महामारी के दौर में बढ़ता साइबर अपराध

(प्रारंभिक परीक्षा : राष्ट्रीय एवं अंतरराष्ट्रीय सामयिक घटनाएँ)
(मुख्य परीक्षा: सामान्य अध्ययन प्रश्नपत्र 3 - आंतरिक सुरक्षा के लिये चुनौती उत्पन्न करने वाले शासन विरोधी तत्वों की भूमिका, संचार नेटवर्क के माध्यम से आंतरिक सुरक्षा को चुनौती से संबंधित मुद्दे)

संदर्भ

- हाल ही में जारी 'नॉर्टन साइबर सेफ्टी इनसाइट्स रिपोर्ट, 2021' से पता चलता है कि ऑनलाइन धोखाधड़ी के मामलों में विगत वर्ष की अपेक्षा वृद्धि हुई है।
- **कोविड-19 महामारी** में लोग जहाँ एक तरफ महामारी से लड़ने का प्रयास कर रहे हैं, वहीं दूसरी तरफ साइबर धोखाधड़ी के मामलों में निरंतर वृद्धि लोगों पर दोहरी मार का कारण बन रहा है।

रिपोर्ट के प्रमुख बिंदु

- इस रिपोर्ट के अनुसार, फरवरी 2020 से 2021 के मध्य लगभग 120 मिलियन लोगों ने साइबर अपराध का सामना किया है।
- इसके अनुसार वर्ष 2021 में साइबर अपराधों में बढ़ोतरी दर्ज की जाएगी, जिसका कारण लोगों द्वारा घर से काम करना बताया गया है।
- महामारी के कारण लोगों द्वारा ऑनलाइन माध्यम से की जा रही वस्तुओं की खरीददारी साइबर अपराध का अवसर प्रदान कर रहा है।
- ग्रामीण क्षेत्रों के लोगों द्वारा भी मोबाइल बैंकिंग के माध्यम से लेन- देन की प्रवृत्ति बढ़ी है, हालाँकि इनमें साइबर अपराधों से संबंधित जागरूकता का अभाव है।
- इस रिपोर्ट के अनुसार पिछले 12 महीनों में लगभग 59 प्रतिशत भारतीय वयस्क साइबर अपराध के शिकार बने। साथ ही, भारत में लगभग 52 प्रतिशत वयस्क इस बात से अनभिज्ञ हैं कि साइबर अपराध से स्वयं को कैसे बचाया जाए।
- रिपोर्ट में बताया गया कि वर्ष 2020 में लगभग 45% वयस्क भारतीयों को इंटरनेट पर अपनी पहचान के चोरी होने का सामना करना पड़ा।
- इस रिपोर्ट का मानना है कि साइबर अपराध के शिकार लोगों ने इन समस्याओं के समाधान हेतु सामूहिक रूप से 1.3 बिलियन घंटे इंटरनेट पर व्यतीत किये।

- अधिकांश भारतीय उपभोक्ताओं (लगभग 90 प्रतिशत) द्वारा अपनी डेटा की सुरक्षा हेतु सक्रिय प्रयास किये जा रहे हैं, फिर भी लगभग 42 प्रतिशत लोगों को गोपनीयता की रक्षा करना असंभव प्रतीत होता है।

साइबर सुरक्षा की प्रमुख चुनौतियाँ

- साइबर जागरूकता का अभाव।
- सख़्त कानूनों व केंद्रीकृत व्यवस्था का अभाव।
- संस्थाओं में प्रभावी समन्वय की कमी।
- उत्तरदायित्व एवं कार्यक्षेत्र में अतिव्यापन व अस्पष्टता।
- सूचना प्रौद्योगिकी अधिनियम के अनावश्यक प्रावधानों में संशोधन।
- स्पष्ट जवाबदेहिता का अभाव।
- महिलाओं के खिलाफ बढ़ते साइबर अपराध।
- साइबर कुशल कर्मचारियों का अभाव।
- 'निजता बनाम निगरानी' का मुद्दा।
- साइबर सशक्त देशों द्वारा किये जाने वाले साइबर हमले।

