भारत की साइबर सुरक्षा

यह एडिटोरियल 13/08/2024 को 'द हिंदू' में प्रकाशित "Disinformation, AI and 'cyber chakravyuh'" लेख पर आधारित है। इसमें वर्ष 2024 में AI और साइबर हमलों के बढ़ते खतरे की चर्चा की गई है और इन उभरते डिजिटल खतरों से निपटने के लिये, विशेष रूप से लोकतांत्रिक देशों में, सतर्कता एवं समन्वित वैश्विक कार्रवाई की आवश्यकता पर बल दिया गया है। लेख में दैनिक जीवन में AI-सक्षम दुष्प्रचार और साइबर धोखाधड़ी के बढ़ते जोखिम को संबोधित करने के महत्त्व को भी रेखांकित किया गया है।

प्रिलिम्स के लिये:

डिजिटल खतरा, कृत्रिम बुद्धिमत्ता, डीप फेक, WannaCry रैनसमवेयर अटैक, फिशिंग, इंटरनेट ऑफ थिंग्स, राष्ट्रीय साइबर सुरक्षा नीति, भारतीय साइबर अपराध समन्वय केंद्र, कंप्यूटर आपातकालीन प्रतिक्रिया टीम - भारत, साइबर स्वच्छता केंद्र, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम 2023।

मेन्स के लिये:

भारत के समक्ष वर्तमान प्रमुख साइबर खतरे, भारत में साइबर सुरक्षा से संबंधित प्रमुख सरकारी पहल।

वर्ष 2024 में जैसे डिजिटल खतरों के एक नए युग का आरंभ हो गया है, जहाँ कृत्रिम बुद्धिमत्ता **(AI)** और इसके विभिन्न रूपों **(जैसे जनरेटिव AI और आर्टिफिशियल जनरल इंटेलिजेंस- AGI) से** संबद्ध सुरक्षा चिंताएँ सबसे प्रमुख हैं। **डिजिटल हमलों, दुष्प्रचार (disinformation) अभियानों** और साइबर खतरों की उच्च संभावना बनी हुई है। **माइक्रोसॉफ्ट विंडो सॉफ्टवेयर अपडेट** में एक 'ग्लिच' के कारण हाल ही में उत्पन्न हुआ वैश्विक व्यवधान हमारी परस्पर जुड़ी डिजिटल अवसंरचना में विद्यमान कमज़ोरियों की याद दिलाता है।

शेष विश्व की तरह भारत के लिये भी खतरे का यह परिदृश्य तेज़ी से आकार ग्रहण कर रहा है। AI-सक्षम 'डीप फेक' से लेकर महत्त्वपूर्ण अवसंरचना को निशाना बनाने वाले परिष्कृत साइबर हमलों तक, हमारे समक्ष बहुआयामी चुनौतियाँ मौजूद हैं और उनकी जटिलता में वृद्धि हो रही है। आम नागरिकों को प्रभावित करने वाली **साइबर धोखाधड़ी (जैसे फिशिंग', पहचान की चोरी, वित्तीय स्कैम** आदि) में वृद्धि लोगों में जागरूकता को बढ़ाने और सुदृढ़ साइबर सुरक्षा उपायों को अपनाने की आवश्यकता को रेखांकित करती है। इस नई डिजिटल वास्तविकता का सामना करने के लिये भारत में सार्वजनिक और निजी दोनों क्षेत्रों के लिये **साइबर सुरक्षा को प्राथमिकता देना, उन्नत सुरक्षात्मक उपायों में निवेश करना तथा राष्ट्रीय सुरक्षा एवं व्यक्तिगत निजता** की रक्षा के लिये डिजिटल सतर्कता की संस्कृति को बढ़ावा देना अनिवार्य हो गया है।

भारत के समक्ष विद्यमान प्रमुख साइबर खतरे:

