3. साइबर सुरक्षा (Cyber Security)

3.1. साइबर सुरक्षा (Cyber Security)

साइबर सुरक्षा – एक नज़र में

साइबर सुरक्षा के बारे मे

- साइबर स्पेस में एकत्रित जानकारी या संपत्ति को अनधिकृत पहुंच, उपयोग, प्रकटीकरण, बाधा, संशोधन या विनाश से **सुरक्षित करने की प्रक्रिया** साइबर सुरक्षा कहलाती है।
- साइबर स्पेस में **लोगों, सॉफ्टवेयर और सेवाओं के बीच अंतर्संबंध** होता है। यह सूचना और संचार प्रौद्योगिकी उपकरणों तथा नेटवर्क के विश्वव्यापी वितरण द्वारा समर्थित होता है।
- **भारत**, वैश्विक साइबर सुरक्षा सूचकांक (Global Cybersecurity Index: GCI) 2020 में चीन और पाकिस्तान से आगे **10वें** (194 देशों में) स्थान पर है।

साइबर सुरक्षा की आवश्यकता

- **राष्ट्रीय सुरक्षा:** कई देश (चीन सहित) साइबर हमलों में क्षमता विकसित कर रहे हैं, जो युद्ध के समय निर्णायक भूमिका निभा सकते हैं।
- यह बांधों, आपातकालीन सेवाओं, बिजली और ऊर्जा, बैंकिंग एवं वित्तीय सेवाओं आदि जैसे **महत्वपूर्ण बुनियादी ढांचे की रक्षा** करने के लिए आवश्यक है।
- **सरकार का डिजिटल प्रयास** बड़ी संख्या में नागरिकों, कंपनियों और सरकारी एजेंसियों को ऑनलाइन लेनदेन हेतु प्रेरित कर रहा है।
- **डिजिटल रूप से असुरक्षित लक्ष्य** (1.15 बिलियन से अधिक फोन और 700 मिलियन से अधिक इंटरनेट उपयोगकर्ता)।
- **आर्थिक नुकसान को रोकने के लिए** (अगले 10 वर्षों में साइबर हमलों के कारण नुकसान 20 बिलियन डॉलर तक पहुंच सकता है)।
- **स्टार्टअप डिजिटल प्रयास** (भारत डिजिटल प्रौद्योगिकियों के लिए सबसे तेजी से बढ़ते बाजारों में से एक है)।

साइबर सुरक्षा सुनिश्चित करने में चुनौतियाँ

- व्यापक **डिजिटल निरक्षरता**।
- अपर्याप्त सुरक्षा अवसंरचना वाले **निम्न कोटि के उपकरणों का उपयोग**।
- सुभेद्यता के बारे में जानकारी साझा करने में **निजी और सार्वजनिक क्षेत्र का संकोच**।
- अधिकांश इलेक्ट्रॉनिक उपकरणों के लिए **आयात पर निर्भरता**।
- **एजेंसियों के बीच समन्वय की स्पष्ट कमी**।
- **पर्याप्त बुनियादी ढांचे** और प्रशिक्षित कर्मचारियों **की कमी**।
- **अन्य चुनौतियाँ:** राज्य स्तर पर क्षमता की कमी, भौगोलिक बाधाओं का अभाव, भारत के बाहर स्थित अधिकांश सर्वर, साइबर स्पेस में तेजी से विकसित हो रही तकनीक आदि।

साइबर सुरक्षा के लिए मौजूदा तंत्र

- **विधायी उपाय**
  - **राष्ट्रीय साइबर सुरक्षा रणनीति 2020:** राष्ट्र की समृद्धि के लिए एक सुरक्षित, संरक्षित, विश्वसनीय, लचीला और जीवंत साइबर स्पेस सुनिश्चित करना।
  - **राष्ट्रीय साइबर सुरक्षा नीति, 2013:** इसका उद्देश्य साइबर स्पेस में सूचना के बुनियादी ढांचे की रक्षा करना और साइबर घटनाओं से होने वाले नुकसान को कम करना है।
  - **सूचना प्रौद्योगिकी अधिनियम, 2000:** साइबर सुरक्षा के लिए डेटा एक्सेस, इलेक्ट्रॉनिक डेटा इंटरचेंज के माध्यम से किए गए लेनदेन आदि के लिए कानूनी ढांचा प्रदान करता है।
- **संस्थागत उपाय**
  - भारतीय साइबर अपराध समन्वय केंद्र (I4C)।
  - भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT–In)
  - राष्ट्रीय साइबर समन्वय केंद्र (NCCC)।
  - रक्षा मंत्रालय ने रक्षा साइबर एजेंसी का गठन किया।
  - राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC)।
  - साइबर स्वच्छता केंद्र (बॉटनेट क्लीनिंग एंड मैलवेयर एनालिसिस सेंटर)
  - राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल।

आगे की राह

- **अंतर्राष्ट्रीय सहयोग में बढ़ोतरी:** साइबर अपराध पर बुडापेस्ट कन्वेंशन को अपनाने पर विचार किया जाना चाहिए।
- **विभिन्न संस्थानों/एजेंसियों के बीच समन्वय सुनिश्चित करना** और साइबर सुरक्षा के लिए एक समन्वित दृष्टिकोण तैयार करना चाहिए।
- बदलते साइबर परिदृश्य के साथ तालमेल रखने के लिए आई. टी. अधिनियम में संशोधन करना व साइबर सुरक्षा नीति को अपडेट करना आवश्यक है।
- अंतर्राष्ट्रीय मानकों का पालन करते हुए **साइबर बीमा ढांचे** और साइबर ऑडिट की **स्थापना की जानी चाहिए**।
- **क्षमता निर्माण** और कौशल विकास जरूरी है।
- साइबर संचालन के लिए **तेलिन मैनुअल (Tallinn manual) जैसी अंतर्राष्ट्रीय सर्वोत्तम प्रथाओं से सीखना चाहिए**।