भारत के लिये एक अनुकूल साइबर सुरक्षा ढाँचा

प्रिलिम्स के लिये: डिजिटिल थ्रेट्स, आर्टिफिशियल इंटेलिजेंस, डीप फेक, वानाक्राई रैंसमवेयर अटैक, फिशिंग, इंटरनेट ऑफ थिंग्स, राष्ट्रीय साइबर सुरक्षा नीति, भारतीय साइबर अपराध समन्वय केंद्र, कंप्यूटर आपातकालीन प्रतिक्रिया टीम- भारत, साइबर स्वच्छता केंद्र, डिजिटिल व्यक्तिगत डेटा संरक्षण अधिनियम 2023।

मेन्स के लिये: भारत के समक्ष वर्तमान प्रमुख साइबर खतरे, भारत में साइबर सुरक्षा से संबंधित प्रमुख सरकारी पहल।

स्रोत: ET

चर्चा में क्यों?

गृह मामलों की **संसदीय स्थायी समिति** ने भारत में **बढ़ते साइबर खतरों** को रेखांकित किया तथा **इंटरनेट पहुँच और ऑनलाइन लेनदेन में तेज़ी** से हो रहे विस्तार के मद्देनजर अधिक जन जागरूकता, **बेहतर साइबर सुरक्षा और मज़बूत डिजिटिल सुरक्षा** की मांग की।

भारत के समक्ष प्रमुख साइबर खतरे क्या हैं?

