ग्लोबल साइबरसिक्योरिटी आउटलुक 2025

प्रिलिम्स के लिये:

विश्व आर्थिक मंच (WEF), ग्लोबल साइबरसिक्योरिटी आउटलुक 2025, साइबर अपराध, सूचना प्रौद्योगिकी अधिनियम, 2000, डिजिटल व्यक्तिगत डेटा संरक्षण विधेयक, 2022, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल, राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC), भारत राष्ट्रीय साइबर सुरक्षा अभ्यास 2024, दूरसंचार (महत्त्वपूर्ण दूरसंचार अवसंरचना) नियम, 2024 , बुडापेस्ट साइबर अपराध अभिसमय

मेन्स के लिये:

ग्लोबल साइबरसिक्यूरिटी आउटलुक 2025 रिपोर्ट की मुख्य विशेषताएँ, साइबर सुरक्षा के लिये वर्तमान रूपरेखा, प्रमुख उभरते साइबर खतरे, आगे की राह

स्रोत: डाउन टू अर्थ

चर्चा में क्यों?

हाल ही में विश्व आर्थिक मंच (WEF) ने **ग्लोबल साइबरसिक्योरिटी आउटलुक 2025 रिपोर्ट** जारी की।

- इस रिपोर्ट में **भू-राजनीतिक तनाव, अप्रचलित प्रणालियों और साइबर सुरक्षा कौशल के अभाव** के कारण महत्त्वपूर्ण बुनियादी ढाँचे के लिये बढ़ते साइबर खतरों पर प्रकाश डाला गया है और सुरक्षा बढ़ाए जाने और लचीलेपन की आवश्यकता पर बल दिया गया है।

विश्व आर्थिक मंच (WEF)

- **परिचय:** विश्व आर्थिक मंच (WEF) सार्वजनिक-निजी सहयोग के लिये एक अंतर्राष्ट्रीय संगठन है। इस फोरम/मंच में वैश्विक, क्षेत्रीय और उद्योग एजेंडा को आयाम देने के लिये समाज के अग्रणी राजनीतिक, व्यावसायिक, सांस्कृतिक और अन्य अभिकर्त्ता शामिल होते हैं।
- **मुख्यालय:** जिनेवा, स्विट्ज़रलैंड
- **स्थापना:** इसकी स्थापना **वर्ष 1971** में जर्मन प्रोफेसर **क्लॉस श्वाब** द्वारा की गई थी। इसका मूल नाम **यूरोपीय प्रबंधन मंच** था।

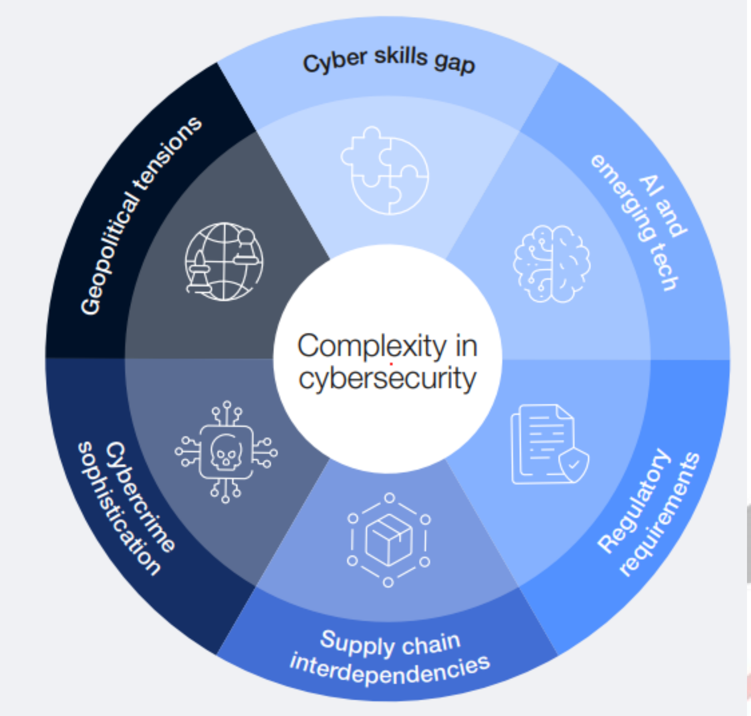
टिप्पणी:

