PLUTUS IAS

CURRENT AFFAIRS

Argasia Education PVT. Ltd. (GST NO.-09AAPCAI478E1ZH)
Address: Basement C59 Noida, opposite to Priyagold Building gate, Sector 02,
Pocket I, Noida, Uttar Pradesh, 201301, CONTACT NO:-8448440231

Date –23- January 2025

विश्व आर्थिक मंच द्वारा वैश्विक साइबर सुरक्षा आउटलुक रिपोर्ट 2025 जारी

खबरों में क्यों?

- हाल ही में, विश्व आर्थिक मंच (WEF) ने 2025 के लिए वैश्विक साइबर सुरक्षा आउटलुक रिपोर्ट 2025 जारी की है।
- इस रिपोर्ट में वैश्विक स्तर पर भू-**राजनीतिक** तनाव, पुराने तकनीकी ढाँचों और साइबर सुरक्षा में आवश्यक कौशल की कमी के कारण महत्वपूर्ण **ढाँचों** को बढ़ते साइबर खतरों से होने वाले जोखिमों पर चिंता जताई गई है।

- इसके साथ – ही – साथ ही, साइबर खतरों से होने वाले जोखिमों से बचने के लिए साइबर सुरक्षा को मजबूत बनाने और इसके ढाँचों की लचीलापन **क्षमता** में वृद्धि करने की आवश्यकता पर जोर **दिया** गया है।

क्या है विश्व आर्थिक मंच (WEF) ?

- विश्व आर्थिक मंच एक **अंतरराष्ट्रीय** संस्था है, जो सार्वजनिक और निजी क्षेत्रों के बीच सहयोग को बढ़ावा देने का कार्य करती है।
- इस मंच पर वैश्विक, क्षेत्रीय और उद्योग संबंधित मुद्दों पर चर्चा करने के लिए प्रमुख राजनीतिक, व्यावसायिक, सांस्कृतिक और अन्य विशिष्ट **क्षेत्रों** के प्रतिनिधि एकत्र होते हैं।
- **मुख्यालय :** इसका मुख्यालय **स्विट्ज़रलैंड** के जिनेवा में स्थित है।
- **स्थापना :** इस संगठन की **स्थापना** वर्ष 1971 में जर्मन प्रोफेसर क्लॉस श्वाब द्वारा की गई थी, और इसका प्रारंभिक नाम **"यूरोपीय प्रबंधन मंच"** था।

ग्लोबल साइबर सिक्यूरिटी इंडेक्स (GCI) :

- यह सूचकांक अंतर्राष्ट्रीय दूरसंचार संघ (ITU) द्वारा प्रकाशित किया जाता है, **जिसमें** देशों की साइबर सुरक्षा के प्रति प्रतिबद्धता के आधार पर उनका **मूल्यांकन** किया जाता है।
- भारत ने GCI 2024 के पांचवें **संस्करण** में **' टियर 1 '** श्रेणी में स्थान प्राप्त किया है, जो साइबर सुरक्षा के क्षेत्र में एक महत्वपूर्ण उपलब्धि मानी जाती है।

वैश्विक साइबर सुरक्षा आउटलुक रिपोर्ट 2025 में उल्लिखित प्रमुख मुद्दे :

