भारत की साइबर सुरक्षा

यह एडिटोरियल 28/05/2025 को द लाइवमिंट में प्रकाशित "Arm employees against sophisticated cyberattacks" पर आधारित है। यह लेख स्कैटर्ड स्पाइडर समूह द्वारा मार्क्स एंड स्पेंसर पर हाल ही में किये गए साइबर हमले पर प्रकाश डालता है, जो मानवीय कमज़ोरियों को उजागर करता है। यह भारत के तेजी से बढ़ते डिजिटल परिदृश्य में मज़बूत साइबर सुरक्षा उपायों और कर्मचारी जागरूकता की त्वरित आवश्यकता को रेखांकित करता है।

प्रिलिम्स के लिये:

साइबर अपराध, डिजिटल अरेस्ट, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल, राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र, साइबर स्वच्छता केंद्र, रैनसमवेयर हमला, साइबर अपराध पर बुडापेस्ट कन्वेंशन।

मेन्स के लिये:

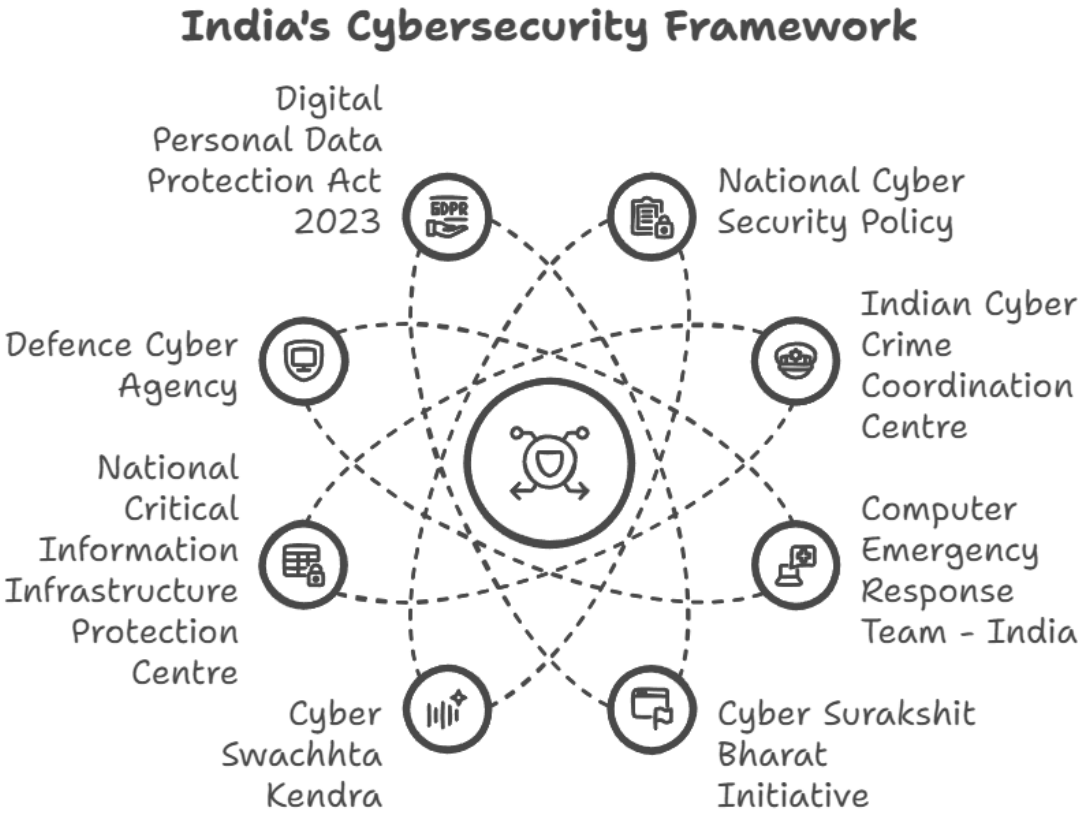
भारत के समक्ष बढ़ती प्रमुख साइबर संबंधी सुरक्षा चुनौतियाँ, भारत के विकसित हो रहे साइबर रक्षा ढाँचे में प्रमुख कमियाँ

