भारत के लिये एक अनुकूल साइबर सुरक्षा ढाँचा

प्रलिमि्स के लिये: डिजिटिल थ्रेट्स, आर्टफिशियिल इंटेलजिंस, डीप फेक, वानाक्राई रैंसमवेयर अटैक, फशिगि, इंटरनेट ऑफ थगि्स, राष्ट्रीय साइबर सुरक्षा नीति, भारतीय साइबर अपराध समन्वय केंद्र, कंप्यूटर आपातकालीन प्रतक्रियिा टीम- भारत, साइबर स्वच्छता केंद्र, डिजिटिल व्यक्तगित डेटा संरक्षण अधनियिम 2023।

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

स्रोत: ET

चर्चा में क्यों?

गृह मामलों की **संसदीय स्थायी समति** ने भारत में **बढ़ते साइबर खतरों** को रेखांकति कयिा तथा **इंटरनेट पहुँच और ऑनलाइन लेनदेन में तेज़ी** से हो रहे वसि्तार के मद्देनजर अधकि जन जागरूकता, **बेहतर साइबर सुरक्षा और मज़बूत डिजिटिल सुरक्षा** की मांग की।

भारत के समक्ष प्रमुख साइबर खतरे क्या हैं?

- **साइबर-सक्षम वत्तिीय धोखाधड़ी: भारत में फशिगि, रैनसमवेयर, पहचान की चोरी, यूपीआई और ऑनलाइन बैंकगि धोखाधड़ी** में वृद्धि देखी जा रही है।
  - वर्ष 2024 में, देश में **1.91 मलियिन साइबर अपराध** से संबंधति शकियतें दर्ज की गईं, जो डिजिटिल वत्तिीय भेद्यता के पैमाने को दर्शाती हैं।
- **रैनसमवेयर और मैलवेयर हमले: अस्पताल, सरकारी डेटाबेस और महत्त्वपूर्ण नजिी उद्यम** रैनसमवेयर और मैलवेयर के प्रमुख लक्ष्य हैं।
  - **AIIMS दल्लिी साइबर हमले (2022)** ने स्वास्थ्य और सार्वजनकि सेवा प्रणालयिों की कमज़ोरी को उजागर कर दयिा।
- **महत्वपूर्ण अवसंरचना की भेद्यता:** पावर ग्रडि, दूरसंचार नेटवर्क, परमाणु सुवधिाएँ और बंदरगाह जैसे रणनीतकि परसिंपत्तयिाँ लगातार साइबर खतरों का सामना कर रही हैं।
  - **कुडनकुलम परमाणु ऊर्जा संयंत्र पर 2019** का हमला राष्ट्रीय सुरक्षा के जोखमिों को उजागर करता है।
- **डेटा उल्लंघन और गोपनीयता जोखमि: सरकारी और नजिी क्षेत्र के डेटाबेस** में लगातार साइबर घुसपैठ के कारण बड़े पैमाने पर **व्यक्तगित डेटा** लीक हुआ है।
  - **एयर इंडयिा उल्लंघन (2021) में** लगभग **4.5 मलियिन यात्रयिों** की जानकारी से समझौता कयिा गया।
- **डीपफेक और गलत सूचना:** AI-संचालति **डीपफेक सामग्री और फर्जी न्यूज़** अभयिान सामाजकि सामंजस्य, लोकतांत्रकि संस्थाओं और चुनावी अखंडता के लिये खतरा हैं।
  - वर्ष 2024 के चुनाव **अभयिान** में राजनीतकि नेताओं के **डीपफेक वीडयिो व्यापक रूप से प्रसारति** हुए।
- **डार्क वेब और साइबर आतंकवाद: डार्क वेब का इस्तेमाल कट्टरपंथ, अवैध हथयिारों/नशीले पदार्थों** के व्यापार और क्रप्टिोकरेंसी के ज़रयि आतंकवाद के वत्तिपोषण के लिये तेज़ी से कयिा जा रहा है। ऐसे गुप्त नेटवर्क भारत में **संगठति 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 नयिामक ढाँचा: आईटी अधनियिम, 2000** और **डिजिटिल व्यक्तगित डेटा संरक्षण अधनियिम, 2023** जैसे मौजूदा कानूनों में **AI-सक्षम हमलों और डीपफेक** जैसे उभरते खतरों के लिये वशिष्ट प्रावधानों का अभाव है।
- **कुशल साइबर सुरक्षा पेशेवरों की कमी:** भारत को वास्तवकि समय में खतरों की नगिरानी और प्रतक्रियिा करने के लिये **प्रशक्षिति साइबर सुरक्षा वशिषज्ञों की भारी कमी** का सामना करना पड़ रहा है।
  - **नैसकॉम** की एक रपिोर्ट में कहा गया है कि भारत को **कम-से-कम दस लाख साइबर सुरक्षा पेशेवरों** की आवश्यकता है, लेकनि वर्तमान में **इसकी संख्या आधी** से भी कम है।
- **तेजी से डिजिटिलाइजेशन और कम साइबर जागरूकता:** जैसे-जैसे भारत का डिजिटिल पारस्थितिकिी तंत्र तेजी से वसि्तार कर रहा है, साइबर खतरों