- ग्लोबल साइबरसिक्यूरिटी इंडेक्स (GCI) नामक यह सूचकांक अंतर्राष्ट्रीय दूरसंचार संघ (ITU) द्वारा जारी किया जाता है तथा इसके अंतर्गत **साइबर सुरक्षा के प्रति देशों की प्रतिबद्धता** के आधार पर उनका मूल्यांकन और श्रेणीकरण किया जाता है।
- भारत ने GCI 2024 **के 5वें संस्करण में टियर 1 का दर्जा** प्राप्त कर साइबर सुरक्षा में एक बड़ी उपलब्धि हासिल की है।

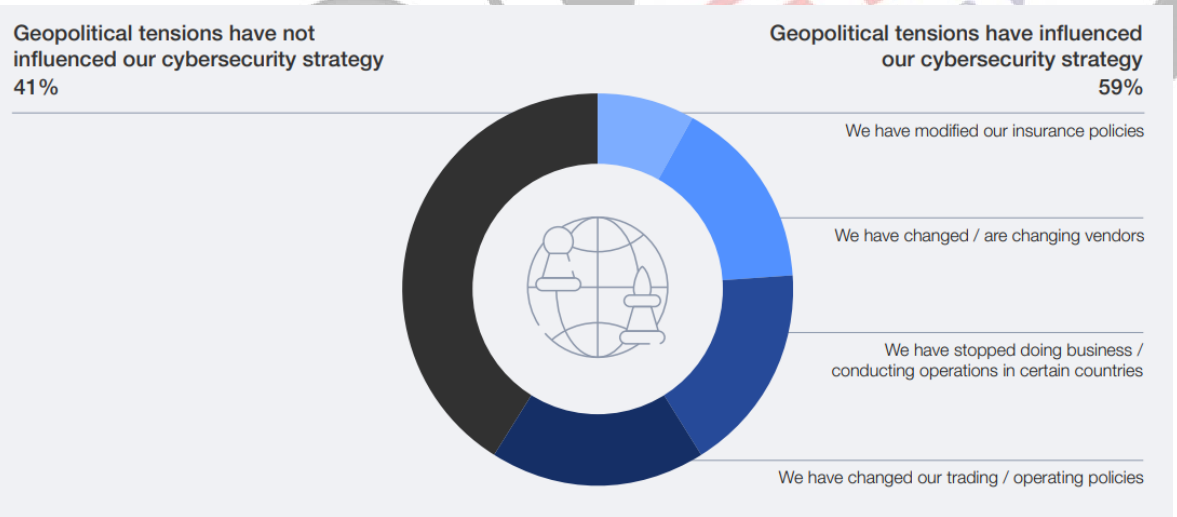
रिपोर्ट में उजागर किये गए प्रमुख मुद्दे कौन-से हैं?

- **महत्त्वपूर्ण बुनियादी ढाँचे की सुभेद्यता: जल,** जैव सुरक्षा**, संचार, ऊर्जा** और **जलवायु** जैसे महत्त्वपूर्ण बुनियादी ढाँचे क्षेत्र **पुरानी प्रौद्योगिकियों और परस्पर संबद्ध प्रणालियों** के कारण साइबर हमलों के प्रति सुभेद्य हैं।
  - साइबर अपराधी और राज्य अभिकर्त्ता **अधोसमुद्री केबलों** सहित **परिचालन प्रौद्योगिकी को लक्षित करते हैं**, जिससे वैश्विक डेटा प्रवाह के लिये खतरे उत्पन्न होते हैं।
  - वर्ष 2024 में **फिशिंग और सोशल इंजीनियरिंग हमलों** में एकाएक बढ़ोतरी हुई, जिसमें 42% संगठनों ने ऐसी घटनाओं की रिपोर्ट की।
  - **उदाहरण: वर्ष 2024** में एक **अमेरिकी जल यूटिलिटी कंपनी पर हुए साइबर हमले** से परिचालन बाधित हुआ, जिससे जल उपचार सुविधाओं