मार्क्स एंड स्पेंसर (M&S) पर हाल ही में हुआ साइबर हमला भारत में साइबर अपराध के बढ़ते खतरे को रेखांकित करता है, जहाँ डिजिटल बुनियादी ढाँचा तेज़ी से फैल रहा है। हैकर समूह **स्कैटर्ड स्पाइडर द्वारा** ज़िम्मेदार इस उल्लंघन ने **सोशल इंजीनियरिंग रणनीति** के माध्यम से मानवीय कमज़ोरियों का लाभ उठाया, जिससे वित्तीय और प्रतिष्ठा को काफी नुकसान पहुँचा। यह घटना यह दर्शाती है कि साइबर सुरक्षा के मज़बूत उपायों की तत्काल आवश्यकता है, जिसमें **कर्मचारियों को प्रशिक्षित करना और उन्नत खतरा पहचान प्रणाली** शामिल है। जैसे-जैसे साइबर हमले और अधिक जटिल होते जा रहे हैं, भारत की ऐसी खतरों से निपटने की तैयारी उसकी बढ़ती डिजिटल अर्थव्यवस्था की सुरक्षा के लिये अत्यंत महत्त्वपूर्ण है।

भारत के सामने प्रमुख उभरते साइबर सुरक्षा खतरे क्या हैं?

- **AI-संचालित फिशिंग और सोशल इंजीनियरिंग हमलों की परिष्कृत तकनीक: फिशिंग हमले एआई-जनरेटेड सामग्री और वास्तविक समय सोशल इंजीनियरिंग का उपयोग करके** विकसित हुए हैं, जो पारंपरिक फिल्टर को दरकिनार करते हैं और कर्मचारियों को प्रभावी ढंग से धोखा देते हैं।
  - ये हमले मानवीय कमजोरियों का फायदा उठाते हैं, जैसा कि हाल ही में **मार्क्स एंड स्पेंसर में हुए उल्लंघन** में देखा गया, जिसका श्रेय **स्कैटर्ड स्पाइडर** द्वारा सोशल इंजीनियरिंग को दिया जाता है।
  - हालिया आँकड़ों से पता चलता है कि **वर्ष 2024 की शुरुआत में भारत के BFSI क्षेत्र में फिशिंग हमलों में 175% की वृद्धि हुई** है, जिसमें 54% हमले बहानेबाजी की रणनीति से जुड़े थे।
    - **वर्ष 2024 में दैनिक साइबर अपराध की शिकायतों में 113.7% की वृद्धि** होगी, जो इस बढ़ते खतरे को रेखांकित करती है।
- **क्लाउड और API कमज़ोरियों का दोहन:** तेज़ी से क्लाउड को अपनाने से गलत तरीके से कॉन्फिगर किये गए **वातावरण और कमज़ोर API सुरक्षा** के माध्यम से नए हमले के खतरा उत्पन्न हो गए हैं।
  - हमलावर **सार्वजनिक रूप से सुलभ क्लाउड बकेट और खराब** तरीके से सुरक्षित एडमिन कंसोल का फायदा उठाते हैं, जिससे संवेदनशील डेटा तक अनधिकृत पहुँच संभव हो जाती है तथा सेवाएँ बाधित होती हैं। यह भारत की बढ़ती अर्थव्यवस्था में विकसित हो रहे डिजिटल बुनियादी ढाँचे को सुरक्षित करने में एक महत्त्वपूर्ण कमी को दर्शाता है।
  - उदाहरण के लिये, **CERT-In ने वर्ष 2024 में क्लाउड मिसकॉन्फिगरेशन और API को लक्षित** करने वाले शोषणों में **180% की वृद्धि** की सूचना दी, जो इन वैक्टरों पर बढ़ते प्रतिकूल फोकस को उजागर करता है।
- **महत्त्वपूर्ण पारिस्थितिकी प्रणालियों को लक्ष्य करके आपूर्ति शृंखला हमलों में वृद्धि: साइबर अपराधी** प्राथमिक सुरक्षा को दरकिनार करने के लिये **विश्वसनीय विक्रेताओं और तृतीय-पक्ष प्रदाताओं** में तेजी से घुसपैठ कर रहे हैं, जिससे संपूर्ण आपूर्ति शृंखला को खतरा उत्पन्न हो रहा है।
  - यह **अप्रत्यक्ष हमला पद्धति महत्त्वपूर्ण वित्तीय और सरकारी नेटवर्क की अखंडता** को खतरे में डालती है, जिससे बचाव के लिये उन्नत अंतर-क्षेत्रीय समन्वय की आवश्यकता होती है।
  - **DDoS हमलों** से आपूर्ति शृंखला में भी बाधा उत्पन्न हो सकती है, जैसा कि **कुछ वर्ष पहले देखा** गया था, जब **सूडानी हैकरों** ने हवाई अड्डों और अस्पतालों की वेबसाइटों को बंद कर दिया था, जिससे लंबे समय तक उनके संचालन पर गंभीर असर पड़ा था।
  - डिजिटल थ्रेट रिपोर्ट 2024 **आपूर्ति शृंखला जोखिमों को एक बड़ी** चुनौती के रूप में रेखांकित करती है, जिसमें दुर्भावनापूर्ण कोड लाइब्रेरी और समझौता किये गए विक्रेता सॉफ्टवेयर सामान्य प्रवेश बिंदु हैं।

