साइबर-सुरक्षा में आत्मनिर्भरता

प्रिलिम्स के लिये:

साइबर-सुरक्षा में आत्मनिर्भरता, भारत मोबाइल कॉन्ग्रेस, भारत का डिजिटल बुनियादी ढाँचा, राष्ट्रीय सुरक्षा, इलेक्ट्रॉनिक उपकरण, राष्ट्रीय साइबर सुरक्षा रणनीति 2020।

मेन्स के लिये:

साइबर सुरक्षा में आत्मनिर्भरता, IT, अंतरिक्ष, कंप्यूटर, रोबोटिक्स, नैनो-प्रौद्योगिकी, जैव-प्रौद्योगिकी के क्षेत्र में जागरूकता।

स्रोत: इंडियन एक्सप्रेस

चर्चा में क्यों?

हाल ही में भारत के प्रधानमंत्री ने **इंडिया मोबाइल कॉन्ग्रेस** के 7वें संस्करण के दौरान साइबर सुरक्षा में आत्मनिर्भरता के महत्त्व को रेखांकित किया।

- हार्डवेयर, सॉफ्टवेयर और कनेक्टिविटी सहित संपूर्ण साइबर सुरक्षा मूल्य शृंखला में आत्मनिर्भरता पर प्रधानमंत्री का ज़ोर भारत के डिजिटल बुनियादी ढाँचे **की सुरक्षा के बारे में बढ़ती चिंता** को दर्शाता है।

साइबर सुरक्षा:

- साइबर सुरक्षा **कंप्यूटर सिस्टम, नेटवर्क, डिवाइस और डेटा की** चोरी, क्षति, अनधिकृत पहुँच या किसी भी प्रकार के दुर्भावनापूर्ण इरादे से **बचाने की प्रथा** है।
- इसमें डिजिटल जानकारी के साथ-साथ इसे संगृहीत, संसाधित व प्रसारित करने वाले बुनियादी ढाँचे की सुरक्षा के लिये डिज़ाइन की गई प्रौद्योगिकियों, प्रक्रियाओं और प्रथाओं की एक विस्तृत शृंखला शामिल है।

साइबर सुरक्षा में आत्मनिर्भरता:

- **परिचय:**
  - साइबर सुरक्षा में आत्मनिर्भरता से तात्पर्य किसी अन्य देश की प्रौद्योगिकी या सहायता पर बहुत अधिक निर्भर हुए बिना अपने **डिजिटल बुनियादी ढाँचे, डेटा** एवं **सूचना प्रणालियों की सुरक्षा के लिये** अपनी क्षमताओं, प्रौद्योगिकियों और विशेषज्ञता को विकसित करने व इसे बनाए रखने की क्षमता से है।
  - यह साइबर सुरक्षा उपकरणों और विशेषज्ञता के लिये बाह्य स्रोतों पर निर्भरता को कम करते हुए स्वदेशी साइबर सुरक्षा समाधानों एवं प्रथाओं के विकास व इसकी तैनाती पर बल देती है।
- **साइबर सुरक्षा में आत्मनिर्भरता की आवश्यकता:**
  - **राष्ट्रीय सुरक्षा:** देश की कई महत्त्वपूर्ण बुनियादी ढाँचा प्रणालियाँ, जैसे ऊर्जा ग्रिड, परिवहन नेटवर्क और संचार प्रणालियाँ, डिजिटल प्रौद्योगिकी पर निर्भर हैं।
    - आधुनिक सैन्य अभियान **काफी हद तक डिजिटल तकनीक पर निर्भर हैं।**
    - साइबर सुरक्षा में किसी भी समझौते के परिणामस्वरूप व्यवधान उत्पन्न हो सकता है, जिससे राष्ट्रीय सुरक्षा के लिये भी सीधा खतरा उत्पन्न हो सकता है।
  - **भू-राजनीतिक विचार:** विदेशी प्रौद्योगिकी पर अत्यधिक निर्भरता, विशेष रूप से उन देशों से जिनके साथ भारत के चीन जैसे तनावपूर्ण संबंध हो सकते हैं, सुरक्षा जोखिम उत्पन्न कर सकते हैं।
    - भारत चिंतित है क्योंकि वह इलेक्ट्रॉनिक्स के लिये अपना अधिकांश कच्चा माल चीन से आयात करता है।
    - आत्मनिर्भर होने से प्रौद्योगिकी के लिये बाह्य **प्रौद्योगिकी स्रोतों पर निर्भर रहने से जुड़े जोखिम** कम हो जाते हैं।
- **तकनीकी स्वतंत्रता:** आत्मनिर्भरता के लिये सुरक्षित और विश्वसनीय हार्डवेयर, सॉफ्टवेयर तथा नेटवर्किंग घटकों के निर्माण की आवश्यकता