की सुभेद्यता उजागर हुईं।


Cyber skills gap
AI and emerging tech
Regulatory requirements
Supply chain interdependencies
Cybercrime sophistication
Geopolitical tensions
Complexity in cybersecurity

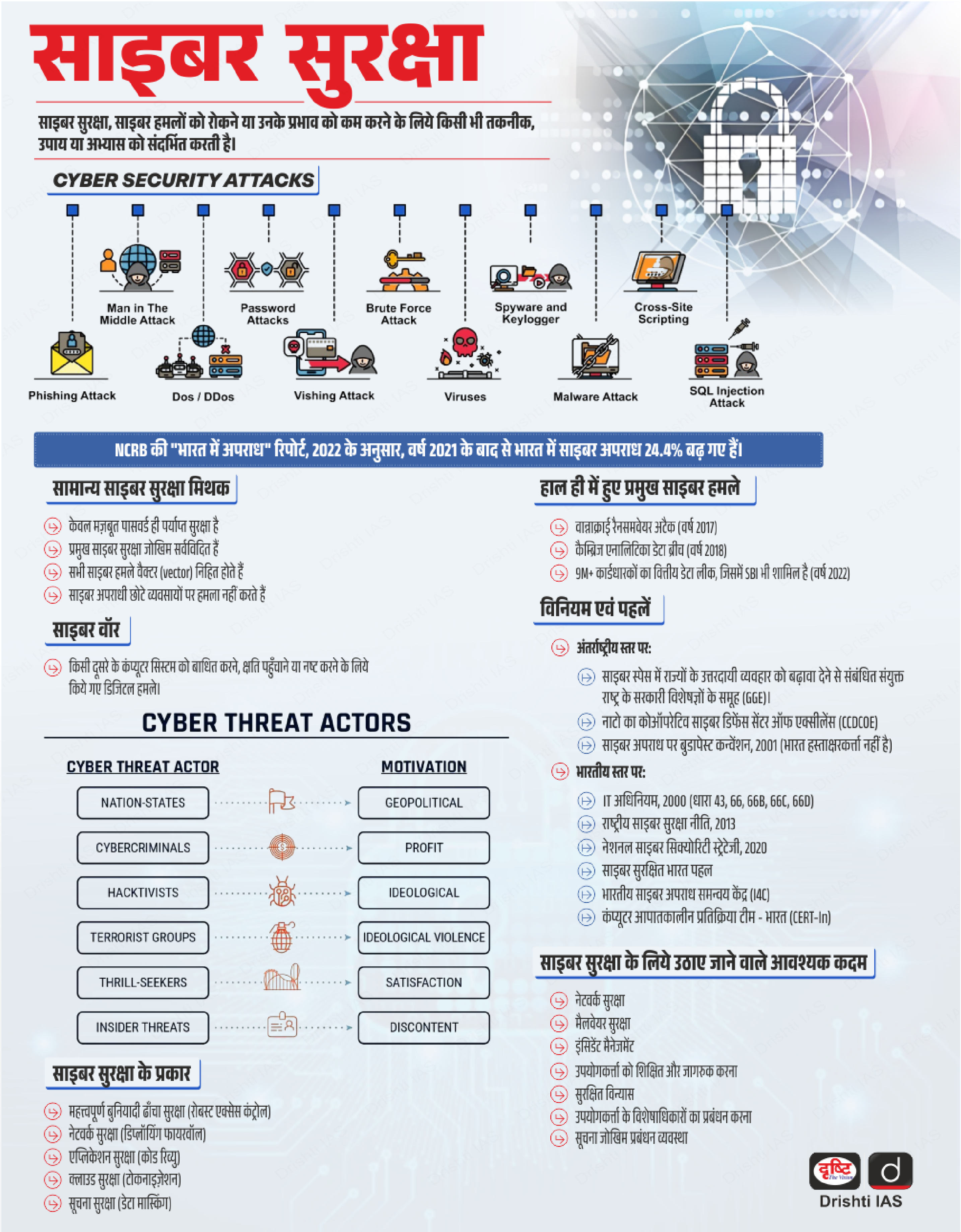
- **भू-राजनीतिक तनाव:** रूस-यूक्रेन युद्ध जैसे भू-राजनीतिक संघर्षों ने ऊर्जा, दूरसंचार और जल जैसे **महत्त्वपूर्ण क्षेत्रों पर साइबर और भौतिक हमलों** को बढ़ा दिया है।
  - लगभग **60% संगठनों** का कहना है कि **भू-राजनीतिक तनावों ने उनकी साइबर** सुरक्षा रणनीति को प्रभावित किया है।



