर सकती हैं।
    - बिग टेक फर्म्स और साइबर सुरक्षा स्टार्टअप डीपफेक कंटेंट को चिह्नित करने तथा उसका मुकाबला करने के लिये AI-आधारित पहचान मॉडल बना सकते हैं।
        - उदाहरण के लिये, **McAfee®** डीपफेक डिटेक्टर किसी वीडियो में AI-जनरेटेड ऑडियो का पता लगाने पर कुछ सेकंड में लोगों को अलर्ट कर देता है, जिससे भारतीय उपभोक्ताओं को असली और नकली में अंतर करने में मदद मिलती है।
- **साइबर-जागरूक कॉर्पोरेट संस्कृति को बढ़ावा देना:** निजी संगठन नियमित प्रशिक्षण, फिशिंग सिमुलेशन और नीति प्रवर्तन आयोजित करके कर्मचारियों के बीच **साइबर सुरक्षा-प्रथम मानसिकता को बढ़ावा** दे सकते हैं।
    - **मानवीय त्रुटि सबसे बड़ी साइबर सुरक्षा कमज़ोरियों में से एक** है, जिसके कारण डेटा उल्लंघन और **सिस्टम से समझौता** होता है।
    - नियमित साइबर सुरक्षा अभ्यास और घटना प्रतिक्रिया योजनाएँ साइबर जोखिमों को बहुत हद तक कम कर सकती हैं।
        - यह संवेदनशील डेटा प्रबंधन वाले **IT, BFSI और स्वास्थ्य सेवा क्षेत्रों के लिये** विशेष रूप से महत्त्वपूर्ण है।

साइबर सुरक्षा में निजी क्षेत्र को शामिल करने में प्रमुख चुनौतियाँ क्या हैं?

- **स्पष्ट विनियामक कार्यढाँचे और नीतिगत प्रोत्साहनों का अभाव:** एक **सुपरिभाषित साइबर सुरक्षा इंफ्रास्ट्रक्चर का अभाव** राष्ट्रीय साइबर रक्षा पहलों में निजी क्षेत्र की भागीदारी को हतोत्साहित करता है।
    - राष्ट्रीय साइबर सुरक्षा रणनीति जैसी नीतियाँ बड़े पैमाने पर क्रियान्वित नहीं हुई हैं तथा मौजूदा नियम कई एजेंसियों में विखंडित हैं।
    - **स्पष्ट प्रोत्साहन, कर लाभ या देयता सुरक्षा के बिना,** निजी कंपनियाँ राष्ट्रीय साइबर सुरक्षा प्रयासों में निवेश करने में हिचकिचाती रहती हैं।
- **साइबर सुरक्षा निवेश की उच्च लागत:** मज़बूत साइबर सुरक्षा इंफ्रास्ट्रक्चर को लागू करने के लिये पर्याप्त वित्तीय निवेश की आवश्यकता होती है, जिसे **कई निजी कंपनियाँ, विशेष रूप से MSME, वहन करने के लिये संघर्ष** करती हैं।
    - उन्नत सुरक्षा समाधान जैसे कि **AI-संचालित खतरे का पता लगाना, जीरो ट्रस्ट फ्रेमवर्क** और क्लाउड सुरक्षा निरंतर उन्नयन की मांग करते हैं।
    - लागत कारक **निजी भागीदारों को साइबर सुरक्षा में सक्रिय रूप से निवेश करने से हतोत्साहित करता है,** जिससे वे साइबर हमलों के प्रति असुरक्षित हो जाते हैं।
        - भारतीय संगठन साइबर सुरक्षा पर प्रतिवर्ष औसतन केवल **2.8 मिलियन डॉलर खर्च** करते हैं, जो आमतौर पर **उनके IT बजट का 10% से भी कम** है।
- **कमज़ोर सार्वजनिक-निजी खतरा खुफिया साझेदारी:** प्रभावी साइबर सुरक्षा के लिये **सरकारी एजेंसियों** और **निजी फर्मों के बीच सटीक समय की खुफिया साझेदारी की आवश्यकता** होती है, लेकिन भारत में इसके लिये संरचित कार्यढाँचे का अभाव है।
    - निजी कंपनियों को डर है कि यदि वे साइबर घटनाओं का खुलासा करेंगी तो उन पर विनियामक कार्रवाई होगी और उनकी प्रतिष्ठा को नुकसान पहुँचेगा।
    - **CERT-In ने उल्लंघन की सूचना देने के लिये 6 घंटे का समय अनिवार्य** कर दिया है, लेकिन दंड के डर के कारण अनुपालन कम बना हुआ है।
- **विदेशी साइबर सुरक्षा समाधानों पर निर्भरता: भारत में कई निजी कंपनियाँ विदेशी साइबर सुरक्षा उपकरणों और सॉफ्टवेयर पर बहुत अधिक निर्भर** हैं, जिससे भू-राजनीतिक कमज़ोरियों एवं निगरानी की सुभेद्यता का खतरा बढ़ जाता है।
    - जबकि निजी कंपनियाँ लागत प्रभावी विदेशी समाधानों को प्राथमिकता देती हैं, इससे **राष्ट्रीय सुरक्षा के लिये रणनीतिक जोखिम** उत्पन्न होता है।
        - स्वदेशी साइबर सुरक्षा उत्पादों की कमी के कारण भारतीय कंपनियों को महत्त्वपूर्ण सुरक्षा अवसंरचना के लिये वैश्विक विक्रेताओं पर निर्भर रहना पड़ता है।
- **आपूर्ति शृंखला विक्रेताओं के लिये कमज़ोर साइबर सुरक्षा मानक:** कई **निजी फर्म तृतीय पक्ष के विक्रेताओं पर निर्भर** हैं, लेकिन भारत में आपूर्ति शृंखलाओं के लिये मज़बूत साइबर सुरक्षा अनुपालन आवश्यकताओं का अभाव है।
    - हमलावर बड़ी कंपनियों, विशेषकर BFSI, दूरसंचार और IT क्षेत्रों तक पहुँच बनाने के लिये **आपूर्ति शृंखलाओं में कमज़ोर कड़ी को**