1. **महत्त्वपूर्ण बुनियादी ढाँचे की सुभेद्यता :** जल, जैव सुरक्षा, संचार, ऊर्जा और जलवायु जैसे क्षेत्र पुराने तकनीकी ढाँचों और आपसी निर्भरता के कारण साइबर हमलों से प्रभावित हो सकते हैं। साइबर अपराधी और राज्य अभिकर्त्ता इन क्षेत्रों में परिचालन प्रौद्योगिकी को लक्षित कर रहे हैं, जिससे वैश्विक डेटा प्रवाह में खतरे उत्पन्न हो रहे हैं।
2. **भू-राजनीतिक तनाव :** रूस-यूक्रेन युद्ध जैसे संघर्षों ने ऊर्जा, दूरसंचार और जल जैसे महत्वपूर्ण क्षेत्रों में साइबर और भौतिक हमलों को बढ़ा दिया है। लगभग 60% संगठनों का कहना है कि भू-राजनीतिक तनावों के कारण उनकी साइबर सुरक्षा रणनीतियाँ प्रभावित हुई हैं।
3. **जैव सुरक्षा संबंधी खतरे :** कृत्रिम बुद्धिमत्ता (AI), आनुवंशिक इंजीनियरिंग और जैव प्रौद्योगिकी में हुई प्रगति ने जैव सुरक्षा जोखिमों को बढ़ा दिया है। जैव प्रयोगशालाओं पर साइबर हमलों से अनुसंधान और सुरक्षा प्रोटोकॉल को खतरा हो सकता है। WHO ने इस मुद्दे पर चेतावनी दी है, जैसा कि 2024 में दक्षिण अफ्रीका और ब्रिटेन में हुए हमलों से स्पष्ट हुआ है।
4. **साइबर सुरक्षा कौशल अंतराल का बढ़ना :** इस रिपोर्ट में साइबर सुरक्षा कौशल में बड़े अंतराल को उजागर किया गया है। वर्तमान में दुनिया भर में 4.8 मिलियन पेशेवरों को आवश्यक योग्यताओं की कमी है। दो-तिहाई संगठनों को इस कमी का सामना करना पड़ रहा है, जिनमें से केवल 14% के पास वर्तमान साइबर सुरक्षा परिदृश्य के लिए योग्य कार्मिक हैं।

5. **क्षेत्रीय साइबर सुरक्षा असमानताएँ :** इस रिपोर्ट में विभिन्न क्षेत्रों के बीच साइबर सुरक्षा में असमानताओं को उजागर किया गया है। उदाहरण स्वरूप, यूरोप/उत्तरी अमेरिका में 15% से बढ़कर अफ्रीका में 36% और लैटिन अमेरिका में 42% तक साइबर हमलों के प्रति प्रतिक्रिया में देरी हो रही है।
6. **साइबर अपराध का बढ़ता खतरा :** साइबर अपराध अब एक सुरक्षित और आकर्षक व्यापार बन चुका है, जिसमें कम परिचालन खर्च और उच्च लाभ की संभावना है। अमेरिकी संघीय जांच ब्यूरो (FBI) का अनुमान है कि 2023 में साइबर अपराध से होने वाली वित्तीय हानि 12.5 बिलियन अमेरिकी डॉलर से अधिक हो सकती है।

समाधान / आगे की राह :

1. **साइबर सुरक्षा के लिए रणनीतिक रूप से निवेश को प्राथमिकता देने अत्यंत जरूरत :** वर्ष 2025 के वैश्विक साइबर सुरक्षा परिदृश्य में, सरकारों से आग्रह किया गया है कि वे पुरानी प्रणालियों को उन्नत करें और महत्त्वपूर्ण क्षेत्रों जैसे जल, ऊर्जा व जैव सुरक्षा की रक्षा के लिए साइबर सुरक्षा में निवेश बढ़ाएं। वर्ष 2022 में कोस्टा रिका पर हुए साइबर हमले ने यह स्पष्ट किया कि साइबर सुरक्षा को केवल एक खर्च के रूप में नहीं, बल्कि भविष्य के लिए एक महत्वपूर्ण निवेश के रूप में देखा जाना चाहिए। व्यावसायिक प्राथमिकताओं के साथ साइबर सुरक्षा में निवेश को संतुलित करना बेहद आवश्यक है।
2. **साइबर सुरक्षा बढ़ाने के लिए सार्वजनिक और निजी क्षेत्र के बीच सहयोग की जरूरत :** साइबर सुरक्षा बढ़ाने के लिए सार्वजनिक और निजी क्षेत्र के बीच सहयोग आवश्यक है, जिसमें खुफिया जानकारी साझा करना और सुरक्षित प्रौद्योगिकियाँ विकसित करना शामिल है। SMEs को सरकार से मजबूत प्रोत्साहन मिलना चाहिए ताकि वे भी साइबर सुरक्षा में निवेश कर सकें।
3. **उभरते साइबर खतरों से निपटने के लिए विशेष प्रशिक्षण कार्यक्रमों का विस्तार और कार्यबल विकास को बढ़ावा देने की आवश्यकता :** नए साइबर खतरों से निपटने के लिए कुशल कर्मियों की आवश्यकता है। इसके लिए विशेष प्रशिक्षण कार्यक्रमों का विस्तार और कार्यबल विकास को बढ़ावा देने की आवश्यकता है।
4. **साइबर खतरों से निपटने के लिए त्वरित प्रतिक्रिया तंत्र और संकट प्रबंधन ढाँचों का विकास करना आवश्यक :** साइबर खतरों से निपटने के लिए रोकथाम के बजाय लचीलापन पर अधिक ध्यान दिया जाना चाहिए। त्वरित प्रतिक्रिया तंत्र और संकट प्रबंधन ढाँचों का विकास करना आवश्यक है।
5. **अंतर्राष्ट्रीय स्तर पर आपसी सहयोग की जरूरत :** वर्तमान समय में साइबर खतरों से निपटने के लिए विश्व के सभी देशों को संयुक्त राष्ट्र और G-20 जैसे मंचों के माध्यम से सहयोग करना चाहिए और विकसित देशों को उभरती अर्थव्यवस्थाओं की साइबर सुरक्षा क्षमता को मजबूत करने में मदद करनी चाहिए।
6. **भारत में साइबर सुरक्षा के लिए संस्थागत ढाँचों की स्थापना करने की आवश्यकता :** भारत ने साइबर सुरक्षा के लिए कई विधायी उपायों और संस्थागत ढाँचों की स्थापना की है, जैसे IT अधिनियम, CERT-In, NCIIPC, और I4C। इसके साथ ही, राष्ट्रीय साइबर सुरक्षा नीति और क्षेत्र-विशिष्ट विनियम जैसे सेबी द्वारा अनिवार्य साइबर सुरक्षा ढाँचों को लागू किया गया है।