- **जैव सुरक्षा संबंधी खतरे:** कृत्रिम बुद्धिमत्ता (AI), आनुवंशिक इंजीनियरिंग और जैव प्रौद्योगिकी में प्रगति ने **जैव सुरक्षा जोखिमों को बढ़ा दिया** है, जैव प्रयोगशालाओं पर साइबर हमलों से **अनुसंधान और सुरक्षा प्रोटोकॉल** को खतरा हो रहा है।
  - विश्व स्वास्थ्य संगठन (WHO) ने इन जोखिमों के बारे में चेतावनी जारी की है। जैसा कि **वर्ष 2024 में दक्षिण अफ्रीका और ब्रिटेन में प्रयोगशालाओं** पर होने वाले हमलों से स्पष्ट है।
- **साइबर सुरक्षा कौशल अंतराल (Cybersecurity Skills Gap):** रिपोर्ट में एक **महत्त्वपूर्ण साइबर सुरक्षा कौशल अंतराल पर प्रकाश डाला गया है**। विश्व में 4.8 मिलियन पेशेवरों में आवश्यक योग्यताओं का अभाव है।
  - दो-तिहाई संगठनों को उल्लेखनीय कौशल अंतराल का सामना करना पड़ रहा है, जिनमें से केवल 14% के पास वर्तमान साइबर परिदृश्य के लिये **आवश्यक कुशल कार्मिक** हैं।
- **साइबर के अनुकूल: 35% छोटे संगठनों का** मानना है कि उनकी **साइबर अनुकूलता** अपर्याप्त है।
  - **सार्वजनिक क्षेत्र के संगठनों को** अधिक चुनौतियों का सामना करना पड़ रहा है, जिनमें से **38% ने कम लचीलेपन की रिपोर्ट दी है** और 49% में साइबर सुरक्षा प्रतिभा की कमी है, जो 2024 की तुलना में 33% की वृद्धि है।
- **क्षेत्रीय साइबर सुरक्षा असमानताएँ:**
  - रिपोर्ट में वैश्विक साइबर सुरक्षा असमानताओं पर प्रकाश डाला गया है, जिसमें **घटना प्रतिक्रिया में विश्वसनीय यूरोप/उत्तरी अमेरिका में 15% से बढ़कर अफ्रीका में 36% और लैटिन अमेरिका** में 42% हो गया है।

- **साइबर अपराध के कारण नुकसान:** साइबर अपराध के कारण नुकसान: कम परिचालन व्यय और उच्च रिटर्न की संभावना के साथ, साइबर अपराध एक बहुत ही आकर्षक व्यवसाय बन गया है।
- अमेरिकी **संघीय जांच ब्यूरो (FBI)** का अनुमान है कि वर्ष 2023 में साइबर अपराध से होने वाला नुकसान **12.5 बिलियन अमेरिकी डॉलर** से अधिक हो जाएगा।