नशिाना बना रहे हैं।
- उदाहरण के लयि, भारत में **आधे से अधकि (55%) स्मार्ट वनिर्माण फर्मों ने** वर्ष 2023 में **6 से अधकि अंतर्वेधन** की सूचना दी।

साइबर सुरक्षा में सार्वजनकि-नजिी भागीदारी बढ़ाने के लयि क्या उपाय अपनाए जा सकते हैं?

- **राष्ट्रीय साइबर सुरक्षा समन्वय नकिाय: सार्वजनकि-नजिी सहयोग को सुचारू बनाने के लयि** मज़बूत **नजिी क्षेत्र के प्रतनिधित्वि के साथ** एक एकीकृत **राष्ट्रीय साइबर सुरक्षा परषिद** बनाई जानी चाहयि।
  - वर्तमान में, साइबर सुरक्षा प्रयास **MeitY, CERT-In, NCIIPC और RBI में वखिंडति** हैं, जसिसे **अक्षमताएँ** उत्पन्न होती हैं। एक केंद्रीकृत नकिाय नरि्बाध खुफयि-साझाकरण, समन्वति घटना प्रतक्रियिा और नीतसिंरेखण सुनश्चिति कर सकता है।
- **सुरक्षति खतरा खुफयिा-साझाकरण मंच का क्रयिान्वयन: सरकारी एजेंसयिों और नजिी उद्यमों के बीच ठीक समय पर स्वचालति खुफयिा-साझाकरण की सुवधिा के लयि** एक **राष्ट्रीय साइबर खतरा खुफयिा एक्सचेंज (NCTIX)** की स्थापना की जानी चाहयि।
  - उत्तरदायत्वि सुरक्षा के साथ एक **संरचति, अनाम डेटा-साझाकरण कार्यढाँचा भागीदारी** को प्रोत्साहति कर सकता है।
  - उन्नत AI-संचालति नगिरानी साइबर खतरों का अधकि प्रभावी ढंग से पता लगाने, एनालसिसि करने और उन्हें कम करने में मदद कर सकती है।
- **साइबर सुरक्षा नविेश के लयि कर प्रोत्साहन की पेशकश:** नजिी कंपनयिों, वशिेष रूप से MSME को सुदृढ़ साइबर सुरक्षा उपायों के अंगीकरण को प्रोत्साहति करने की दशिा में साइबर सुरक्षा में नवेश के लयि **कर क्रेडटि और सब्सडिी** प्रदान की जानी चाहयि।
  - सरकार वदिेशी तकनीक पर नरि्भरता कम करने के लयि **स्वदेशी साइबर सुरक्षा समाधानों के लयि अनुसंधान एवं वकिास प्रोत्साहन** दे सकती है।
  - AI-संचालति साइबर रक्षा समाधानों पर काम करने वाली फर्मों को वशिेष अनुदान आवंटति कयिा जाना चाहयि।
- **साइबर सुरक्षा कौशल वकिास कार्यक्रमों को सुदृढ़ करना:** नगिम **वशिेष साइबर प्रशक्षिण** प्रदान करने के लयि **वश्ववविद्यालयों, IT प्रशक्षिण संस्थानों और स्कलि इंडयिा** जैसे सरकारी कार्यक्रमों के साथ सहयोग कर सकते हैं।
  - साइबर सुरक्षा को इंजीनयिरगि और प्रबंधन पाठ्यक्रम में शामलि कयिा जाना चाहयि। नयिमति**साइबर अभ्यास, हैकथॉन और नैतकि हैकगि प्रतयिोगताएँ** कुशल प्रतभिाओं का एक समूह तैयार कर सकती हैं।
- **नजिी उद्यमों के लयि साइबर सुरक्षा मानकों को अनवािर्य बनाना:** एक **साइबर सुरक्षा अनुपालन सूचकांक** शुरू कयिा जाना चाहयि, जसिमें व्यवसायों को उनकी सुरक्षा परपिक्वता स्तरों के आधार पर वर्गीकृत कयिा जाना चाहयि।
  - नजिी कंपनयिों, वशिेषकर **BFSI, दूरसंचार और IT** जैसे महत्त्वपूर्ण क्षेत्रों में, को जोखमि-आधारति अनुपालन कार्यढाँचे के तहत **न्यूनतम साइबर सुरक्षा मानकों को पूरा करना आवश्यक** होना चाहयि।
  - सरकार MSME के अंगीकरण में सुधार के लयि **सुरक्षा ऑडटि के लयि सब्सडिी** दे सकती है। डजिटिल पर्सनल डेटा प्रोटेक्शन एक्ट **(DPDPA), 2023 के प्रवर्तन को दृढ़ करने से जवाबदेही** सुनश्चिति होगी।
- **स्वदेशी साइबर सुरक्षा प्रौद्योगकिी परवेिश:** सरकार को वदिेशी तकनीक पर नरि्भरता कम करने के लयि **स्वदेशी साइबर सुरक्षा उपकरण वकिसति करने हेतु नजिी फर्मों और स्टार्टअप्स के साथ** काम करना चाहयि।
  - **AI-संचालति खतरे का पता लगाने, ब्लॉकचेन सुरक्षा और क्लाउड एन्क्रप्शिन पर ध्यान केंद्रति करने वाले स्टार्टअप्स** को प्रोत्साहन प्रदान कयिा जाना चाहयि।
  - एक समर्पति **साइबर सुरक्षा स्टार्टअप फंड** इस क्षेत्र में नवाचार को गतदिे सकता है।