- **रैनसमवेयर का प्रकोप (Ransomware Rampage):** भारत में हाल में रैनसमवेयर **हमलों** में वृद्धि देखी गई है, जहाँ स्वास्थ्य सेवा क्षेत्र विशेष रूप से असुरक्षित है।
  - **सिक्योरिटी सॉफ्टवेयर निर्माता कंपनी क्विक हील (Quick Heal)** ने बताया कि उसने भारत में **'WannaCry' रैनसमवेयर हमले के 48000** से अधिक मामलों का पता लगाया।
  - नवंबर 2022 में अखिल भारतीय आयुर्विज्ञान संस्थान (एम्स) दिल्ली पर साइबर हमले का मामला प्रकाश में आया।
    - भारतीय चिकित्सा अनुसंधान परिषद (ICMR) के सर्वर को हैक करने के कम से कम 6,000 प्रयास किये गए।
- **'फिशिंग पैराडॉक्स' (Phishing Paradox):** भारत में **वर्ष 2023 में 79 मिलियन से अधिक** फिशिंग हमले दर्ज किये गए। वित्तीय क्षेत्र को इसका खामियाजा भुगतना पड़ा, जो अधिकांश फिशिंग हमलों का शिकार हुआ।
  - इसके उदाहरणों में **भारतीय स्टेट बैंक के उपयोगकर्त्ताओं** को लक्षित करने वाले **फिशिंग अभियान शामिल** हैं, जहाँ धोखेबाज़ों ने लाखों ग्राहकों को नकली SMS संदेश भेजकर उनके बैंकिंग क्रेडेंशियल्स चुराने का प्रयास किया।
  - यह रुझान उपयोगकर्ता शिक्षा और उन्नत ईमेल सुरक्षा समाधान के महत्त्व को रेखांकित करता है।
- **क्लाउड की पहेली (Cloud Conundrum):** चूँकि भारत तेज़ी से क्लाउड प्रौद्योगिकियों को अपना रहा है, जहाँ वर्ष 2028 तक समग्र **भारतीय सार्वजनिक क्लाउड सेवा (PCS) बाज़ार** के 24.2 बिलियन अमेरिकी डॉलर तक पहुँचने की उम्मीद है**, क्लाउड संबंधी सुरक्षा खतरे** गंभीर चिंता का विषय बन गए हैं।
  - वर्ष 2023 में **एयर इंडिया पर एक गंभीर डेटा उल्लंघन हमले ने 4.5 मिलियन** यात्रियों के व्यक्तिगत डेटा को उजागर कर दिया। इस घटना के लिये **क्लाउड सेवा प्रदाता के सिस्टम** में कमज़ोरी को ज़िम्मेदार माना गया था।

