साइबर हमलों से रक्षा हेतु एन.आई.सी.-सी.ई.आर.टी. केंद्र की उपयोगिता

चर्चा में क्यों?

इलेक्ट्रॉनिक्स एवं सूचना प्रौद्योगिकी मंत्रालय द्वारा 11 दिसंबर, 2017 को राष्ट्रीय सूचना विज्ञान केंद्र के तहत "एनआईसी-सीईआरटी" केंद्र का उद्घाटन किया गया। इस केंद्र के उद्घाटन के साथ-साथ मंत्रालय द्वारा 'डिजिटल भारत' पहल के तहत अन्य कई सेवाओं को भी ऑनलाइन किया गया।

डिज़िटल लॉकर

- भारत को डिज़िटल अर्थव्यवस्था बनाने के लिये सरकार एक कार्यक्रम पर कार्य कर रही है। इसके लिये डिज़िटल लॉकर से लेकर विमुद्रीकरण जैसे कई कदम उठाए गए हैं।
- डिज़िटल अर्थव्यवस्था के बनने से आर्थिक विकास में नई लहर आने की संभावना है, जिससे विभिन्न क्षेत्रों में निवेश में वृद्धि होगी तथा रोज़गार के नए अवसर पैदा होंगे।
- यह डिज़िटल इंडिया कार्यक्रम का एक अहम् हिस्सा है। यह दस्तावेज़ों की छायाप्रति सुरक्षित रखने के काम आती है।
- भारत सरकार के सूचना एवं प्रौद्योगिकी मंत्रालय द्वारा प्रबंधित इस वेबसाइट आधारित सेवा के ज़रिये उपयोगकर्त्ता अपने दस्तावेज़ों को ऑनलाइन सुरक्षित रख सकते हैं।

वर्तमान स्थिति

- इंटरनेट तथा कंप्यूटर नेटवर्क के बढ़ते प्रयोग के कारण भारत की साइबर हमलों के प्रति सुभेद्यता में वृद्धि हुई है।
- ASSOCHAM के एक अध्ययन के अनुसार, भारत में वर्ष 2011 से वर्ष 2014 तक पंजीकृत साइबर अपराध मामलों में 350 प्रतिशत की वृद्धि हुई है।
- हाल ही में साइबर हमलों में तेज़ी आई है, जिससे डाटा चोरी होने की चिंताएँ बढ़ गई हैं। इसी समस्या के संदर्भ में सरकार डाटा संरक्षण अधिनियम का मसौदा तैयार कर रही है।
- स्पष्ट है कि तकनीकी रूप से अधिक समृद्ध न होने के कारण भारत में साइबर सुरक्षा के उल्लंघन की संभावनाएँ बहुत प्रबल हैं।
- ऐसे में विदेशी कंपनियों के अनुसार अपनी साइबर सुरक्षा को व्यवस्थित करना, इस समस्या का उचित समाधान प्रतीत नहीं होता है।
- इसका एक अन्य कारण यह है कि डाटा सुरक्षा के संबंध में किसी भी कानून का उल्लंघन करने पर भारतीय कानून के तहत उक्त कंपनी के संबंध में कार्यवाही की जा सकती है, परंतु ऐसा विदेशी कंपनियों के संबंध में संभव नहीं है।
- वस्तुतः विदेशी कंपनियों की प्रमुख प्राथमिकता व्यवसाय करना एवं मुनाफा कमाना होता है। ऐसे में आप उनसे यह उम्मीद नहीं कर सकते कि वे भारत की संप्रभुता को ध्यान में रखते हुए कार्य करेंगी।

चिंताएँ

- भारत में महत्त्वपूर्ण जानकारी प्रदान करने से संबंधित बुनियादी ढाँचे के लिये सुरक्षा उपायों की पहचान नहीं की गई है।
- "राष्ट्रीय साइबर सुरक्षा समन्वयक" के अंतर्गत अब तक राज्यों में संपर्क अधिकारियों की नियुक्ति नहीं की गई है।
- कंप्यूटर इमरजेंसी रिस्पाँस टीम (CERT-In) भी कर्मचारियों की कमी से जूझ रही है।
- निजी क्षेत्र ने भी डिजिटल नेटवर्कों में सेंध के मामलों में प्रतिक्रिया देने अथवा रिपोर्ट करने में रुचि नहीं दिखाई है। अतः ऐसे अधिकांश मामले दर्ज़ ही नहीं होते हैं। भारत में साइबर सुरक्षा को कम महत्त्व दिया जाता है।
- एक अनुमान के अनुसार वर्तमान में भारत में साइबर हमले से 25000 करोड़ रुपए से अधिक का नुकसान हो रहा है।
- साइबर हमले के दौरान नुकसान कई कारणों से होता है, जैसे- व्यवसाय के संचालन में व्यवधान आने से, संवेदनशील सूचनाओं एवं डिज़ाइनों के खो जाने से, ब्रांड की छवि खराब होने से तथा कानूनी दावों एवं बीमा प्रीमियमों के बढ़ने से।
- जिस तरह से भारत में व्यवसायों का आपस में जुड़ाव होता जा रहा है, उससे यह अनुमान लगाया जा सकता है कि भविष्य में इन समस्याओं में और वृद्धि होगी तथा आने वाले समय में यह आँकड़ा $20 बिलियन तक पहुँच सकता है।
- कारोबारी जगत साइबर सुरक्षा को रणनीतिक एजेंडा मानने के बजाय एक छोटी-मोटी घटना मानकर चलता है।
- ठीक इसी प्रकार डिज़िटल अर्थव्यवस्था की अपनी चुनौतियाँ भी हैं। डिज़िटल अर्थव्यवस्था के बनने से बड़ी मात्रा में ग्राहकों एवं नागरिकों के डाटा को डिज़िटल रूप में रखने की आवश्यकता पड़ेगी तथा बड़ी मात्रा में ऑनलाइन विनिमय भी होंगे, जिसके कारण भारत साइबर अपराधियों एवं हैकरों का बड़ा लक्ष्य बन सकता है। इसलिये इस चुनौती से निपटने के लिये विभिन्न दावेदारों को अपनी तैयारी बेहतर बनानी होगी।

भारत सरकार द्वारा उठाए गए कदम

- देश में साइबर अपराध का अवलोकन, राष्ट्रीय नगिरानी और चेतावनी जारी करने के लयि कंप्यूटर इमरजेंसी रस्पिाँस टीम (CERT-In) 24 × 7 कार्य पर रही है।
- सरकार ने राष्ट्रीय साइबर सुरक्षा नीति, 2013 जारी की, जसिके अंतर्गत साइबर क्षेत्र के महत्त्वपूर्ण बुनयिादी ढाँचे की सुरक्षा के लयि राष्ट्रीय अतसिंवेदनशील सूचना अवसंरचना संरक्षण केंद्र (National Critical Information Infrastructure Protection Centre: NCIIPC) का गठन कयिा।
- सूचना सुरक्षा के लयि मानव संसाधन वकिसति करने के लयि सरकार ने सूचना, सुरक्षा और जागरूकता (Information Security Education and Awareness: ISEA) परयिोजना प्रारंभ की है।
- भारत सूचना साझा करने तथा साइबर सुरक्षा पर सर्वोत्तम कार्यप्रणाली अपनाने के लयि अमेरकिा, ब्रटिेन और चीन जैसे देशों के साथ समन्वय कर रहा है। इसके अलावा भारत सरकार सुरक्षा पर बुडापेस्ट अभसिमय को स्वीकार करने पर वचिार कर रही है।