भारत की साइबर सुरक्षा के लिये चुनौतियाँ

प्रलिम्सि के लिये:

[हैकिंग](), [फिशिंग](), साइबर सुरक्षा, कंप्यूटर आपातकालीन प्रतिक्रिया टीम, भारत (CERT-IN), सूचना प्रौद्योगिकी (IT) संशोधन अधिनियम 2008, [स्विफ्ट प्रणाली]()

मेन्स के लिये:

भारत की साइबर सुरक्षा से संबंधित चुनौतियाँ।

स्रोत: [द हिंदू]()

चर्चा में क्यों?

कॉर्पोरेट मामलों के मंत्रालय (Ministry of Corporate Affairs- MoCA) ने एक साइबर सुरक्षा विशेषज्ञ द्वारा मुद्दा उठाए जाने के 10 महीने बाद, देश के शीर्ष उद्योगपतियों, मशहूर हस्तियों और खेल आइकनों सहित वीवीआईपी की व्यक्तिगत जानकारी को उजागर करने वाली एक महत्त्वपूर्ण भेद्यता को ठीक कर दिया है।

- साइबर सुरक्षा दोष की शुरुआत में एक साइबर सुरक्षा विशेषज्ञ द्वारा पहचान की गई थी, जिसने [कंप्यूटर इमरजेंसी रिस्पांस टीम इंडिया (CERT-IN)]() को इस मुद्दे की सूचना दी थी।
- अलर्ट के बावजूद, भेद्यता कई महीनों तक सक्रिय रही, जिससे संभावित डेटा चोरी या दुरुपयोग के बारे में चिंताएँ बढ़ गईं।

CERT-In क्या है?

- **परिचय:**
    - CERT-In एक नोडल एजेंसी है जिसका कार्य [हैकिंग]() और [फिशिंग]() जैसे **साइबर सुरक्षा खतरों से निपटना** है। यह **इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (Ministry of Electronics and Information Technology - MoEIT)** के तहत संचालित होता है।
    - CERT-In **जनवरी 2004** से परिचालन में है।
- **CERT-In के कार्य:**
    - **सूचना प्रौद्योगिकी संशोधन अधिनियम, 2008** के अनुसार, CERT-In को साइबर सुरक्षा के क्षेत्र में निम्नलिखित कार्य करने के लिये **राष्ट्रीय एजेंसी के रूप में नामित** किया गया है:
        - साइबर घटनाओं पर सूचना का संग्रहण, विश्लेषण और प्रसार।
        - साइबर सुरक्षा घटनाओं का पूर्वानुमान और अलर्ट।
        - साइबर सुरक्षा घटनाओं से निपटने हेतु आपातकालीन उपाय।
        - साइबर घटना प्रतिक्रिया गतिविधियों का समन्वय।
        - सूचना सुरक्षा प्रथाओं, प्रक्रियाओं, रोकथाम, प्रतिक्रिया और साइबर घटनाओं की रिपोर्टिंग से संबंधित दिशा-निर्देश, सलाह, भेद्यता नोट तथा श्वेतपत्र जारी करना।
        - साइबर सुरक्षा से संबंधित ऐसे अन्य कार्य जो निर्धारित किये जा सकते हैं।
- **भारत के लिये महत्त्व:**
    - CERT-In भारत के लिये महत्त्वपूर्ण है क्योंकि यह देश की महत्त्वपूर्ण सूचना अवसंरचना और डिजिटल संपत्तियों को साइबर हमलों से बचाने में सहायता करता है।
    - यह देश के विभिन्न क्षेत्रों, जैसे सरकार, रक्षा, बैंकिंग, दूरसंचार आदि की साइबर लचीलापन और तत्परता को बढ़ाने में भी सहायता करता है।
    - यह एक सुरक्षित साइबर वातावरण को बढ़ावा देकर देश की राष्ट्रीय सुरक्षा और आर्थिक विकास में भी योगदान देता है।

क्रिटिकिल इंफॉर्मेशन इंफ्रास्ट्रक्चर क्या है?