- **AI-संचालित डीपफेक और चैटबॉट फिशिंग: प्रतिरूपण** और चैटबॉट-आधारित फिशिंग अभियानों के लिये **AI-जनरेटेड डीपफेक ऑडियो और वीडियो** का उद्भव धोखाधड़ी को काफी हद तक बढ़ा देता है।
  - ये तकनीकें बड़े पैमाने पर क्रेडेंशियल थेफ्ट्स और सामाजिक हेरफेर को सक्षम बनाती हैं, जिससे डिजिटल संचार में भरोसा कम होता है। खतरे का परिदृश्य अब AI-जागरूक पहचान एवं प्रतिक्रिया तंत्र की मांग करता है।
  - **WormGPT और FraudGPT जैसे दुर्भावनापूर्ण LLMs (लार्ज लैंग्वेज मॉडल्स)** के ज़रिये होने वाले हमलों की घटनाएं सामने आई हैं, जो वित्तीय और प्रशासनिक क्षेत्रों में बहुआयामी जोखिम उत्पन्न कर रहे हैं।
- **मोबाइल मैलवेयर और मुद्रीकरण योजनाओं का प्रसार:** मोबाइल प्लेटफॉर्म, **विशेष रूप से Android, पर मैलवेयर, एडवेयर और संभावित अवांछित प्रोग्राम (PUPs)** के संक्रमण की दर बहुत अधिक है, जिसे व्यावसायिक उद्देश्यों द्वारा संचालित किया जा रहा है।
  - **भारत की साइबर सुरक्षा स्थिति में मोबाइल सुरक्षा एक कमज़ोर कड़ी** बनी हुई है। सेक्राइट (Seqrite) के टेलीमेट्री डेटा के अनुसार, मोबाइल खतरों में से **42% मैलवेयर, 32% PUPs और 26% एडवेयर** हैं, जो मोबाइल सुरक्षा को तत्काल मज़बूत करने की आवश्यकता को रेखांकित करता है।
  - हाल ही में राजस्थान में एक घटना सामने आई, जिसमें **व्हाट्सएप** के माध्यम से भेजी गई एक साधारण तस्वीर डाउनलोड करने पर फोन हैक हो गया और खाते से पैसे चोरी हो गए। यह **स्टेगनोग्राफी हमलों** का एक उदाहरण है।
- **महत्त्वपूर्ण क्षेत्रों में IoT कमज़ोरियाँ:** भारत में तेजी से अपनाए जा रहे IoT (इंटरनेट ऑफ थिंग्स) उपकरण पुराने और असुरक्षित तकनीक के कारण जटिल सुरक्षा चुनौतियाँ पेश कर रहे हैं।
  - ज्ञात IoT कमज़ोरियों का दोहन **उच्च प्रभाव वाले उल्लंघनों** का कारण बन सकता है, विशेष रूप से BFSI एवं स्वास्थ्य सेवा क्षेत्रों में, जहाँ डिवाइस सुरक्षा को अक्सर नज़रअंदाज कर दिया जाता है।
  - उदाहरण के लिये **99% IoT हमले ज्ञात खामियों का फायदा उठाते हैं, जिनमें से 34% के कारण बैंकिंग, वित्तीय सेवाओं और बीमा संस्थाओं को 5-10 मिलियन डॉलर का नुकसान** होता है, जिससे गंभीर वित्तीय और परिचालन जोखिम सामने आते हैं।
- **डिजिटल प्लेटफॉर्म के माध्यम से वित्तीय धोखाधड़ी में वृद्धि: ऑनलाइन निवेश घोटाले, अवैध ऋण देने वाले ऐप, टेलीग्राम कार्य धोखाधड़ी और ट्रेडिंग घोटाले सहित वित्तीय धोखाधड़ी**, विनियामक और तकनीकी अंतराल का फायदा उठाते हुए बढ़ रही हैं।
  - ये धोखाधड़ी उपभोक्ताओं की संपत्ति को नष्ट करती हैं और डिजिटल वित्त में विश्वास को कमजोर करती हैं, जिससे नियामकों, फिनटेक कंपनियों और कानून प्रवर्तन एजेंसियों के बीच समन्वित प्रयासों की आवश्यकता होती है।
  - वर्ष 2024 में ही साइबर अपराधियों ने **डिजिटल धोखाधड़ी** के ज़रिए **₹1,750 करोड़ से अधिक** की हानि पहुँचाई है तथा नेशनल साइबरक्राइम रिपोर्टिंग पोर्टल पर 7.4 लाख से अधिक शिकायतें दर्ज की गईं, जो खतरे की गंभीरता को दर्शाता है।
- **डिजिटल गिरफ्तारी घोटाले और सामाजिक हेरफेर का बढ़ता खतरा:** साइबर अपराधी अब कानून प्रवर्तन एजेंसियों का रूप धारण कर "डिजिटल अरेस्ट स्कैम", ब्लैकमेल और फिरौती वसूलने जैसी धोखाधड़ी कर रहे हैं, जो आम जनता के सरकारी संस्थाओं पर विश्वास का फायदा उठाते हैं।
  - इन घोटालों के कारण, विशेष रूप से कमज़ोर समूहों को भारी वित्तीय नुकसान और मनोवैज्ञानिक संकट का सामना करना पड़ा है।
    - **उदाहरण के लिये हरियाणा के नूंह गाँव** में इस तरह की धोखाधड़ी (ओटीपी घोटाले सहित) की कई रिपोर्टें सामने आई हैं, जो ग्रामीण क्षेत्रों में इन घोटालों के व्यापक प्रभाव को उजागर करती हैं।
  - **भारत सरकार ने 2024 में डिजिटल अरेस्ट स्कैम से जुड़े 83,000** से अधिक **व्हाट्सएप अकाउंट्स** को ब्लॉक किया और ₹120 करोड़ का नुकसान दर्ज की गई, जो इस समस्या के व्यापक प्रभाव को दर्शाता है।