- यह घटना **उओयुक्त कॉन्फगिरेशन, एक्सेस प्रबंधन और निरंतर नगिरानी** सहति सशक्त क्लाउड सुरक्षा रणनीतियों की आवश्यकता को उजागर करती है।
- **IoT पर आक्रमण:** भारत के IoT बाज़ार के वर्ष 2025 तक 9.28 बलियिन अमेरकिी डॉलर तक पहुँचने के अनुमान के साथ **इंटरनेट ऑफ थगि्स (IoT)** से संबंद्ध उपकरणों की सुरक्षा भी एक गंभीर महत्त्वपूर्ण मुद्दा बन गया है।
  - शोधकर्त्ताओं ने भारत भर में लगाए गए लाखों स्मार्ट मीटरों में एक कमज़ोरी का पता लगाया है, जसिसे हैकर्स को बजिली खपत के आँकड़ों में हेरफेर करने का अवसर प्राप्त हो सकता है।
  - इससे **उपभोक्ता और औद्योगकि व्यवस्था दोनों में ही IoT उपकरणों** के लयि कड़े सुरक्षा मानकों और नयिमति अद्यतन की आवश्यकता उजागर होती है।
- **आपूर्त शृंखला की घेराबंदी (Supply Chain Siege):** भारत की डजिटिल आपूर्त शृंखलाओं को वर्ष 2023 में अभूतपूर्व हमलों का सामना करना पड़ा, जहाँ सॉफ्टवेयर आपूर्त शृंखला से जुड़ी कमज़ोरयिों में बड़े पैमाने पर वृद्धि हुई।
  - वर्ष 2023 में आईटी सेवा दग्गिज कंपनी पर **सोलरवड्सि (SolarWinds)** जैसा हमला इसका प्रमुख उदाहरण है।
  - इस घटना ने **आपूर्त शृंखला हमलों (supply chain attacks)** के व्यापक प्रभाव को उजागर कयिा और भारतीय उद्योगों में वक्रिेता जोखमि प्रबंधन एवं सॉफ्टवेयर अखंडता सत्यापन प्रक्रयिाओं की आवश्यकता पर प्रकाश डाला।
- **क्रप्टिो अपराधों की लहर: 'ब्रॉडबैंड इंडयिा फोरम'** द्वारा प्रकाशति एक रपिोर्ट के अनुसार वर्ष **2021 में क्रप्टिोकरेंसी चोरी में लगभग 3.2 बलियिन डॉलर मूल्य की वृद्धि** हुई, जो वर्ष 2020 की तुलना में 516% की वृद्धि थी।
  - **कुख्यात वज़ीरएक्स क्रप्टिो हाइस्ट (WazirX Crypto Heist)** —जसिने वज़ीरएक्स की **45% क्रप्टिो परसिंपत्तयिों** को जोखमि में डाल दयिा, ने डजिटिल परसिंपत्त प्लेटफॉर्मों में गंभीर कमज़ोरयिों को उजागर कयिा।
  - इस प्रवृत्त को देखते हुए मज़बूत वनियिमन, **क्रप्टिो एक्सचेंजों के लयि उन्नत साइबर** सुरक्षा उपायों और सुरक्षति क्रप्टिो अभ्यासों के बारे में उपयोगकर्त्ता जागरूकता बढ़ाने की आवश्यकता है।
- **'डीपफेक डाइलेमा'** (Deepfake Dilemma): भारत में वर्ष 2023 में डीपफेक वीडयिो में 230% की वृद्धि देखी गई, जसिमें राजनीतकि भ्रामक सूचना अभयिान सबसे आगे रहे।
  - **वर्ष 2024 के चुनाव अभयिान के दौरान वाइरल** हुए एक डीपफेक वडियिो (जसिमें एक प्रमुख भारतीय नेता को भड़काऊ बयान देते हुए दखिाया गया) व्यापक सामाजकि अशांत का कारण बना।
  - यह घटना **डीपफेक डटिक्शन प्रौद्योगकियिों, सख्त कंटेंट मॉडरेशन नीतयिों और डजिटिल मीडयिा साक्षरता** के बारे में जन जागरूकता अभयिान की तत्काल आवश्यकता को उजागर करती है।
- **साइबर सुरक्षा पेशेवरों की कमी:** भारत को कुशल साइबर सुरक्षा पेशेवरों की भारी कमी का सामना करना पड़ रहा है, जसिसे भारतीय संगठन साइबर खतरों के प्रत असुरक्षति बने हुए हैं।
  - भारत में लगभग **8 लाख साइबर सुरक्षा पेशेवरों** की कमी है। वशिष रूप से AI और क्लाउड सुरक्षा जैसी उभरती प्रौद्योगकियिों में इनकी गंभीर कमी पाई जाती है।
  - वशिषज्ञता की यह कमी साइबर सुरक्षा उपायों और घटना प्रतक्रियिा क्षमताओं के कार्यान्वयन में बाधा उत्पन्न करती है, जसिसे यह भारत की समग्र साइबर सुरक्षा स्थति के लयि एक गंभीर खतरा बन जाता है।
- **'हनी ट्रैप' का खतरा: 'हनी ट्रैपगि'** भारत में एक महत्त्वपूर्ण साइबर खतरे के रूप में उभरा है, जो वशिष रूप से सरकारी अधकिारयिों, सैन्य कर्मयिों और हाई-प्रोफाइल व्यक्तयिों को नशिाना बनाता है।
  - धोखाधड़ी के इस अभ्यास में में आमतौर पर आकर्षक व्यक्तयिों के फर्जी सोशल मीडयिा प्रोफाइल बनाकर लक्षति व्यक्तयिों को समझौतापूर्ण स्थतियिों में फँसाने या संवेदनशील सूचना का खुलासा करने का प्रयास कयिा जाता है।
  - भारतीय सेना ने पाया कि वर्ष 2023 में पछिले वर्ष की तुलना में इसके कर्मयिों की हनी ट्रैपगि के प्रयासों में नाटकीय वृद्धि हुई।
  - वर्ष 2023 में **DRDO के एक वरषि्ठ तकनीकी अधकिारी** को भारत के मसिाइल परीक्षण के बारे में एक पाकस्तिानी खुफयिा ऑपरेटवि को सूचना देने के संदेह में हरिासत में लयिा गया था।