वर्तमान में साइबर धोखाधड़ी के मामले

- कोविड-19 मामलों की संख्या में लगातार वृद्धि होती जा रही है तथा प्रयोगशालाएँ परीक्षणों की माँग को पूरा करने में असमर्थ हैं। इसी का लाभ उठाकर साइबर अपराधी धोखाधड़ी को अंजाम दे रहे हैं।
- सरकार के द्वारा कोविड-19 के टीकाकरण के लिए Co-Win नामक एक प्लेटफॉर्म बनाया गया है, जिस पर लोगों द्वारा पंजीकरण करना अनिवार्य है।
- अपराधियों द्वारा फर्जी एप के माध्यम से टीकाकरण हेतु एडवांस बुकिंग, नकली दवाओं की बिक्री, फर्जी सरकारी अधिकारी बनकर लोगों की व्यक्तिगत जानकारी की चोरी, जरूरतमंदों के नाम पर ऑनलाइन धोखाधड़ी इत्यादि को अंजाम दिया जा रहा है।
- इसके अलावाँ, अपराधियों द्वारा लोगों के फेसबुक या ट्विटर अकाउंट हैक कर धोखाधड़ी किया जा रहा है।

भारत की संस्थागत साइबर सुरक्षा अवसंरचनाएँ

पिछले दो दशकों से भारत में साइबर सुरक्षा की बढ़ती चुनौतियों से निपटने के लिये विभिन्न संस्थानों की स्थापना की गई है। इनमें से कुछ प्रमुख निम्नलिखित हैं :

- सूचना प्रौद्योगिकी मंत्रालय (MEITY) के अंतर्गत वर्ष 2004 में भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (Indian Computer Emergency Response Team - CERT-In) की स्थापना की गई।

- वर्ष 2014 में ऊर्जा, वित्त, दूरसंचार, परिवहन आदि से जुड़ी महत्त्वपूर्ण अवसंरचनाओं की सुरक्षा हेतु एक नोडल एजेंसी के रूप में 'राष्ट्रीय अतिसंवेदनशील सूचना अवसंरचना संरक्षण केंद्र' (National Critical Information Infrastructure– NCIIPC) की स्थापना की गई। इसकी स्थापना राष्ट्रीय तकनीकी अनुसंधान संगठन (National Technical Research Organization - NTRO) के अधीन सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा-70 के तहत की गई है।
- प्रधानमंत्री को साइबर सुरक्षा से जुड़े महत्त्वपूर्ण रणनीतिक मुद्दों पर सलाह देने के लिये वर्ष 2013-14 में 'राष्ट्रीय साइबर सुरक्षा समन्वय केंद्र' (NCCC) की स्थापना की गई।
- भारतीय साइबर नीति परितंत्र के विकास में राष्ट्रीय सुरक्षा परिषद् की महत्त्वपूर्ण भूमिका है।इसकी अध्यक्षता राष्ट्रीय सुरक्षा सलाहकार करते हैं।
- ध्यातव्य है कि राष्ट्रीय सूचना बोर्ड, साइबर सुरक्षा एवं नीति निर्माण संबंधी अंतर मंत्रालयी समायोजन हेतु शीर्ष निकाय है। इसके अध्यक्ष भी राष्ट्रीय सुरक्षा सलाहकार होते हैं।
- वर्ष 2018 में साइबर जागरूकता व नई तकनीकों से जुड़े शोध एवं विकास कार्यों के संचालन के लिये गृह मंत्रालय के अधीन 'भारतीय साइबर अपराध समन्वय केंद्र' (Indian Cybercrime Coordination Centre) की स्थापना की गई।
- साइबर अपराधों के प्रति जागरूकता बढ़ाने तथा क्षमता विकास हेतु सूचना प्रोद्योगिकी मंत्रालय द्वारा 1 जनवरी, 2018 को 'साइबर सुरक्षित भारत पहल' की शुरुआत की गई।
- वर्ष 2018-19 में डिफेंस साइबर एजेंसी (रक्षा मंत्रालय के अधीन) को एकीकृत कमान एवं संयुक्त साइबर ऑपरेशन हेतु पुनर्गठित किया गया।
- साइबर सुरक्षा से जुड़े अंतर्राष्ट्रीय सहयोग एवं नीति निर्माण के लिये विदेश मंत्रालय भी लगातार प्रयासरत रहा है।

भारतीय साइबर अपराध समन्वय केंद्र

- वर्ष 2020 में गृह मंत्रालय द्वारा साइबर अपराध से निपटने के लिये 'भारतीय साइबर अपराध समन्वय केंद्र' (Indian Cyber Crime Coordination Centre-I4C) का शुभारंभ किया गया।