भारत का वर्तमान सुरक्षा ढाँचा बढ़ते खतरों के लिये अपर्याप्त क्यों है?

- **एजेंसियों और अधिकार क्षेत्रों के बीच विखंडित समन्वय:** भारत का साइबर सुरक्षा पारिस्थितिकी तंत्र **केंद्रीय और राज्य एजेंसियों** के बीच विखंडित समन्वय से ग्रस्त है, जिसके कारण प्रतिक्रिया में देरी और प्रवर्तन में अंतराल होता है।
  - **ओवरलैपिंग जनादेश और एकीकृत प्रोटोकॉल** की कमी तेजी से खतरे की रोकथाम और खुफिया जानकारी साझा करने को कमज़ोर करती है। प्रभावी साइबर सुरक्षा के लिये निर्बाध अंतर-एजेंसी सहयोग की आवश्यकता होती है, जो अभी भी प्रगति पर है।
  - I4C (इंडियन साइबर क्राइम कोऑर्डिनेशन सेंटर) और **संयुक्त साइबर अपराध समन्वय दल (JCCT)** की स्थापना के बावजूद, **वर्ष 2023 में साइबर अपराध की शिकायतें 1.5 मिलियन** से अधिक हो गईं, जिससे समय पर शमन में प्रणालीगत समन्वय चुनौतियों का पता चलता है।
- **अपर्याप्त कुशल साइबर कार्यबल और प्रशिक्षण:** साइबर खतरों का तेजी से विकास **कुशल साइबर सुरक्षा पेशेवरों** की उपलब्धता को पीछे छोड़ देता है, जिसके परिणामस्वरूप प्रतिभा की गंभीर कमी बनी हुई है।
  - **साइट्रेन** जैसी प्रशिक्षण पहलों से मदद तो मिली है, लेकिन वे सार्वजनिक और निजी क्षेत्रों में **विशेषज्ञों की विशाल मांग को पूरा करने के लिये अपर्याप्त हैं।**
  - यह अंतर प्रभावी खतरे का पता लगाने, घटना की प्रतिक्रिया और सक्रिय रक्षा रणनीतियों में बाधा डालता है।
  - **MOOC प्लेटफॉर्म्स** के माध्यम से लगभग **76,000** पुलिस अधिकारियों को साइबर अपराध का प्रशिक्षण मिला है, फिर भी एक बड़ा हिस्सा अभी भी विशेष प्रशिक्षण से वंचित है।
- **उन्नत खतरा पहचान प्रौद्योगिकियों को अपर्याप्त रूप से अपनाना:** भारत का सुरक्षा बुनियादी ढाँचा **मुख्यतः सिग्नेचर-आधारित पहचान** पर निर्भर है, जो **ज़ीरो-डे एक्सप्लॉइट्स और AI-आधारित हमलों** जैसे जटिल खतरों के विरुद्ध पर्याप्त नहीं है।
  - व्यवहार-आधारित, AI-संचालित खतरा खुफिया जानकारी को धीमी गति से अपनाने से गंभीर कमजोरियाँ उजागर हो जाती हैं।
  - आधुनिक साइबर सुरक्षा के लिये अनुकूल प्रतिद्वंद्वियों से आगे रहने के लिये अत्याधुनिक प्रौद्योगिकी एकीकरण की आवश्यकता है।
  - हाल ही में सेक्राइट के आँकड़ों से पता चलता है **कि 85% निर्भरता हस्ताक्षर-आधारित पहचान** पर है, जबकि **केवल 14.5%** खतरों की पहचान व्यवहार-आधारित तरीकों से की जाती है, जो प्रौद्योगिकी अंतराल को दर्शाता है।
- **क्लाउड और API सुरक्षा प्रशासन पर सीमित ध्यान:** भारत में तेजी से हो रही **क्लाउड अपनाने की प्रक्रिया** के बावजूद, **API और क्लाउड कॉन्फिगरेशन** की सुरक्षा के लिये मज़बूत गवर्नेंस फ्रेमवर्क की कमी बनी हुई है, जिससे व्यापक जोखिम उत्पन्न हो रहा है।
  - कई भारतीय उद्यमों के पास क्लाउड वातावरण में सतत् निगरानी और पैच प्रबंधन के लिये व्यापक नीतियों का अभाव है।
  - **CERT-In ने वर्ष 2024 में क्लाउड और API एक्सप्लॉइट में 180% की वृद्धि** दर्ज की, जो क्लाउड सुरक्षा स्थिति में स्पष्ट कमियों को दर्शाता है।
- **उभरते डिजिटल क्षेत्रों में अपर्याप्त विनियमन और प्रवर्तन:** फिनटेक, IoT और डिजिटल भुगतानों में तीव्र वृद्धि नियामक ढाँचों से आगे निकल