भारत में साइबर सुरक्षा से संबंधति प्रमुख सरकारी पहलें:

- **राष्ट्रीय साइबर सुरक्षा नीत (National Cyber Security Policy):** यह नीत साइबरस्पेस सूचना एवं अवसंरचना की रक्षा करने, **साइबर हमलों को रोकने एवं जवाबी** कार्रवाई के लयि क्षमताओं का नरि्माण करने और संस्थागत संरचनाओं, व्यक्तयिों, प्रक्रयिाओं एवं प्रौद्योगकिी के समन्वति प्रयासों के माध्यम से क्षत को न्यूनतम करने के लयि वभिन्नि उद्देश्यों एवं रणनीतियिों की रूपरेखा तैयार करता है।
- **भारतीय साइबर अपराध समन्वय केंद्र (Indian Cyber Crime Coordination Centre- I4C):** इस केंद्र की स्थापना **कानून प्रवर्तन एजेंसियिों** को व्यापक एवं समन्वति तरीके से साइबर अपराधों से नपिटने के लयि एक रूपरेखा एवं पारतिंत्र प्रदान करने के लयि की गई थी। इसके सात घटक हैं:
  - **नेशनल साइबरक्राइम थ्रेट एनालटिकि्स यूनटि (National Cybercrime Threat Analytics Unit)**
  - नेशनल साइबर क्राइम रपिोर्टगि पोर्टल (National Cyber Crime Reporting Portal)
  - संयुक्त साइबर अपराध जाँच दल के लयि मंच (Platform for Joint Cyber Crime Investigation Team)
  - राष्ट्रीय साइबर अपराध फोरेंसकि प्रयोगशाला पारस्थितिकिी तंत्र (National Cyber Crime Forensic Laboratory Ecosystem)
  - राष्ट्रीय साइबर क्राइम प्रशक्षिण केंद्र (National Cyber Crime Training Centre)
  - साइबर क्राइम इकोसस्टिम मैनेजमेंट यूनटि (Cyber Crime Ecosystem Management Unit)
  - राष्ट्रीय साइबर अनुसंधान और नवाचार केंद्र (National Cyber Research and Innovation Centre)
- **कंप्यूटर आपातकालीन प्रतक्रियिा दल - भारत (CERT-In):** यह **इलेक्ट्रॉनकिी एवं सूचना प्रौद्योगकिी मंत्रालय (MeitY)** के तहत कार्यरत संगठन है, जो साइबर घटनाओं पर सूचना संग्रहण, वश्लिेषण और प्रसारण के साथ-साथ साइबर सुरक्षा खतरों पर चेतावनी जारी करने के लयि ज़म्मिेदार है।
- **'साइबर सुरक्षति भारत' पहल:** साइबर अपराधों के बारे में जागरूकता बढ़ाने और सभी सरकारी वभिागों में **मुख्य सूचना सुरक्षा अधकिारयिों**