नषि्कर्ष:

भारत की साइबर सुरक्षा को सुदृढ़ करने के लयि **सरकार और नजिी क्षेत्र दोनों को शामलि करते हुए एक सहयोगी दृष्टकिोण की आवश्यकता** है। यद्यपCCITR जैसी पहल आशाजनक दखिती हैं, भारत को **स्पष्ट वनियिामक कार्यढाँचे, बढ़ी हुई नीतगित प्रोत्साहन और सुदृढ़ सार्वजनकि-नजिी भागीदारी को प्राथमकिता** देनी चाहयि। स्वदेशी साइबर सुरक्षा समाधानों को बढ़ावा देना, खुफयिा जानकारी साझा करना और कार्यबल को बेहतर बनाना महत्त्वपूर्ण कदम हैं।

[illegible]:

प्रश्न. भारत के साइबर सुरक्षा इंफ्रास्ट्रक्चर में नजिी क्षेत्र को शामलि करने के संभावति लाभों और चुनौतयिों पर चर्चा कीजयि। सार्वजनकि-नजिी भागीदारी देश की साइबर समुत्थानशक्तकिैसे बढ़ा सकती है?

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

[illegible]

प्रश्न 1. भारत में, कसिी व्यक्तकिे साइबर बीमा कराने पर, नधिकिी हानकिी भरपाई एवं अन्य लाभों के अतरिकि्त, सामान्यतः नम्निलखिति में से कौन-कौन से लाभ दयि जाते हैं ?(2020)

1. यदि कोई मैलवेयर कंप्यूटर तक उसकी पहुँच 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 जान-बूझकर कंप्यूटर को नुकसान पहुँचाया 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 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 2. भारत में, साइबर सुरक्षा घटनाओं पर रिपोर्ट करना निम्नलिखित में से किसके/किनके लिये विधितः अधिदेशात्मक है/हैं? (2017)

1. सेवा प्रदाता (सर्विस प्रोवाइडर)
2. डेटा सेंटर
3. कॉर्पोरेट निकाय (बॉडी कॉर्पोरेट)

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)

?????

प्रश्न. साइबर सुरक्षा के विभिन्न तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतियों को ध्यान में रखते हुए समीक्षा कीजिये कि भारत ने किस हद तक एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक विकसित की है। (2022)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/public-private-synergy-in-cybersecurity