होती है।

  - यह साइबर सुरक्षा के क्षेत्र में नवाचार और अनुसंधान को प्रोत्साहित करता है।
  - विदेशी प्रौद्योगिकी पर निर्भरता आपूर्ति शृंखला में कमज़ोरियाँ उत्पन्न कर सकती है। आत्मनिर्भरता भारत के संभावित जोखिमों को कम करते हुए संपूर्ण प्रौद्योगिकी आपूर्ति शृंखला पर अधिक नियंत्रण रखने की अनुमति देती है।

भारत में साइबर सुरक्षा से संबंधित चुनौतियाँ:

- **लाभ-अनुकूल बुनियादी ढाँचा मानसिकता:**
  - उदारीकरण के बाद, **सूचना प्रौद्योगिकी (IT), विद्युत और दूरसंचार क्षेत्र** में निजी क्षेत्र द्वारा बड़े निवेश देखे गए हैं। हालाँकि साइबर हमले की तैयारी और नियामक ढाँचे में सुधार पर पर्याप्त ध्यान न देना चिंता का विषय है।
  - सभी ऑपरेटरों के लिये लाभ मुख्य प्राथमिकता है और वे बुनियादी ढाँचे में निवेश नहीं करना चाहते हैं जिससे उन्हें लाभ नहीं मिलेगा।
- **पृथक प्रक्रियात्मक संहिता का अभाव:**
  - साइबर या कंप्यूटर से संबंधित अपराधों की जाँच के लिये कोई पृथक प्रक्रियात्मक संहिता उपलब्ध नहीं है।
- **साइबर हमलों की ट्रांस-नेशनल प्रकृति:**
  - अधिकांश साइबर अपराध अंतर्राष्ट्रीय प्रकृति के होते हैं। विदेशी क्षेत्रों से साक्ष्य एकत्र करना न केवल एक कठिन बल्कि धीमी प्रक्रिया है।
- **डिजिटल पारिस्थितिकी तंत्र का विस्तार:**
  - विगत कुछ वर्षों में भारत अपने विभिन्न आर्थिक पहलुओं को डिजिटल बनाने की राह पर आगे बढ़ा है और उसने सफलतापूर्वक अपने लिये एक स्थान सुनिश्चित किया है।
  - **5G** और **इंटरनेट ऑफ थिंग्स (IoT) जैसी** नवीनतम प्रौद्योगिकियाँ इंटरनेट से जुड़े पारिस्थितिकी तंत्र के कवरेज को बढ़ाने में सहायता प्रदान करेंगी।
  - डिजिटलीकरण के आगमन के साथ, सर्वोपरि उपभोक्ता और नागरिक डेटा को डिजिटल रूप से एकत्र किया जाएगा तथा लेनदेन की प्रक्रिया ऑनलाइन किये जाने की संभावना है जो मुख्य रूप से हैकर्स एवं साइबर अपराधियों को अपनी ओर आकर्षित करती है।
- **सीमित विशेषज्ञता और अधिकार:**
  - देश में **क्रिप्टोकरेंसी** से संबंधित **दर्ज अपराधों की संख्या कम है** क्योंकि ऐसे अपराधों को हल करने की क्षमता सीमित है।
  - हालाँकि अधिकांश राज्य साइबर लैब हार्ड डिस्क और मोबाइल फोन का विश्लेषण करने में सक्षम हैं, फिर भी उन्हें **इलेक्ट्रॉनिक साक्ष्य के परीक्षक'** (केंद्र सरकार द्वारा) के रूप में मान्यता नहीं दी गई है। मान्यता के बिना वे इलेक्ट्रॉनिक डेटा संबंधित विशेषज्ञ राय प्रस्तुत नहीं कर सकते हैं।

प्रौद्योगिकी में भारत का प्रदर्शन:

- **घरेलू आपूर्ति शृंखला भागीदार:**
  - भारत अपने आपूर्ति शृंखला भागीदारों, विशेषकर प्रौद्योगिकी क्षेत्र में विविधता लाने के लिये सक्रिय रूप से कार्य कर रहा है। विनिर्माण पारिस्थितिकी तंत्र में चीनी भागीदारों के प्रभुत्व को देखते हुए यह विविधीकरण आवश्यक है।
  - सरकार मैलवेयर और साइबर खतरों को रोकने के लिये अधिक विश्वसनीय एवं सुरक्षित आपूर्ति शृंखला स्थापित करना चाहती है।
- **5G और मोबाइल ब्रॉडबैंड:**
  - सरकार ने **देश भर के शैक्षणिक संस्थानों को 100 5G यूज़ केस लैब से सम्मानित किया** , जो 5G बुनियादी ढाँचे को आगे बढ़ाने के लिये उसकी प्रतिबद्धता को दर्शाता है।
  - भारत इंटरनेट सेवा के मामले में **5G रोलआउट चरण से 5G रीच-आउट चरण में पहुँच गया है** । केवल एक वर्ष में औसत मोबाइल ब्रॉडबैंड स्पीड तीन गुना बढ़ गई है।
  - **6G तकनीक में अग्रणी** होने के भारत के प्रयास **तकनीकी प्रगति में सबसे आगे रहने की देश की महत्त्वाकांक्षा** को रेखांकित करता है।
- **ब्रॉडबैंड स्पीड:**
  - ब्रॉडबैंड स्पीड के मामले में भारत की स्थिति में काफी सुधार हुआ है, जो वैश्विक स्तर पर **118वें से 43वें स्थान** पर पहुँच गया है, यह देश में **हाई-स्पीड इंटरनेट एक्सेस की वृद्धि** को इंगित करता है।
- **इलेक्ट्रॉनिक्स और स्मार्टफोन विनिर्माण:**
  - देश में इलेक्ट्रॉनिक्स और स्मार्टफोन निर्माण में उल्लेखनीय प्रगति हुई है।
  - सेमीकंडक्टर विनिर्माण प्रौद्योगिकी आपूर्ति शृंखला का एक महत्त्वपूर्ण घटक है और हार्डवेयर उत्पादन में महत्त्वपूर्ण भूमिका निभाता है।
- **स्टार्टअप इकोसिस्टम:**
  - **भारत का स्टार्टअप इकोसिस्टम** फल-फूल रहा है, स्टार्टअप की संख्या में तेज़ी से वृद्धि हो रही है।
  - **वर्ष 2014 से पहले 100 स्टार्टअप थे, जिनकी संख्या बढ़कर आज लगभग 100,000 तक पहुँच गई** है।

साइबर सुरक्षा से संबंधित पहल:

- **वैश्विक पहल:**
  - **साइबर अपराध पर बुडापेस्ट अभिसमय:**
  - **इंटरनेट गवर्नेंस फोरम (IGF)**

- [UNGA प्रस्ताव]
- भारतीय पहल:
  - राष्ट्रीय साइबर सुरक्षा रणनीति 2020
  - राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC)
  - भारतीय साइबर अपराध समन्वय केंद्र (I4C)
  - राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल
  - कंप्यूटर आपातकालीन प्रतिक्रिया टीम - भारत (CERT-In)
  - भारत का डिजिटिल व्यक्तिगत डेटा संरक्षण विधेयक 2022

आगे की राह

- **साइबर सुरक्षा के क्षेत्र में अनुसंधान और विकास** को प्रोत्साहित करना। **नवाचार और स्वदेशी साइबर सुरक्षा प्रौद्योगिकियों के विकास** को बढ़ावा देने के लिये सरकारी एजेंसियों, शैक्षणिक संस्थानों एवं निजी क्षेत्र की कंपनियों के बीच साझेदारी स्थापित करना।
- नवीन साइबर सुरक्षा समाधानों पर कार्य करने वाले साइबर सुरक्षा स्टार्टअप और छोटे व मध्यम आकार के उद्यमों (SME) को सहायता, वित्त पोषण एवं प्रोत्साहन प्रदान करना। **ये स्टार्टअप देश में घरेलू सुरक्षा तकनीक स्थापित करने में महत्त्वपूर्ण भूमिका निभा सकते हैं।**

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/self-reliance-in-cybersecurity