(CISOs) एवं अग्रमि पंक्ति के आईटी कर्मचारियों के लिये सुरक्षा उपायों का क्रियान्वयन करने के लिये इस पहल की शुरुआत की गई थी।

- साइबर सुवच्छता केंद्र **(बॉटनेट शोधन और मालवेयर वश्लिेषण केंद्र):** वर्ष 2017 में लॉन्च किये गए इस केंद्र का उद्देश्य भारत में बॉटनेट संक्रमणों का पता लगाकर और भविष्य के संक्रमणों को रोकने के लिये उपयोगकर्त्ताओं को अपने सिस्टिम का शोधन करने एवं उसे सुरक्षित बनाने के लिये सूचित कर एक सुरक्षित साइबरस्पेस का निर्माण करना है।
- **राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure Protection Centre-NCIIPC:** इसे बिजली, बैंकिंग, दूरसंचार, परिवहन, सरकार और रणनीतिक उद्यमों जैसे क्षेत्रों में महत्त्वपूर्ण सूचना अवसंरचना (CIC) की सुरक्षा के लिये स्थापित किया गया।
  - **DCyA में हैकिंग, निगिरानी, डेटा रिकिवरी, एन्क्रिप्शन और विभिन्न साइबर खतरों** के विरुद्ध जवाबी कार्रवाई सहित साइबर ऑपरेशन करने की क्षमता है।
- रक्षा साइबर एजेंसी **(Defence Cyber Agency- DCyA):** यह भारतीय सशस्त्र बलों की एक त्रि-सेवा कमान है जो साइबर सुरक्षा खतरों से निपटने के लिये ज़िम्मेदार है।
  - CII को ऐसे कंप्यूटर संसाधन के रूप में परिभाषित किया गया है, जिसके नष्ट होने से राष्ट्रीय सुरक्षा, अर्थव्यवस्था, सार्वजनिक स्वास्थ्य या सुरक्षा पर प्रतिकूल प्रभाव पड़ेगा।
- **डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम (Digital Personal Data Protection Act) 2023:** इस ऐतिहासिक विधान का उद्देश्य भारत में व्यक्तियों के डिजिटल व्यक्तिगत डेटा की सुरक्षा करना और ऐसे डेटा के **संग्रहण, भंडारण, प्रसंस्करण एवं साझाकरण को** विनियमित करना है।
  - **प्रमुख विशेषताएँ:**
    - अनुपालन प्रवर्तित करने के लिये भारतीय डेटा संरक्षण बोर्ड की स्थापना की गई
    - **डेटा संग्रहण और प्रसंस्करण** के लिये स्पष्ट सहमति की आवश्यकता है
    - डेटा फिड्यूशरीज़ (data fiduciaries) को उचित सुरक्षा उपाय लागू करने का आदेश दिया गया

भारत अपनी साइबर सुरक्षा को सुदृढ़ करने के लिये कौन-से उपाय कर सकता है?