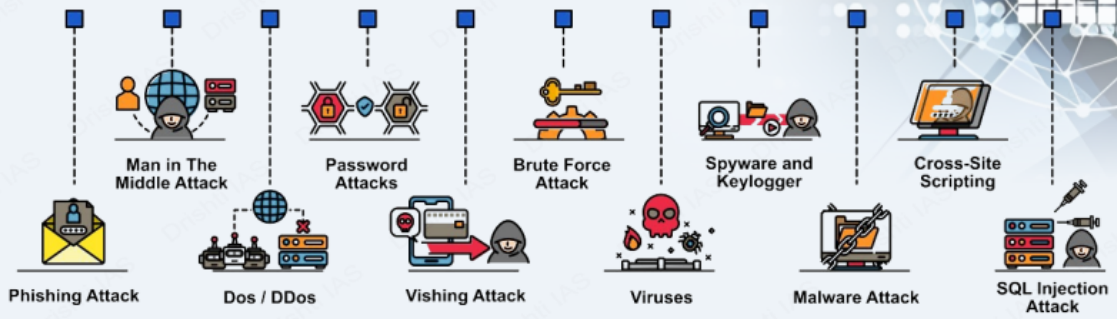
का पैमाना और उनकी जटिलता भी समान रूप से बढ़ रही है।

- इसके अलावा, भारत में नागरिकों के बीच कमजोर साइबर हाइजीन है, जहाँ कई उपयोगकर्त्ता **फिशिंग हमलों, धोखाधड़ी वाली वेबसाइटों और ठगी कॉल** को पहचानने में असफल रहते हैं, जबकि ग्रामीण क्षेत्रों में सीमित **डिजिटल साक्षरता कार्यक्रम साइबर धोखाधड़ी** के प्रति संवेदनशीलता को और बढ़ा देते हैं।
- **महत्त्वपूर्ण बुनियादी ढाँचे की कमज़ोर सुरक्षा:** पुराने सुरक्षा प्रोटोकॉल के कारण पावर ग्रिड, दूरसंचार नेटवर्क और परमाणु संयंत्र असुरक्षित बने हुए हैं।
    - साथ ही, **भारत में लघु एवं मध्यम उद्यम (SMEs) और महत्त्वपूर्ण क्षेत्रों में मज़बूत सुरक्षा** का अभाव है, तथा आयातित आईटी/दूरसंचार उपकरणों पर निर्भरता से **अंतर्निहित कमज़ोरियों** का जोखिम बढ़ जाता है।
- **एजेंसियों के बीच समन्वय का अभाव: CERT-In**, **राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC)** और निजी हितधारकों जैसी कई एजेंसियाँ सीमित समन्वय के साथ कार्य करती हैं, जिसके कारण **खतरे का पता लगाने और प्रतिक्रिया** में देरी होती है।

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



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 (डिफेंसिव फायरवॉल)
- एप्लिकेशन सुरक्षा (कोड रिव्यू)
- क्लाउड सुरक्षा (टोकनाइज़ेशन)
- सूचना सुरक्षा (डेटा मास्किंग)

हाल ही में हुए प्रमुख साइबर हमले

- वानाक्राई 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

साइबर सुरक्षा बढ़ाने से संबंधित प्रमुख पहल क्या हैं?

- **वधिायी उपाय:**
  - सूचना प्रौद्योगकिी अधनियिम, 2000 (आईटी अधनियिम)
  - डजिटिल व्यक्तगित डेटा संरक्षण अधनियिम, 2023
- **संस्थागत ढाँचा:**
  - भारतीय कंप्यूटर आपातकालीन प्रतकि्रयिा दल (CERT-In)
  - राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी)
  - भारतीय साइबर अपराध समन्वय केंद्र (I4C)
  - साइबर स्वच्छता केंद्र
  - नागरकि वत्तिीय साइबर धोखाधड़ी रपिोर्टगि और प्रबंधन प्रणाली
- **रणनीतकि पहल:**
  - भारत राष्ट्रीय साइबर सुरक्षा अभ्यास 2024
  - राष्ट्रीय साइबर सुरक्षा नीति, 2013
  - डजिटिल इंटेलजिेंस प्लेटफॉर्म और चक्षु
  - दूरसंचार (महत्त्वपूर्ण दूरसंचार अवसंरचना) नयिम, 2024

भारत में साइबर सुरक्षा ढाँचे को मज़बूत करने के लयि क्या उपाय अपनाए जाने चाहयि?