गई है, जिससे महत्त्वपूर्ण क्षेत्र नए साइबर खतरों के प्रति संवेदनशील हो गए हैं।
    - मौजूदा कानून अक्सर प्रतिक्रियाशील होते हैं और AI-संचालित धोखाधड़ी या IoT कमज़ोरियों जैसे नए हमलों को पूरी तरह से संबोधित नहीं कर पाते।
    - **डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023** AI टूल्स को उस स्थिति में छूट देता है जब वे अनुसंधान, संग्रह या सांख्यिकी उद्देश्यों के लिये व्यक्तिगत डेटा को संसाधित करते हैं—जब तक कि व्यक्तियों पर कोई निर्णय नहीं लिया जाता और निर्धारित मानकों का पालन किया जाता है। यह प्रावधान संभावित दुरुपयोग का रास्ता खोल सकता है।
- **सक्रिय साइबर आक्रामक रणनीति का अभाव:** भारत वर्तमान में **रक्षात्मक साइबर सुरक्षा पर ज़ोर** देता है, लेकिन एक अच्छी तरह से व्यक्त आक्रामक साइबर क्षमता की अनुपस्थिति साइबरस्पेस में विरोधियों को चुनौती देने में असमर्थ बना देती है।
    - सक्रिय प्रतिवाद और खतरे की खोज के माध्यम से साइबर रोकथाम, परिष्कृत हमलों को समय रहते रोकने के लिये महत्त्वपूर्ण है। **"सुपर साइबर फोर्स" अवधारणा** को अभी क्रियान्वित किया जाना है।
    - **PRAHAR की रिपोर्ट** के अनुसार, वर्ष 2033 तक साइबर हमलों की संख्या प्रति वर्ष 1 ट्रिलियन तक पहुँच सकती है, जिससे रणनीतिक आक्रामक क्षमताओं के निर्माण की तात्कालिक आवश्यकता उजागर होती है।
- **अत्याधुनिक साइबर सुरक्षा अवसंरचना में अपर्याप्त निवेश: भारत में AI-आधारित** खतरा पहचान, डेटा अखंडता के लिये ब्लॉकचेन और **नेक्स्ट-जेन फायरवॉल** जैसे अत्याधुनिक साइबर सुरक्षा तकनीकों में निवेश वैश्विक स्तर की तुलना में पीछे है।
    - **बजटीय बाधाओं और प्राथमिकता संबंधी मुद्दों** के कारण महत्त्वपूर्ण बुनियादी ढाँचे में सुधार के क्रियान्वयन में देरी होती है।

साइबर समुत्थानशीलता को बढ़ाने के लिये भारत क्या उपाय अपना सकता है?