- **साइबर फ्यूज़न सेंटर (Cyber Fusion Centers):** सार्वजनिक और निजी क्षेत्रों के बीच वास्तविक समय में खतरे की खुफिया सूचना साझा करने की सुविधा प्रदान करने के लिये क्षेत्रीय साइबर फ्यूज़न सेंटर स्थापित किये जाएँ।
  - पूर्वानुमानित खतरा विश्लेषण के लिये **उन्नत AI और मशीन लर्निंग प्रणालियों** को लागू किया जाए।
  - बड़ी साइबर घटनाओं से निपटने के लिये त्वरित तैनाती में सक्षम एक**केंद्रीकृत घटना प्रतिक्रिया दल (centralized incident response team)** का गठन किया जाए।
  - समन्वय का परीक्षण करने और उसे बेहतर बनाने के लिये विभिन्न हितधारकों को संलग्न करते हुए नियमित रूप से संयुक्त**साइबर अभ्यास** आयोजित किये जाएँ।
- **डिजिटल साक्षरता अभियान:** साइबर सुरक्षा जागरूकता पर ध्यान केंद्रित करने के साथ जनसांख्यिकी के सभी वर्गों को लक्षित करते हुए एक राष्ट्रव्यापी डिजिटल साक्षरता अभियान शुरू किया जाए।
  - **साइबर सुरक्षा शिक्षा** को माध्यमिक से लेकर उच्च शिक्षा स्तर तक स्कूल पाठ्यक्रम में एकीकृत किया जाए।
  - नागरिकों को रियल-टाइम साइबर सुरक्षा संबंधी सुझाव और खतरे की चेतावनी देने के लिये एक मोबाइल ऐप विकसित किया जाए।
  - **स्थानीय भाषाओं और प्रासंगिक परिदृश्यों** का उपयोग करते हुए ग्रामीण क्षेत्रों में नियमित रूप से साइबर स्वच्छता कार्यशालाएँ आयोजित की जाएँ।
  - युवाओं में साइबर सुरक्षा के प्रति जागरूकता के प्रसार के लिये सोशल मीडिया इन्फ्लुएंसर्स के साथ साझेदारी का निर्माण करें।
- **वर्तमान डेटा संरक्षण ढाँचे को सुदृढ़ करना:** भारत को व्यक्तिगत डेटा के **AI संचालित** उल्लंघनों को विनियमित करने, उल्लंघनों के लिये कठोर दंड आरोपित करने और कठोर कार्यान्वयन एवं संवीक्षा लागू करने के प्रावधानों को शामिल करने के माध्यम से मौजूदा**डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम 2023** को सुदृढ़ बनाना चाहिये।
  - वर्तमान अधिनियम के दायरे एवं क्षमता को बढ़ाकर विधायी प्रयासों के दुहराव के बिना नवीन उभरते खतरों का समाधान किया जा सकेगा।
- **सक्रियोर-बाय-डिज़ाइन पहल (Secure-by-Design Initiative):** विभिन्न उद्योगों में सॉफ्टवेयर एवं हार्डवेयर विकास में 'सक्रियोर-बाय-डिज़ाइन' दृष्टिकोण को बढ़ावा दिया जाए।
  - सुरक्षा मानकों का पालन सुनिश्चित करने के लिये एक राष्ट्रीय साइबर सुरक्षा उत्पाद प्रमाणन कार्यक्रम (national cybersecurity product certification program) स्थापित किया जाए।
  - साइबर सुरक्षा समाधान विकसित करने पर ध्यान केंद्रित करने वाले स्टार्टअप्स के लिये अनुदान और वित्तपोषण की पेशकश की जाए।
  - भविष्य के खतरों से निपटने के लिये तैयारी हेतु क्वांटम-प्रतिरोधी क्रिप्टोग्राफी के लिये एक समर्पित अनुसंधान एवं विकास निधि का गठन किया जाए।
- **AI-संचालित साइबर सुरक्षा:** भारत के अपने विशिष्ट खतरा परिदृश्य के अनुरूप AI-संचालित साइबर सुरक्षा समाधान विकसित करने में निवेश किया जाए।
  - **नेटवर्क ट्रैफिक और उपयोगकर्त्ता** व्यवहार में विसंगति का पता लगाने के लिये मशीन लर्निंग एल्गोरिदम को लागू किया जाए।
  - उभरते साइबर खतरों की सक्रिय रूप से पहचान करने और उन्हें प्रभावहीन करने के लिये AI-संचालित खतरा निवारण क्षमताओं का विकास किया जाए।
- **आपूर्ति शृंखला का सुदृढ़ीकरण:** हार्डवेयर और सॉफ्टवेयर खरीद दोनों के लिये एक व्यापक आपूर्ति शृंखला जोखिम प्रबंधन ढाँचे को लागू किया जाए।
  - थर्ड-पार्टी विक्रेताओं और सेवा प्रदाताओं का नियमित सुरक्षा मूल्यांकन किया जाए।
  - विश्वसनीय आपूर्तिकर्त्ताओं का एक **राष्ट्रीय डाटाबेस विकसित** किया जाए और सरकारी एवं अन्य महत्त्वपूर्ण क्षेत्रों की खरीद में इसके उपयोग को अनिवार्य बनाया जाए।