दृष्टि The Vision



साइबर सुरक्षा

साइबर सुरक्षा, साइबर हमलों को रोकने या उनके प्रभाव को कम करने के लिये किसी भी तकनीक, उपाय या अभ्यास को संदर्भित करती है।

CYBER SECURITY ATTACKS

- Phishing Attack
- Man in The Middle Attack
- Dos / DDos
- Password Attacks
- Vishing Attack
- Brute Force Attack
- Viruses
- Spyware and Keylogger
- Malware Attack
- Cross-Site Scripting
- SQL Injection Attack

NCRB की "भारत में अपराध" रिपोर्ट, 2022 के अनुसार, वर्ष 2021 के बाद से भारत में साइबर अपराध 24.4% बढ़ गए हैं।

सामान्य साइबर सुरक्षा मिथक

- केवल मज़बूत पासवर्ड ही पर्याप्त सुरक्षा है
- प्रमुख साइबर सुरक्षा जोखिम सर्वविदित हैं
- सभी साइबर हमले वैक्टर (vector) निहित होते हैं
- साइबर अपराधी छोटे व्यवसायों पर हमला नहीं करते हैं

साइबर वॉर

- किसी दूसरे के कंप्यूटर सिस्टम को बाधित करने, क्षति पहुँचाने या नष्ट करने के लिये किये गए डिजिटल हमले।

CYBER THREAT ACTORS

CYBER THREAT ACTOR	MOTIVATION
NATION-STATES	GEOPOLITICAL
CYBERCRIMINALS	PROFIT
HACKTIVISTS	IDEOLOGICAL
TERRORIST GROUPS	IDEOLOGICAL VIOLENCE
THRILL-SEEKERS	SATISFACTION
INSIDER THREATS	DISCONTENT

साइबर सुरक्षा के प्रकार

- महत्त्वपूर्ण बुनियादी ढाँचा सुरक्षा (रोबस्ट एक्सेस कंट्रोल)
- नेटवर्क सुरक्षा (डिप्लॉयिंग फायरवॉल)
- एप्लिकेशन सुरक्षा (कोड रिव्यु)
- क्लाउड सुरक्षा (टोकनाइज़ेशन)
- सूचना सुरक्षा (डेटा मास्किंग)

हाल ही में हुए प्रमुख साइबर हमले

- वान्नाक्राई रैनसमवेयर अटैक (वर्ष 2017)
- कैम्ब्रिज एनालिटिका डेटा ब्रीच (वर्ष 2018)
- 9M+ कार्डधारकों का वित्तीय डेटा लीक, जिसमें SBI भी शामिल है (वर्ष 2022)

विनियम एवं पहलें

- **अंतर्राष्ट्रीय स्तर पर:**
  - साइबर स्पेस में राज्यों के उत्तरदायी व्यवहार को बढ़ावा देने से संबंधित संयुक्त राष्ट्र के सरकारी विशेषज्ञों के समूह (GGE)।
  - नाटो का कोऑपरेटिव साइबर डिफेंस सेंटर ऑफ एक्सीलेंस (CCDCOE)
  - साइबर अपराध पर बुडापेस्ट कन्वेंशन, 2001 (भारत हस्ताक्षरकर्त्ता नहीं है)
- **भारतीय स्तर पर:**
  - IT अधिनियम, 2000 (धारा 43, 66, 66B, 66C, 66D)
  - राष्ट्रीय साइबर सुरक्षा नीति, 2013
  - नेशनल साइबर सिक्योरिटी स्ट्रेटेजी, 2020
  - साइबर सुरक्षित भारत पहल
  - भारतीय साइबर अपराध समन्वय केंद्र (I4C)
  - कंप्यूटर आपातकालीन प्रतिक्रिया टीम - भारत (CERT-In)

