क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर

प्रिलिम्स के लिये:

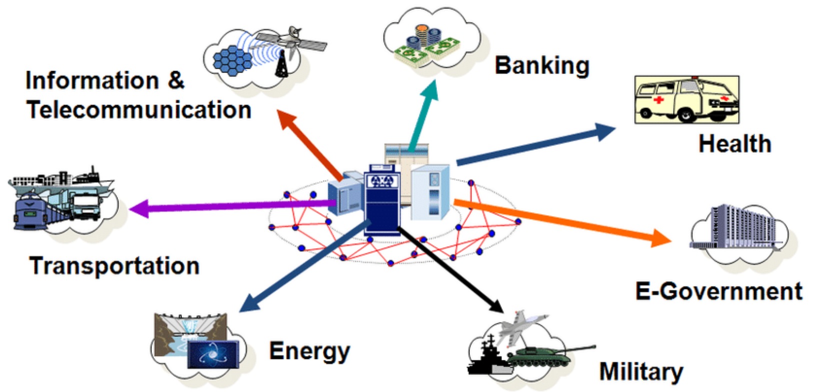
क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर, साइबर अटैक, एनपीसीआई, आईटी अधिनियम 2000

मेन्स के लिये:

क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर, साइबर सुरक्षा, साइबर युद्ध और साइबर कल्याण

चर्चा में क्यों?

हाल ही में केंद्रीय इलेक्ट्रॉनिक्स और आईटी मंत्रालय (MeitY) ने आईसीआईसीआई बैंक, एचडीएफसी बैंक और भारतीय राष्ट्रीय भुगतान निगम (NPCI) के सूचना प्रौद्योगिकी (IT) संसाधनों को 'महत्त्वपूर्ण सूचना अवसंरचना/क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर '(Critical Information Infrastructure- CII) के रूप में घोषित किया है।



//

प्रमुख बिंदु

क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर:

- सूचना प्रौद्योगिकी अधिनियम, 2000 महत्त्वपूर्ण सूचना अवसंरचना को एक कंप्यूटर संसाधन के रूप में परिभाषित करता है, जिसकी अक्षमता या विनाश का राष्ट्रीय सुरक्षा, अर्थव्यवस्था, सार्वजनिक स्वास्थ्य या सुरक्षा पर दुर्बल प्रभाव पड़ेगा।
- सरकार, 2000 के आईटी अधिनियम के तहत, उस डिजिटल संपत्ति की रक्षा के लिये किसी भी डेटा, डेटाबेस, आईटी नेटवर्क या संचार बुनियादी ढाँचे को CII के रूप में घोषित करने की शक्ति रखती है।
- कोई भी व्यक्ति जो कानून के उल्लंघन में किसी संरक्षित प्रणाली तक पहुँच सुरक्षित करता है या सुरक्षित होने का प्रयास करता है, उसे 10 साल तक की जेल की सजा हो सकती है।

CII के वर्गीकरण और संरक्षण की आवश्यकता:

- **वैश्विक अभ्यास:** दुनिया भर की सरकारें अपने महत्त्वपूर्ण सूचना बुनियादी ढाँचे की रक्षा के लिये तत्परता से आगे बढ़ रही हैं।
- **अनगिनत अतिमहत्त्वपूर्ण अभियानों की रीढ़:** आईटी संसाधन, देश के बुनियादी ढाँचे में अनगिनत महत्त्वपूर्ण संचालन की रीढ़ हैं और उनकी परस्परता को देखते हुए, व्यवधानों का सभी क्षेत्रों में व्यापक प्रभाव हो सकता है।