- इस योजना को संपूर्ण भारत में लागू किया गया है। साइबर अपराध से बेहतर तरीके से निपटने के लिये तथा I4C को समन्वित और प्रभावी तरीके से लागू करने के लिए इस योजना को 7 प्रमुख घटकों में बाँटा गया है-
    - राष्ट्रीय साइबर अनुसंधान और नवाचार केंद्र (National Cyber Research and Innovation Centre)
    - नेशनल साइबर अपराध रिपोर्टिंग पोर्टल (National Cyber Crime Reporting Portal)
    - साइबर क्राइम इकोसिस्टम मैनेजमेंट यूनिट (Cyber Crime Ecosystem Management Unit)
    - संयुक्त साइबर अपराध जाँच दल के लिये मंच (Platform for Joint Cyber Crime Investigation Team)
    - राष्ट्रीय साइबर अपराध प्रशिक्षण केंद्र (National Cyber Crime Training Centre)
    - नेशनल साइबरक्राइम थ्रेट एनालिटिक्स यूनिट (National Cybercrime Threat Analytics Unit)
    - राष्ट्रीय साइबर अपराध फोरेंसिक प्रयोगशाला पारिस्थितिकी तंत्र (National Cyber Crime Forensic Laboratory Eco-system)

सुझाव

- कोरोना के परीक्षण के लिए विश्वनीय एवं मान्यता प्राप्त संस्थान का चयन करना।
- किसी भी एप को डाउनलोड करते समय जानकारी संबंधी सुरक्षा सुनिश्चित करना।
- किसी लिंक पर क्लिक करने से पहले लिंक और ईमेल की जाँच करना। URL या ईमेल पते में गलत शब्द या यादृच्छिक अक्षर और संख्या भी एक धोखाधड़ी का संकेत दे सकते हैं।
- अपने खातों को द्विकारक प्रमाणीकरण से सुरक्षित करना। मोबाइल नंबर, जन्म तिथि व अन्य गोपनीय सूचनाओं को ऑनलाइन प्लेटफॉर्म पर डालने से बचना।
- इसके अतिरिक्त, भारत में एक पारदर्शी, सशक्त व सुस्पष्ट साइबर रणनीति की आवश्यकता है, ताकि साइबर अपराधियों के विरुद्ध प्रतिरक्षा तंत्र को मज़बूत किया जा सके।
- केंद्र व राज्य सरकारों के बीच समन्वय बढ़ाया जाए व अंतर्राष्ट्रीय स्तर पर भारत को सॉफ्ट पॉवर के रूप में स्थापित करने के लिये क्षमता विकास पर ध्यान दिया जाए।
- साइबर सक्षम देशों द्वारा लगातार किये जाने वाले साइबर हमलों के खिलाफ जागरूकता बढ़ाने के साथ-साथ इनके खिलाफ अंतर्राष्ट्रीय स्तर पर उचित विनियमन की आवश्यकता है।
- साइबर सुरक्षा में सुधार के लिये कृत्रिम बुद्धिमता तथा रोबोटिक्स का लाभ उठाने के लिये नवाचारी व्यावसायिक पारिस्थितिकी तंत्र का निर्माण किया जाना चाहिये।
- साइबर सुरक्षा क्षेत्र के लिये पर्याप्त मानव संसाधन की आपूर्ति हेतु प्रशिक्षण और कौशल कार्यक्रम शुरू किये जाएँ।

- भारत में साइबर सुरक्षा क्षेत्र हेतु पृथक रूप से बजट आवंटित कर अनुसंधान एवं विकास कार्यक्रमों को प्रोत्साहित किया जाए।

नॉर्टन लाइफ लॉक (NortonLifeLock)

स्थापना- वर्ष 1982 (सिमेंटेक कॉर्पोरेशन - 1982 - 2019)

संस्थापक- गैरी हेंड्रिक्स

मुख्यालय- टेम्पे, एरिजोना अमेरिका

कार्य- साइबर सुरक्षा सॉफ्टवेयर बनाना

विकास केंद्र (Devlopment center)- भारत में पुणे, बेंगलुरु और चेन्नई

इस संस्था द्वारा 'नॉर्टन साइबर सेफ्टी इनसाइट्स रिपोर्ट' का वार्षिक प्रकाशन किया जाता है।

Covid19