निष्कर्ष :

- विश्व आर्थिक मंच द्वारा जारी वैश्विक साइबर सुरक्षा आउटलुक रिपोर्ट 2025 में बढ़ते साइबर खतरों और रणनीतिक निवेश की **आवश्यकता** पर बल दिया गया है। राष्ट्रों को **महत्त्वपूर्ण** बुनियादी ढाँचों की सुरक्षा को प्राथमिकता देनी चाहिए ताकि **राष्ट्रीय** सुरक्षा और आर्थिक स्थिरता सुनिश्चित की जा सके। वैश्विक स्तर पर जैसे-जैसे साइबर खतरे जटिल होते जा रहे हैं, देशों को अपने राष्ट्रीय सुरक्षा, सार्वजनिक सुरक्षा और आर्थिक स्थिरता को सुनिश्चित करने के लिए अपने **महत्त्वपूर्ण** बुनियादी ढाँचों की रक्षा और उसकी **सुरक्षा** को सर्वोच्च प्राथमिकता देनी चाहिए।

स्त्रोत – इंडियन एक्सप्रेस।

प्रारंभिक परीक्षा के लिए अभ्यास प्रश्न :

Q.1. वैश्विक साइबर सुरक्षा आउटलुक रिपोर्ट 2025 में साइबर सुरक्षा के संदर्भ में निम्नलिखित कथनों पर विचार कीजिए।

1. साइबर सुरक्षा को केवल एक खर्च के रूप में देखा जाना चाहिए।
2. साइबर सुरक्षा में रणनीतिक **निवेश** को प्राथमिकता देने की आवश्यकता है।
3. साइबर सुरक्षा कौशल अंतराल में कमी नहीं हो रही है।
4. इसमें सार्वजनिक-निजी सहयोग की अत्यंत आवश्यकता है।

उपर्युक्त कथनों में से कौन सा कथन सही है ?

A. केवल 1 और 3

B. केवल 2 और 4

C. इनमें से कोई नहीं

D. उपरोक्त सभी।

उत्तर – B

मुख्य परीक्षा के लिए अभ्यास प्रश्न :

Q.1. विश्व आर्थिक मंच (WEF) द्वारा जारी वैश्विक साइबर सुरक्षा आउटलुक रिपोर्ट 2025 में जिन प्रमुख मुद्दों पर चिंता जताई गई है, उन्हें रेखांकित करते हुए यह चर्चा कीजिए कि भारत में साइबर सुरक्षा को मजबूत बनाने के लिए कौन-कौन से कदम उठाने की अत्यंत आवश्यकता है? (शब्द सीमा – 250 अंक – 15)

Dr. Akhilesh Kumar Shrivastava