साइबर सुरक्षा के लिये उठाए जाने वाले आवश्यक कदम

- नेटवर्क सुरक्षा
- मैलवेयर सुरक्षा
- इंसिडेंट मैनेजमेंट
- उपयोगकर्त्ता को शिक्षित और जागरुक करना
- सुरक्षित विन्यास
- उपयोगकर्त्ता के विशेषाधिकारों का प्रबंधन करना
- सूचना जोखिम प्रबंधन व्यवस्था

Drishti IAS

आगे की राह:

- **साइबर सुरक्षा में रणनीतिक निवेश:** वैश्विक **साइबर सुरक्षा परिदृश्य 2025 में साइबर सुरक्षा में रणनीतिक निवेश** का आह्वान किया गया है, **तथा** सरकारों से **पुरानी प्रणालियों का आधुनिकीकरण करने, परिचालन प्रौद्योगिकियों** को उन्नत करने तथा जल, ऊर्जा और जैव **सुरक्षा जैसे महत्त्वपूर्ण क्षेत्रों** को बढ़ते खतरों से बचाने का आग्रह किया गया है।
- **कोस्टा रिका पर वर्ष 2022 के साइबर हमलों** ने साइबर सुरक्षा को भविष्य के लिये **एक महत्त्वपूर्ण निवेश के रूप में देखने** की आवश्यकता पर प्रकाश डाला है, न कि केवल एक व्यय के रूप में।
- **प्रतिस्पर्द्धा व्यावसायिक प्राथमिकताओं के साथ साइबर सुरक्षा में निवेश को संतुलित करना** महत्त्वपूर्ण है।
- **सार्वजनिक-निजी सहयोग: खतरे की खुफिया जानकारी साझा करने, सुरक्षित प्रौद्योगिकियों को विकसित करने तथा साइबर सुरक्षा अनुकूलता बढ़ाने के लिये सार्वजनिक-निजी सहयोग महत्त्वपूर्ण है।**
- इसके अलावा, लघु और मध्यम उद्यमों (SME) को मज़बूत सरकारी प्रोत्साहन के बिना साइबर सुरक्षा में निवेश करना चुनौतीपूर्ण लग सकता है।
- **साइबर सुरक्षा कौशल में निवेश: उभरते** साइबर खतरों का मुकाबला करने के लिये कुशल प्रतिभा पूल बनाने हेतु **विशेष प्रशिक्षण कार्यक्रमों** का विस्तार करने**,** प्रमाणपत्र प्रदान करने और **कार्यबल विकास को प्रोत्साहित करने की** आवश्यकता है ।
- **रोकथाम की बजाय लचीलेपन पर ध्यान केंद्रित करना:** उभरते साइबर खतरों के मद्देनजर, राष्ट्रों को त्वरित प्रतिक्रिया तंत्र को बढ़ाकर, संकट प्रबंधन ढाँचे की स्थापना करके, तथा हमलों के दौरान आवश्यक सेवाओं की निरंतरता सुनिश्चित करके लचीलेपन को प्राथमिकता देनी चाहिये।
- **अंतर्राष्ट्रीय सहयोग:** सीमाहीन साइबर खतरों से निपटने के लिये, राष्ट्रों को साइबर सुरक्षा मानकों को स्थापित करने के लिये संयुक्त राष्ट्र (UN) **और** G-20 जैसे मंचों के माध्यम से सहयोग करना चाहिये, जबकि **विकसित देशों को उभरती अर्थव्यवस्थाओं को उनके साइबर सुरक्षा ढाँचे को मज़बूत करने** और साइबर हमलों के खिलाफ लचीलापन बढ़ाने में **सहायता** करनी चाहिये।

भारत में साइबर सुरक्षा के लिये वर्तमान रूपरेखा क्या है?