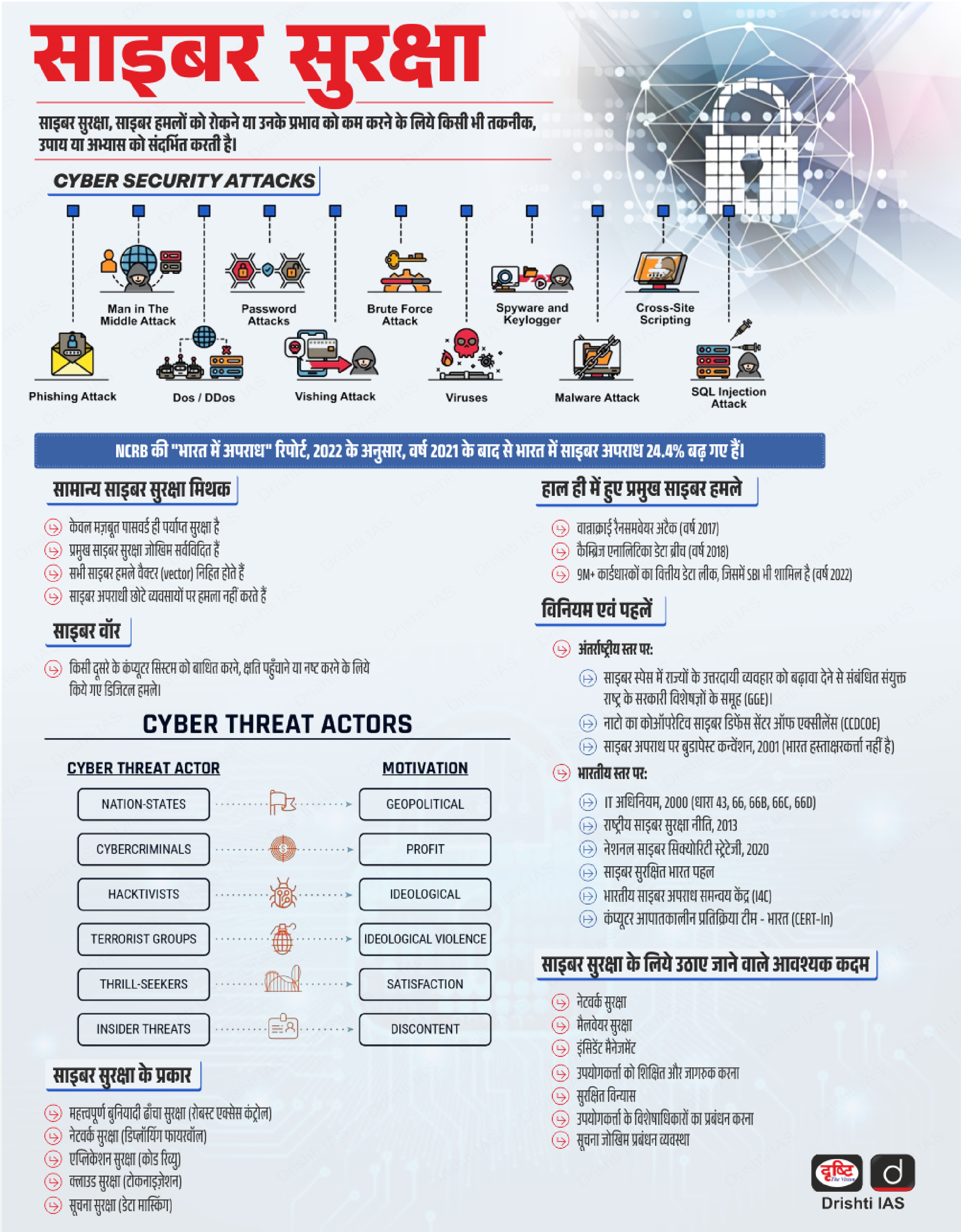
- **साइबर-सक्षम वित्तीय धोखाधड़ी: भारत में फिशिंग, रैनसमवेयर, पहचान की चोरी, यूपीआई और ऑनलाइन बैंकिंग धोखाधड़ी** में वृद्धि देखी जा रही है।
  - वर्ष 2024 में, देश में **1.91 मिलियन साइबर अपराध** से संबंधित शिकायतें दर्ज की गईं, जो डिजिटिल वित्तीय भेद्यता के पैमाने को दर्शाती हैं।
- **रैनसमवेयर और मैलवेयर हमले: अस्पताल, सरकारी डेटाबेस और महत्त्वपूर्ण निजी उद्यम** रैनसमवेयर और मैलवेयर के प्रमुख लक्ष्य हैं।
  - **AIIMS दिल्ली साइबर हमले (2022)** ने स्वास्थ्य और सार्वजनिक सेवा प्रणालियों की कमज़ोरी को उजागर कर दिया।
- **महत्वपूर्ण अवसंरचना की भेद्यता:** पावर ग्रिड, दूरसंचार नेटवर्क, परमाणु सुविधाएँ और बंदरगाह जैसे रणनीतिक परिसंपत्तियाँ लगातार साइबर खतरों का सामना कर रही हैं।
  - **कुडनकुलम परमाणु ऊर्जा संयंत्र पर 2019** का हमला राष्ट्रीय सुरक्षा के जोखिमों को उजागर करता है।
- **डेटा उल्लंघन और गोपनीयता जोखिम: सरकारी और निजी क्षेत्र के डेटाबेस** में लगातार साइबर घुसपैठ के कारण बड़े पैमाने पर **व्यक्तिगत डेटा** लीक हुआ है।
  - **एयर इंडिया उल्लंघन (2021) में** लगभग **4.5 मिलियन यात्रियों** की जानकारी से समझौता किया गया।
- **डीपफेक और गलत सूचना:** AI-संचालित **डीपफेक सामग्री और फर्जी न्यूज़** अभियान सामाजिक सामंजस्य, लोकतांत्रिक संस्थाओं और चुनावी अखंडता के लिये खतरा हैं।
  - वर्ष 2024 के चुनाव **अभियान** में राजनीतिक नेताओं के **डीपफेक वीडियो व्यापक रूप से प्रसारित** हुए।
- **डार्क वेब और साइबर आतंकवाद: डार्क वेब का इस्तेमाल कट्टरपंथ, अवैध हथियारों/नशीले पदार्थों** के व्यापार और क्रिप्टोकरेंसी के ज़रिये आतंकवाद के वित्तपोषण के लिये तेज़ी से किया जा रहा है। ऐसे गुप्त नेटवर्क भारत में **संगठित अपराध और साइबर आतंकवाद** को बढ़ावा देते हैं।

भारत के साइबर सुरक्षा ढाँचे की प्रभावशीलता को कौन-से कारक कमज़ोर कर रहे हैं?

- **अपर्याप्त कानूनी और नियामक ढाँचा: आईटी अधिनियम, 2000** और **डिजिटिल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023** जैसे मौजूदा कानूनों में **AI-सक्षम हमलों और डीपफेक** जैसे उभरते खतरों के लिये विशिष्ट प्रावधानों का अभाव है।
- **कुशल साइबर सुरक्षा पेशेवरों की कमी:** भारत को वास्तविक समय में खतरों की निगरानी और प्रतिक्रिया करने के लिये **प्रशिक्षित साइबर सुरक्षा विशेषज्ञों की भारी कमी** का सामना करना पड़ रहा है।
  - **नैसकॉम** की एक रिपोर्ट में कहा गया है कि भारत को **कम-से-कम दस लाख साइबर सुरक्षा पेशेवरों** की आवश्यकता है, लेकिन वर्तमान में **इसकी संख्या आधी** से भी कम है।
- **तेजी से डिजिटिलाइजेशन और कम साइबर जागरूकता:** जैसे-जैसे भारत का डिजिटिल पारिस्थितिकी तंत्र तेजी से विस्तार कर रहा है, साइबर खतरों