- **एकीकृत थ्रेट फ्यूज़न के साथ संप्रभु साइबर सुरक्षा कमान: एक उच्च-शक्तिशाली, संप्रभु साइबर सुरक्षा कमान केंद्र** की स्थापना की जाए जो **CERT-In, I4C,** कंप्यूटर सुरक्षा प्रतिक्रिया दल, कानून प्रवर्तन और निजी क्षेत्र की संस्थाओं से खुफिया जानकारी के निर्बाध एकीकरण के लिये एक तंत्रिका केंद्र के रूप में कार्य करता है।
    - इस कमान को शत्रुओं को शीघ्रता से बेअसर करने के लिये **वास्तविक समय में खतरे के संयोजन, समन्वित सामरिक प्रतिक्रियाओं** और रणनीतिक साइबर निवारण नीतियों का लाभ उठाना चाहिये।
    - इस प्रकार की **केंद्रीकृत संरचना क्षेत्राधिकार संबंधी सीमाओं से परे जाकर** , तीव्र निर्णय लेने की क्षमता के साथ एक सुदृढ़ राष्ट्रीय साइबर रक्षा पारिस्थितिकी तंत्र का निर्माण करना चाहिये।
- **अनिवार्य क्षेत्र-विशिष्ट साइबर स्वच्छता: कठोर, उद्योग-अनुकूलित साइबर सुरक्षा अनुपालन अधिदेश** विकसित कर सकते है, जिसमें निरंतर जोखिम आकलन, प्रवेश परीक्षण और घटना रिपोर्टिंग तंत्र शामिल हों।
    - ये ढाँचे वैश्विक मानकों जैसे NIST के अनुरूप हों, लेकिन भारत के अनूठे खतरे परिदृश्य को ध्यान में रखते हुए तैयार किए जाएँ, विशेष रूप से **BFSI, स्वास्थ्य सेवा और महत्त्वपूर्ण बुनियादी ढाँचे** के क्षेत्रों के लिये।
    - अनुपालन स्तरों का **सार्वजनिक प्रकटीकरण पारदर्शिता**, हितधारक जवाबदेही को बढ़ावा दे सकता है तथा देश भर में आधारभूत साइबर स्वच्छता को बढ़ा सकता है।
- **राष्ट्रीय साइबर प्रतिभा संवर्धन पारिस्थितिकी तंत्र:** शैक्षणिक संस्थानों, उद्योग और सरकार के संसाधनों को मिलाकर एक व्यापक राष्ट्रीय साइबर कार्यबल विकास पहल को डिज़ाइन और लागू करना चाहिये।
    - साइबर सुरक्षा शिक्षा केवल **तकनीकी ज्ञान नहीं, बल्कि आलोचनात्मक सोच और समस्या-समाधान कौशल** के समग्र विकास को भी प्रोत्साहित करती है।
    - डिजिटल युग में, जहाँ बच्चों का जीवन स्क्रीन से जुड़ा हुआ है और साइबर अपराध बढ़ रहे हैं, **स्कूली पाठ्यक्रम में साइबर सुरक्षा** को शामिल करना अत्यंत आवश्यक है।
        - अंततः, साइबर सुरक्षा शिक्षा बच्चों की मानसिक लचीलापन बढ़ाने और उनके सामाजिक एवं संज्ञानात्मक विकास को मज़बूत करने में सहायक है।