- **कानूनी एवं वनियिामक ढांचे को मजबूत करना: सूचना प्रौद्योगकिी अधनियिम, 2000** में तत्काल संशोधन की आवश्यकता है ताकि एआई, डीपफेक और रैनसमवेयर जैसे खतरों को कवर कयिा जा सके।
  - *[illegible]* **व्यक्तगित** *[illegible], 2023* का प्रवर्तन और स्पष्ट जवाबदेही के साथ कार्यान्वयन आवश्यक है।
- **संस्थागत एवं ऑडटि सुधार:** बैंकगि, स्वास्थ्य सेवा और उपयोगति सेवाओं जैसे **महत्त्वपूर्ण क्षेत्रों** में **साइबर सुरक्षा ऑडटि और स्ट्रेस टेस्ट** अनविार्य कयि जाएँ।
  - **स्थानीय स्तर पर खतरे के प्रबंधन के लयि 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 एन्क्रप्शिन और वास्तवकि समय नगिरानी प्रणाली** को लागू करना।
  - भारत को महत्वपूर्ण क्षेत्रों में *[illegible]* को बढ़ावा देना चाहयि (सरि्फ परधिि सुरक्षा की बजाय नरिंतर सत्यापन पर ज़ोर)।
- **स्वदेशी साइबर सुरक्षा समाधान को बढ़ावा देना:** भारत को वदिेशी नरि्भरता कम करने के लयि *[illegible]* **साइबर** सुरक्षा उपकरणों को बढ़ावा देना चाहयि। एआई-आधारति खतरे की पहचान वकिसति करने वाले **स्टार्टअप्स को फंडगि और इनक्यूबेशन** के माध्यम से समर्थन दयिा जाना चाहयि।
- **साइबर हाइजीन और जागरूकता में सुधार:** ग्रामीण समुदायों, युवाओं और वरषि्ठ नागरकिों को लक्षति करते हुए क्षेत्रीय भाषाओं में **राष्ट्रीय स्तर पर साइबर साक्षरता अभयिान** शुरू करना।
  - स्कूलों और वशि्ववद्यिालयों में साइबर सुरक्षा शक्षिा को शामलि करना, जसिे **सुरक्षति अवसंरचना और स्टाफ प्रशक्षिण** द्वारा समर्थति कयिा जाए, ताकि प्रारंभकि स्तर से ही डजिटिल अनुकूलता वकिसति कयिा जा सके।

नष्किर्ष:

भारत में **साइबर खतरों का दायरा अब केवल वत्तिीय धोखाधड़ी** तक सीमति नहीं है, बल्कि यह **राष्ट्रीय सुरक्षा, गोपनीयता और लोकतांत्रकि अखंडता** तक पहुँच गया है। शासन और अर्थव्यवस्था के तीव्र डजिटिलाइज़ेशन 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 सुरक्षति करने और इसके वकिास पथ की रक्षा करने के लयि मज़बूत साइबर कानून, संस्थागत क्षमता, जन जागरूकता और **वैश्वकि सहयोग से जुड़ा एक बहुआयामी दृष्टकिोण** आवश्यक है।

दृष्टि मुख्य परीक्षा प्रश्न:

प्रश्न. भारत के बढ़ते डजिटिल पदचहि्न के साथ, साइबर सुरक्षा खतरों ने राष्ट्रीय सुरक्षा, अर्थव्यवस्था और शासन के लयि एक प्रमुख चुनौती का रूप ले लयिा है। इन खतरों की प्रकृति की जाँच कीजयि और भारत के साइबर सुरक्षा ढाँचे को मज़बूत करने के लयि एक व्यापक रणनीति सुझाइये।

UPSC सविलि सेवा परीक्षा, वगित वर्ष के प्रश्न (PYQ)

प्रलिमि्स:

प्रश्न. भारत में व्यक्तयिों के लयि साइबर बीमा के तहत धन की हानि और अन्य लाभों के भुगतान के अलावा, नम्निलखिति में से कौन से लाभ आम तौर पर कवर कयि जाते हैं? (वर्ष 2020)

1. कसिी के कंप्यूटर तक पहुँच को बाधति करने वाले मैलवेयर के मामले में कंप्यूटर सस्टिम की बहाली की लागत।
2. एक नए कंप्यूटर की लागत अगर ऐसा साबति हो जाता है कि कुछ असामाजकि तत्त्वों ने जानबूझकर इसे नुकसान पहुँचाया है।
3. साइबर जबरन वसूली के मामले में नुकसान को कम करने के लिए एक वशिष सलाहकार को काम पर रखने की लागत।
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव की लागत

नीचे दयि गए कूट का प्रयोग कर सही उत्तर चुनयि:

(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 नम्निलखिति में से कसिके लयि साइबर सुरक्षा घटनाओं पर रपिोर्ट करना कानूनी रूप से अनविार्य है? (वर्ष 2017)

1. सेवा प्रदाता
2. डेटा केंद्र
3. नगिमति नकिाय

नीचे दयि गए कूट का प्रयोग कर सही उत्तर चुनयि:

(A) केवल 1
(B) केवल 1 और 2
(C) केवल 3
(D) 1, 2 और 3

उत्तर: (D)

??????:

प्रश्न: साइबर सुरक्षा के वभिन्नि घटक क्या हैं? साइबर सुरक्षा में चुनौतयिों को ध्यान में रखते हुए जाँच करें कि भारत ने व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति को कसि हद तक सफलतापूर्वक वकिसति कयि है। (वर्ष 2022)