का पैमाना और उनकी जटलिता भी समान रूप से बढ़ रही है।

- इसके अलावा, भारत में नागरकिों के बीच कमजोर साइबर हाइजीन है, जहाँ कई उपयोगकर्त्ता **फशिगि हमलों, धोखाधड़ी वाली वेबसाइटों और ठगी कॉल** को पहचानने में असफल रहते हैं, जबकि ग्रामीण क्षेत्रों में सीमति **डजिटिल साक्षरता कार्यक्रम साइबर धोखाधड़ी** के प्रति संवेदनशीलता को और बढ़ा देते हैं।
- **महत्त्वपूर्ण बुनियादी ढाँचे की कमज़ोर सुरक्षा:** पुराने सुरक्षा प्रोटोकॉल के कारण पावर ग्रडि, दूरसंचार नेटवर्क और परमाणु संयंत्र असुरक्षति बने हुए हैं।
    - साथ ही, **भारत में लघु एवं मध्यम उद्यम (SMEs) और महत्त्वपूर्ण क्षेत्रों में मज़बूत सुरक्षा** का अभाव है, तथा आयातति आईटी/दूरसंचार उपकरणों पर नरि्भरता से **अंतर्नहिति कमज़ोरियों** का जोखमि बढ़ जाता है।
- **एजेंसियों के बीच समन्वय का अभाव: CERT-In**, **राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC)** और नजिी हतिधारकों जैसी कई एजेंसियाँ सीमति समन्वय के साथ कार्य करती हैं, जसिके कारण **खतरे का पता लगाने और प्रतक्रियिा** में देरी होती है।



साइबर सुरक्षा बढ़ाने से संबंधित प्रमुख पहल क्या हैं?

- **वधिायी उपाय:**
    - [सूचना प्रौद्योगिकी अधिनियम, 2000 (आईटी अधिनियम)]
    - [डिजिटिल व्यक्तिगत डेटा संरक्षण अधिनियम, 2023]
- **संस्थागत ढाँचा:**
    - [भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (CERT-In)]
    - [राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी)]
    - [भारतीय साइबर अपराध समन्वय केंद्र (I4C)]
    - [साइबर स्वच्छता केंद्र]
    - [नागरिक वित्तीय साइबर धोखाधड़ी रिपोर्टिंग और प्रबंधन प्रणाली]
- **रणनीतिक पहल:**
    - [भारत राष्ट्रीय साइबर सुरक्षा अभ्यास 2024]
    - [राष्ट्रीय साइबर सुरक्षा नीति, 2013]
    - [डिजिटिल इंटेलिजेंस प्लेटफॉर्म और चक्षु]
    - [दूरसंचार (महत्त्वपूर्ण दूरसंचार अवसंरचना) नियम, 2024]

भारत में साइबर सुरक्षा ढाँचे को मज़बूत करने के लिये क्या उपाय अपनाए जाने चाहिये?