- **AI-सक्षम सक्रिय साइबर खतरे की खोज में निवेश करना:** ऐसे अत्याधुनिक AI सिस्टम विकसित करना, जो विविध प्रकार के **थ्रेट डेटा को प्रोसेस कर पूर्वानुमानात्मक** खतरे की जानकारी उत्पन्न करें और अपने-आप नियंत्रण प्रोटोकॉल शुरू कर सकें।
    - गंभीर विसंगति पहचान (advanced anomaly detection) के लिये **डीप लर्निंग मॉडल** (जैसे RBI का Mulehunter.AI) का उपयोग करके, इन प्रणालियों को MTTD (खतरे की पहचान में लगने वाला समय) और MTTR (प्रतिक्रिया में लगने वाला समय) को घटाना चाहिये, जिससे **APTs और ज़ीरो-डे एक्सप्लॉइट्स** को बड़े स्तर पर रोका जा सके।
- **अखिल भारतीय साइबर साक्षरता अभियान चलाना:** सांस्कृतिक रूप से **संवेदनशील साइबर स्वच्छता अभियानों को क्षेत्रीय भाषाओं, लोककथाओं और डिजिटल प्रभावशाली व्यक्तियों** की मदद से संचालित करना चाहिये, ताकि साइबर जागरूकता को ज़मीनी स्तर तक गहराई से पहुँचाया जा सके।
    - ज़मीनी स्तर से आजीवन साइबर-लचीले व्यवहार को विकसित करने के लिये **गेमीफिकेशन, मोबाइल लर्निंग और स्कूल पाठ्यक्रम** एकीकरण को शामिल करना।
    - **RBI द्वारा पंचायतों के साथ सहयोग और साइबर धोखाधड़ी के बारे में फोन कॉल** पर अमिताभ बच्चन की स्वचालित चेतावनी जैसी पहलें समुदायों की रक्षा के लिये प्रभावशाली कदम हैं।
- **स्वदेशी साइबर सुरक्षा नवाचार को बढ़ावा देना: क्वांटम-सुरक्षित एन्क्रिप्शन, एआई-आधारित थ्रेट इंटेलिजेंस, सुरक्षित पहचान प्रबंधन के लिये ब्लॉकचेन और हार्डवेयर-आधारित सुरक्षा मॉड्यूल** जैसी अत्याधुनिक साइबर तकनीकों में अनुसंधान एवं विकास के लिये समर्पित नवाचार केंद्र और एक्सीलेरेटर स्थापित करना।
    - भारत को वैश्विक साइबर सुरक्षा नवाचार में अग्रणी बनाने के लिये सीमा पार अनुसंधान साझेदारी और ज्ञान के आदान-प्रदान को बढ़ावा देना तथा विदेशी प्रौद्योगिकी आयात पर निर्भरता को कम करना।
- **मल्टी-डोमेन साइबर संकट अनुकरण को संस्थागत बनाएँ:** नियमित रूप से बड़े पैमाने पर यथार्थवादी साइबर संकट सिमुलेशन का आयोजन करना, जिसमें **साइबर, भौतिक अवसंरचना, वित्तीय प्रणालियाँ और आपूर्ति शृंखलाएँ** शामिल हों।