- **आईटी की विफलता अन्य क्षेत्रों के लिये प्रतिकूल:** पावर ग्रिड में सूचना प्रौद्योगिकी की विफलता के कारण स्वास्थ्य सेवा, बैंकिंग सेवाओं आदि जैसे अन्य क्षेत्रों में लंबे समय तक व्यवधान हो सकता है।
    - **उदाहरण: एस्टोनिया में सेवा बाधित करने वाले हमलों की शृंखला:** वर्ष 2007 में कथित रूप से रूसी IP एड्रेस द्वारा हमलों की एक शृंखला, प्रमुख एस्टोनियाई बैंकों, सरकारी निकायों - मंत्रालयों और संसद, और मीडिया आउटलेट्स को प्रभावित किया गया। यह उस तरह की साइबर आक्रामकता थी जिसे दुनिया ने पहले नहीं देखा था। हमलों ने लगभग तीन सप्ताह तक दुनिया के सबसे अधिक नेटवर्क वाले देशों में से एक में तबाही मचाई।
    - डिनायल-ऑफ-सर्विस (DoS) हमला एक मशीन या नेटवर्क को बंद करने के लिये किया गया हमला है, जिससे यह अपने इच्छित उपयोगकर्त्ताओं के लिये दुर्गम हो जाता है।
- **भारत के मामले:**
    - अक्तूबर, 2020 में जब भारत महामारी से जूझ रहा था, मुंबई की बिजली ग्रिड की आपूर्ति अचानक बंद हो गई, जिससे बड़े शहर के अस्पतालों, ट्रेनों और व्यवसायों पर असर पड़ा।
    - बाद में, एक अमेरिकी फर्म द्वारा किए गए एक अध्ययन में दावा किया गया कि यह बिजली कटौती एक साइबर हमला हो सकता है, जो कथित तौर पर चीन से जुड़े समूह से महत्वपूर्ण बुनियादी ढाँचे के उद्देश्य से किया गया था। हालाँकि, सरकार ने मुंबई में किसी भी साइबर हमले से इनकार किया।
    - लेकिन इस घटना ने अन्य देशों में इंटरनेट पर निर्भर महत्वपूर्ण प्रणालियों की जाँच करने वाले शत्रुतापूर्ण राज्य और गैर-राज्य अभिकर्त्ताओं की संभावना और ऐसी संपत्तियों को मज़बूत करने की आवश्यकता को रेखांकित किया।

भारत में CIIs संरक्षण:

- **नोडल एजेंसी के रूप में NCIIPC:**
    - इसका निर्माण जनवरी 2014 में किया गया। राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC) देश की महत्वपूर्ण सूचना अवसंरचना की सुरक्षा के लिये सभी उपाय करने हेतु नोडल एजेंसी है।
- **NCIIPC का अधिदेश:**
    - यह CII को अनधिकृत पहुँच, संशोधन, उपयोग, प्रकटीकरण, व्यवधान, अक्षमता से बचाने के लिये अनिवार्य है।
    - यह नीति मार्गदर्शन, विशेषज्ञता साझा करने और प्रारंभिक चेतावनी या अलर्ट के लिये स्थितिजन्य जागरूकता हेतु CII को राष्ट्रीय स्तर के खतरों की निगरानी और पूर्वानुमान करेगा।
    - महत्त्वपूर्ण सूचना अवसंरचना के लिये किसी भी **खतरे की स्थिति में NCIIPC सूचना मांग सकता है और महत्त्वपूर्ण क्षेत्रों या महत्त्वपूर्ण सूचना अवसंरचना पर महत्त्वपूर्ण प्रभाव डालने वाले या सेवा देने वाले व्यक्तियों को निर्देश** दे सकता है।
- **बुनियादी ज़िम्मेदारी:**
    - CII प्रणाली की सुरक्षा की मूल ज़िम्मेदारी उस **CII को चलाने वाली एजेंसी की होगी**।

यूपीएससी सिविल सेवा परीक्षा विगत वर्षों के प्रश्न:

प्रश्न. भारत में निम्नलिखित में से किसके लिये साइबर सुरक्षा घटनाओं पर रिपोर्ट करना कानूनी रूप से अनिवार्य है? (2017)

1. सेवा प्रदाताओं
2. डेटा केंद्र
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)

व्याख्या:

- सूचना प्रौद्योगिकी अधिनियम, 2000 (IT Act) की धारा 70 B के अनुसार, केंद्र सरकार ने अधिसूचना द्वारा घटना प्रतिक्रिया के लिये राष्ट्रीय एजेंसी के रूप में कार्य करने हेतु भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-In) नामक एक एजेंसी का गठन किया गया है।
- केंद्र सरकार ने आईटी अधिनियम, 2000 की धारा 70 B के तहत वर्ष 2014 में CERT-In के लिये नियम स्थापित और अधिसूचित किये। नियम 12 (1) (A) के अनुसार, घटना होने के उचित समय के भीतर CERT-In को साइबर सुरक्षा की घटनाओं के लिये सेवा प्रदाताओं, मध्यस्थों, डेटा केंद्रों और कॉर्पोरेट निकायों हेतु रिपोर्ट करना अनिवार्य है। **अत: विकल्प (d) सही है।**

स्रोत: इंडियन एक्सप्रेस

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/critical-information-infrastructure