- परिचय:
  - 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 का उल्लंघन कर किसी संरक्षित प्रणाली तक पहुँच सुनिश्चित करता है अथवा उस तक पहुँच सुनिश्चित करने का प्रयास करता है, उसे 10 वर्ष तक की जेल की सज़ा हो सकती है।
- भारत में CII का संरक्षण:
  - **केंद्रक अभिकरण के रूप में NCIIPC :**
    - जनवरी 2014 में गठित **नेशनल क्रिटिकिल इंफॉर्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर (NCIIPC)** देश की महत्त्वपूर्ण सूचना बुनियादी ढाँचे की सुरक्षा के लिये सभी उपाय करने वाली केंद्रक अभिकरण है।
  - **NCIIPC का अधिदेश:**
    - यह **CII को अनधिकृत पहुँच, संशोधन**, उपयोग, प्रकटीकरण, व्यवधान, अक्षमता अथवा व्याकुलता **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 तथा 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।

भारत की साइबर सुरक्षा के समक्ष कौ- सी चुनौतियाँ हैं?

- **महत्त्वपूर्ण बुनियादी ढाँचे की भेद्यता:**
  - पावर ग्रिड, परिवहन प्रणाली तथा संचार नेटवर्क **साइबर हमलों के प्रति संवेदनशील** हैं जो आवश्यक सेवाओं एवं राष्ट्रीय सुरक्षा के लिये खतरा उत्पन्न करते हैं।
  - उदाहरणार्थ अक्तूबर 2019 में कुडनकुलम परमाणु ऊर्जा संयंत्र पर साइबर हमले का प्रयास किया गया था जो महत्त्वपूर्ण सूचना बुनियादी ढाँचे के लिये संभावित जोखिमों को उजागर करता है।
- **वित्तीय क्षेत्र को खतरा:**
  - वित्तीय क्षेत्र को **साइबर हमलों के उच्च जोखिम का सामना** करना पड़ता है, साइबर अपराधी को बैंकों, वित्तीय संस्थानों एवं ऑनलाइन भुगतान प्रणालियों को निशाना बना रहे हैं।
  - मार्च 2020 में सिटी यूनियन बैंक के स्विफ्ट सिस्टम (SWIFT System) पर हुए मैलवेयर हमलों के परिणामस्वरूप वित्तीय क्षति, पहचान की चोरी व वित्तीय प्रणाली में लोगों का विश्वास कम हो सकता है।
- **डेटा उल्लंघन तथा गोपनीयता संबंधी चिंताएँ:**
  - भारत द्वारा डिजिटल अर्थव्यवस्था में परिवर्तित होने के साथ वैयक्तिक तथा सरकारी डेटा के ऑनलाइन भंडारण में वृद्धि से डेटा उल्लंघन का खतरा बढ़ जाता है।
  - मई 2021 में **कॉमन एडमिशन टेस्ट (CAT) डेटा लीक** जैसे संवेदनशील डेटा उल्लंघनों का सुरक्षा और गोपनीयता पर हानिकारक प्रभाव पड़ सकता है।
- **साइबर जासूसी:**
  - भारत को साइबर जासूसी/गुप्तचरी संबंधी गतिविधियों का सामना करना पड़ता है जिसका उद्देश्य गोपनीय जानकारी चुराना एवं रणनीतिक लाभ हासिल करना है।
  - **उदाहरणार्थ** वर्ष **2020** में घटित **ऑपरेशन साइडकॉपी**, जहाँ एक पाकिस्तानी थ्रेट एक्टर ने मैलवेयर और फिशिंग ईमेल के माध्यम से भारतीय सैन्य एवं राजनयिक कर्मियों को लक्षित किया था।
- **एडवांस्ड परसिस्टेंट थ्रेट्स-APTs:**
  - APTs का आशय **जटिल एवं दीर्घकालिक साइबर हमलों** से है जो एक चुनौती पेश करते हैं क्योंकि उनका पता लगाना एवं उनका मुकाबला करना मुश्किल होता है।
  - फरवरी 2021 में **चीन से संबंधित APT समूह** द्वारा **भारत के विद्युत क्षेत्र को निशाना बनाना** जो संभावित रूप से भारत में पावर आउटेज का कारण बन सकते थे, इस खतरे की गंभीरता को रेखांकित करता है।
- **आपूर्ति शृंखला की कमज़ोरियाँ:**
  - सरकार एवं व्यवसायों द्वारा उपयोग किये जाने वाले सॉफ्टवेयर अथवा हार्डवेयर घटकों में कमज़ोरियाँ आपूर्ति शृंखला में कमज़ोरियों को जन्म देती हैं।
  - दिसंबर 2020 में **सोलरविंड्स पर वैश्विक साइबर हमले** ने **राष्ट्रीय सूचना विज्ञान केंद्र (NIC)** एवं **इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MeitY)** सहित भारतीय संगठनों को प्रभावित किया।