- **विधायी उपाय:**
    - सूचना प्रौद्योगिकी अधिनियम, 2000 (IT अधिनियम)
    - डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023
- **संस्थागत ढाँचा:**
    - भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In)
    - राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC)
    - भारतीय साइबर अपराध समन्वय केंद्र (I4C)
    - साइबर स्वच्छता केंद्र
- **रणनीतिक पहल:**
    - भारत राष्ट्रीय साइबर सुरक्षा अभ्यास 2024
    - **राष्ट्रीय साइबर सुरक्षा नीति, 2013:** साइबरस्पेस को सुरक्षित करने और महत्त्वपूर्ण सूचना अवसंरचना की रक्षा के लिये दृष्टिकोण और रणनीति प्रदान करती है।
- **क्षेत्र-विशिष्ट विनियम:**
    - **सेबी विनियमित संस्थाओं के लिये साइबर सुरक्षा ढाँचा:** प्रतिभूति बाज़ारों के लिये साइबर सुरक्षा नीतियों को अनिवार्य बनाता है।
    - दूरसंचार (महत्त्वपूर्ण दूरसंचार अवसंरचना) नियम, 2024

दृष्टि The Vision

निष्कर्ष

ग्लोबल साइबरसिक्यूरिटी आउटलुक 2025 में महत्त्वपूर्ण बुनियादी ढाँचे के लिये बढ़ते साइबर खतरों पर प्रकाश डाला गया है, तथा रणनीतिक निवेश, अंतर्राष्ट्रीय सहयोग और मज़बूत साइबर सुरक्षा ढाँचे की आवश्यकता पर बल दिया गया है। जैसे-जैसे साइबर खतरे विकसित होते हैं, राष्ट्रों को राष्ट्रीय सुरक्षा, सार्वजनिक सुरक्षा और आर्थिक स्थिरता सुनिश्चित करने के लिये महत्त्वपूर्ण बुनियादी ढाँचे की सुरक्षा को प्राथमिकता देनी चाहिये।

दृष्टि मेन्स प्रश्न:

प्रश्न: डिजिटल युग में भारत के सामने आने वाली प्रमुख साइबर सुरक्षा चुनौतियों पर चर्चा कीजिये और महत्त्वपूर्ण बुनियादी ढाँचे की सुरक्षा के लिये अपने साइबर सुरक्षा ढाँचे को बढ़ाने के उपायों का सुझाव दीजिये।

UPSC सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न

?????????

प्रश्न. भारत में, किसी व्यक्ति के साइबर बीमा कराने पर, निधि की हानि की भरपाई एवं अन्य लाभों के अतिरिक्त निम्नलिखित में से कौन-कौन से लाभ दिये जाते हैं? (2020)

1. यदि कोई किसी मैलवेयर कंप्यूटर तक उसकी पहुँच को बाधित कर देता है तो कंप्यूटर प्रणाली को पुनः प्रचालित करने में लगने वाली लागत
2. यदि यह प्रमाणित हो जाता है कि किसी शरारती तत्त्व द्वारा जानबूझ कर कंप्यूटर को नुकसान पहुँचाया गया है तो एक नए कंप्यूटर की लागत

3. यदि साइबर बलात्-ग्रहण होता है तो इस हानि को न्यूनतम करने के लिये विशेष परामर्शदाता की की सेवाएँ पर लगने वाली लागत
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव करने में लगने वाली लागत

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1, 2 और 4
(b) केवल 1, 3 और 4
(c) केवल 2 और 3
(d) 1, 2, 3 और 4

उत्तर: (b)

प्रश्न. भारत में साइबर सुरक्षा घटनाओं पर रिपोर्ट करना निम्नलिखित में से किसके/किनके लिये विधितः अधिदेशात्मक है? (2017)

1. सेवा प्रदाता
2. डेटा सेंटर
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)

?????

प्रश्न. साइबर सुरक्षा के विभिन्न तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतियों को ध्यान में रखते हुए समीक्षा कीजिये कि भारत ने किस हद तक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक विकसित की है। (2022)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/global-cybersecurity-outlook-2025