- **कानूनी एवं विनियामक ढांचे को मजबूत करना: सूचना प्रौद्योगिकी अधिनियम, 2000** में तत्काल संशोधन की आवश्यकता है ताकि एआई, डीपफेक और रैनसमवेयर जैसे खतरों को कवर किया जा सके।
    - ***⍰⍰⍰⍰⍰⍰⍰ व्यक्तिगत ⍰⍰⍰⍰ ⍰⍰⍰⍰⍰⍰⍰⍰ ⍰⍰⍰⍰⍰⍰⍰⍰, 2023*** का प्रवर्तन और स्पष्ट जवाबदेही के साथ कार्यान्वयन आवश्यक है।
- **संस्थागत एवं ऑडिट सुधार:** बैंकिंग, स्वास्थ्य सेवा और उपयोगिता सेवाओं जैसे **महत्त्वपूर्ण क्षेत्रों** में **साइबर सुरक्षा ऑडिट और स्ट्रेस टेस्ट** अनिवार्य किये जाएँ।
    - **स्थानीय स्तर पर खतरे के प्रबंधन के लिये ज़िला-स्तरीय साइबर सुरक्षा** इकाइयों की स्थापना करना और **CERT-In** के साथ समन्वय को मज़बूत करना।
- **महत्त्वपूर्ण अवसंरचना को सुदृढ़ करना:** बैंकों जैसे महत्त्वपूर्ण क्षेत्रों में **दो-स्तरीय प्रमाणीकरण (2FA), डेटा एन्क्रिप्शन और वास्तविक समय निगरानी प्रणाली** को लागू करना।
    - भारत को महत्वपूर्ण क्षेत्रों में ***⍰⍰⍰⍰⍰⍰-⍰⍰⍰⍰⍰⍰⍰ ⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰⍰*** को बढ़ावा देना चाहिये (सिर्फ परिधि सुरक्षा की बजाय निरंतर सत्यापन पर ज़ोर)।
- **स्वदेशी साइबर सुरक्षा समाधान को बढ़ावा देना:** भारत को विदेशी निर्भरता कम करने के लिये ***⍰⍰⍰ ⍰⍰ ⍰⍰⍰⍰⍰⍰*** **साइबर** सुरक्षा उपकरणों को बढ़ावा देना चाहिये। एआई-आधारित खतरे की पहचान विकसित करने वाले **स्टार्टअप्स को फंडिंग और इनक्यूबेशन** के माध्यम से समर्थन दिया जाना चाहिये।
- **साइबर हाइजीन और जागरूकता में सुधार:** ग्रामीण समुदायों, युवाओं और वरिष्ठ नागरिकों को लक्षित करते हुए क्षेत्रीय भाषाओं में **राष्ट्रीय स्तर पर साइबर साक्षरता अभियान** शुरू करना।
    - स्कूलों और विश्वविद्यालयों में साइबर सुरक्षा शिक्षा को शामिल करना, जिसे **सुरक्षित अवसंरचना और स्टाफ प्रशिक्षण** द्वारा समर्थित किया जाए, ताकि प्रारंभिक स्तर से ही डिजिटिल अनुकूलता विकसित किया जा सके।

निष्कर्ष:

भारत में **साइबर खतरों का दायरा अब केवल वित्तीय धोखाधड़ी** तक सीमित नहीं है, बल्कि यह **राष्ट्रीय सुरक्षा, गोपनीयता और लोकतांत्रिक अखंडता** तक पहुँच गया है। शासन और अर्थव्यवस्था के तीव्र डिजिटिलाइज़ेशन के साथ, भारत की रैनसमवेयर, डेटा उल्लंघन, डीपफेक और महत्त्वपूर्ण अवसंरचना पर बाधा जैसे खतरों के प्रति संवेदनशीलता कई गुना बढ़ गई है। भारत के **साइबर स्पेस** को सुरक्षित करने और इसके विकास पथ की रक्षा करने के लिये मज़बूत साइबर कानून, संस्थागत क्षमता, जन जागरूकता और **वैश्विक सहयोग से जुड़ा एक बहुआयामी दृष्टिकोण** आवश्यक है।

दृष्टि मुख्य परीक्षा प्रश्न:

प्रश्न. भारत के बढ़ते डिजिटिल पदचिह्न के साथ, साइबर सुरक्षा खतरों ने राष्ट्रीय सुरक्षा, अर्थव्यवस्था और शासन के लिये एक प्रमुख चुनौती का रूप ले लिया है। इन खतरों की प्रकृति की जाँच कीजिये और भारत के साइबर सुरक्षा ढाँचे को मज़बूत करने के लिये एक व्यापक रणनीति सुझाइये।

UPSC सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न (PYQ)

प्रिलिम्स:

प्रश्न. भारत में व्यक्तियों के लिये साइबर बीमा के तहत धन की हानि और अन्य लाभों के भुगतान के अलावा, निम्नलिखित में से कौन से लाभ आम तौर पर कवर किये जाते हैं? (वर्ष 2020)

1. किसी के कंप्यूटर तक पहुँच को बाधित करने वाले मैलवेयर के मामले में कंप्यूटर सिस्टम की बहाली की लागत।
2. एक नए कंप्यूटर की लागत अगर ऐसा साबित हो जाता है कि कुछ असामाजिक तत्त्वों ने जानबूझकर इसे नुकसान पहुँचाया है।
3. साइबर जबरन वसूली के मामले में नुकसान को कम करने के लिए एक विशेष सलाहकार को काम पर रखने की लागत।
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव की 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 निम्नलिखित में से किसके लिये साइबर सुरक्षा घटनाओं पर रिपोर्ट करना कानूनी रूप से अनिवार्य है? (वर्ष 2017)

1. सेवा प्रदाता
2. डेटा केंद्र
3. निगमित 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 घटक क्या हैं? साइबर सुरक्षा में चुनौतियों को ध्यान में रखते हुए जाँच करें कि भारत ने व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति को किस हद तक सफलतापूर्वक विकसित किया है। (वर्ष 2022)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/building-a-resilient-cybersecurity-framework-for-india