- इन अभ्यासों में **सभी हितधारकों- सरकारी एजेंसियों, महत्त्वपूर्ण अवसंरचना संचालकों, फिनटेक फर्मों, दूरसंचार प्रदाताओं और नागरिक समाज**- को शामिल किया जाना चाहिये ताकि प्रणालीगत कमजोरियों की पहचान की जा सके, संकट संचार का परीक्षण किया जा सके तथा उच्च दबाव वाले परिदृश्यों के तहत समन्वित घटना प्रतिक्रिया रणनीतियों को परिष्कृत किया जा सके।

निष्कर्ष:

मार्क्स एंड स्पेंसर साइबर हमला इस बात पर प्रकाश डालता है कि **भारत को बढ़ते जटिल खतरों के बीच अपनी साइबर सुरक्षा स्थिति** को मजबूत करने की तत्काल आवश्यकता है। आगामी **डिजिटल इंडिया अधिनियम** साइबर अपराध पर बुडापेस्ट कन्वेंशन के आधार पर विनियमन, प्रवर्तन और साइबर समुत्थानशीलता को व्यापक रूप से बढ़ाने के उद्देश्य से एक आशावादी मार्ग प्रदान करता है।

दृष्टि मुख्य परीक्षा प्रश्न:

Q. "साइबर सुरक्षा खतरे तेजी से जटिल होते जा रहे हैं और भारत की डिजिटल अर्थव्यवस्था और राष्ट्रीय सुरक्षा के लिए एक बड़ी चुनौती बन रहे हैं। भारत की साइबर लचीलापन को मजबूत करने के उपायों पर चर्चा करें और सुझाव दें।"

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

??????????:

प्रश्न.1 भारत में व्यक्तियों के लिये साइबर बीमा के तहत धन की हानि और अन्य लाभों के भुगतान के अलावा, निम्नलिखित में से कौन से लाभ आम तौर पर 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 लागत अगर ऐसा साबित हो जाता है कि कुछ असामाजिक तत्त्वों ने जानबूझकर इसे नुकसान पहुँचाया है।
3. साइबर जबरन 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 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 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. निगमित निकाय

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