- डिजिटल आपूर्ति शृंखलाओं में बेहतर पता **लगाने की क्षमता (traceability)** और **अखंडता (integrity)** के लिये ब्लॉकचेन प्रौद्योगिकी का प्रयोग किया जाए।
- **क्लाउड सुरक्षा – भारत के डिजिटल स्पेस को सुरक्षित करना:** सभी क्लाउड सेवा प्रदाताओं के लिये कठोर अनुपालन आवश्यकताओं के साथ एक राष्ट्रीय क्लाउड सुरक्षा ढाँचा स्थापित किया जाए।
  - क्लाउड में संग्रहित सभी डेटा के लिये अनिवार्य एन्क्रिप्शन लागू किया जाए, ताकि वैसी कमज़ोरियों को दूर किया जा सके जो एयर इंडिया डेटा उल्लंघन मामले में उजागर हुई थीं।
  - सार्वजनिक क्लाउड सेवाओं में खतरों की निगरानी करने और उन पर प्रतिक्रिया देने के लिये एक **क्लाउड सुरक्षा परिचालन केंद्र (Cloud Security Operations Center)** का सृजन किया जाए।
- **डीपफेक से रक्षा:** भारत में संचालित सभी प्रमुख सोशल मीडिया प्लेटफॉर्मों के लिये सख्त कंटेंट सत्यापन प्रोटोकॉल लागू किया जाए।
  - चुनाव जैसे महत्त्वपूर्ण समय के दौरान वायरल डीपफेक की समस्या से निपटने के लिये एक त्वरित प्रतिक्रिया दल का गठन किया जाए।
  - डीपफेक की पहचान करने और उसकी रिपोर्ट करने के लिये एक जन जागरूकता अभियान शुरू किया जाए।
- **साइबर योद्धा पहल (Cyber Warrior Initiative):** भारत को साइबर सुरक्षा पेशेवरों की गंभीर कमी को दूर करने के लिये एक व्यापक 'साइबर योद्धा पहल' शुरू करनी चाहिये।
  - इस कार्यक्रम में विश्वविद्यालयों के साथ साझेदारी के माध्यम से विशिष्ट साइबर सुरक्षा पाठ्यक्रम विकसित करना, **राष्ट्रीय साइबर सुरक्षा छात्रवृत्ति कार्यक्रम** की स्थापना करना और साइबर रिज़र्व बल का गठन करना शामिल हो सकता है।
  - राष्ट्रीय प्रमाणन कार्यक्रम लागू करने तथा कर्मचारी साइबर सुरक्षा प्रशिक्षण में निवेश करने वाली कंपनियों को कर प्रोत्साहन प्रदान करने से कार्यबल को और मज़बूती मिलेगी।

अभ्यास प्रश्न: भारत के साइबर सुरक्षा परिदृश्य में विद्यमान प्रमुख चुनौतियों की चर्चा कीजिये और इन खतरों से निपटने में मौजूदा उपायों की प्रभावशीलता का मूल्यांकन कीजिये। उभरते डिजिटल खतरों का मुक़ाबला करने के लिये भारत के साइबर सुरक्षा ढाँचे को सुदृढ़ करने के संबंध में आवश्यक रणनीतियों के सुझाव दीजिये।

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 रिपोर्ट करना निम्नलिखित में से किसके/किनके लिये विधितः अधिदेशात्मक है? (2017)

1. सेवा प्रदाता
2. डेटा सेंटर
3. कॉर्पोरेट 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 वभिन्नि तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतियों को ध्यान में रखते हुए समीक्षा कीजयि कि भारत ने कसि हद तक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक वकिसति की है। (2022)