साइबर सुरक्षा के लिये क्या पहल की गई हैं?

- राष्ट्रीय साइबर सुरक्षा नीति
- साइबर सुरक्षित भारत पहल
- भारतीय साइबर अपराध समन्वय केंद्र (I4C)
- साइबर स्वच्छता केंद्र (बॉटनेट सफाई और मैलवेयर विश्लेषण केंद्र)
- रक्षा साइबर एजेंसी (DCyA) ।

आगे की राह

- साइबर अपराधों को नियंत्रित करने वाला भारत का प्राथमिक कानून 2000 का **सूचना प्रौद्योगिकी (IT) अधिनियम** है, जिसे नई चुनौतियों एवं खतरों से निपटने के लिये कई बार संशोधित किया गया है।
- साइबर अपराधियों की कम सज़ा दर के साथ ही कई साइबर अपराधों के लिये सटीक परिभाषाओं, प्रक्रियाओं एवं प्रतिबंधों की अनुपस्थिति आईटी अधिनियम में अंतराल तथा सीमाओं के केवल दो उदाहरण हैं।
- भारत को **व्यापक एवं अद्यतन कानून बनाने की आवश्यकता** है जो साइबर सुरक्षा के सभी पहलुओं, जैसे साइबर आतंकवाद, साइबर युद्ध, साइबर जासूसी और साइबर धोखाधड़ी को कवर करे।
- **भारत की साइबर सुरक्षा में सुधार के लिये कई पहल और नीतियाँ हैं, जैसे राष्ट्रीय साइबर सुरक्षा नीति, साइबर सेल और साइबर अपराध जाँच इकाइयाँ, साइबर अपराध रिपोर्टिंग प्लेटफॉर्म तथा क्षमता निर्माण एवं प्रशिक्षण कार्यक्रम।**

UPSC सिविल सेवा परीक्षा, विगत वर्ष 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 उपयोग करके सही उत्तर चुनिये:

(a) केवल 1
(b) केवल 1 और 2
(c) केवल 3
(d) 1, 2 और 3

उत्तर: (d)

- सूचना प्रौद्योगिकी अधिनियम, 2000 (आईटी अधिनियम) की धारा 70 बी के अनुसार, केंद्र सरकार को अधिसूचना द्वारा घटना प्रतिक्रिया के लिये राष्ट्रीय एजेंसी के रूप में कार्य करने हेतु भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-in) नामक एक एजेंसी नियुक्त करनी चाहिये।
- केंद्र सरकार ने आईटी अधिनियम, 2000 की धारा 70बी के तहत वर्ष 2014 में सीईआरटी-इन के नियमों की स्थापना और अधिसूचित किया।
- नियम 12(1)(ए) के अनुसार, सेवा प्रदाताओं, मध्यस्थों, डेटा केंद्रों और कॉर्पोरेट निकायों के लिये रिपोर्ट करना अनिवार्य है। घटना घटित होने के उचित समय के भीतर CERT-in द्वारा साइबर सुरक्षा। **अतः 1, 2 और 3 सही हैं। अतः विकल्प (d) सही उत्तर है।**

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/challenges-to-india-s-cyber-security