

## पेगासस स्पाइवेयर एवं इसकी नगिरानी संबंधी चर्चाएँ

### प्रलिस के लिये:

पेगासस स्पाइवेयर, स्पाइवेयर, ज़ीरो-डे वलनरेबिलिटी, फशिगि, RTI, भारतीय टेलीग्राफ अधिनियम 1885, भारतीय टेलीग्राफ नियम 2007, IT अधिनियम 2000, इंटरसेप्शन नियम 2009, नजिता का अधिकार, अनुच्छेद 21, केएस पुट्टासवामी केस 2017, वाक और अभवियकता की स्वतंत्रता का अधिकार, संसदीय नरीक्षण, अनुच्छेद 32 और 226, सर्वोच्च न्यायालय, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम 2023, एंड-टू-एंड एनक्रिप्शन।

### मेन्स के लिये:

स्पाइवेयर एवं नजिता संबंधी चर्चाएँ, साइबर हमले।

स्रोत: इंडियन एक्सप्रेस

## चर्चा में क्यों?

पेगासस स्पाइवेयर द्वारा नगिरानी किये जाने से इसके दुरुपयोग को लेकर भारत सहित विश्व भर में विवाद को जन्म मिला है, जिससे नजिता एवं मूल अधिकारों से संबंधित गंभीर चर्चाएँ पैदा हुई हैं।

- हाल ही में एक अमेरिकी कोर्ट ने फैसला सुनाया कि पेगासस स्पाइवेयर ने भारत के 300 उपयोगकर्ताओं सहित 1,400 व्हाट्सएप उपयोगकर्ताओं की नगिरानी करके कंप्यूटर धोखाधड़ी एवं दुरुपयोग अधिनियम, 1986 का उल्लंघन किया है।

## पेगासस स्पाइवेयर क्या है?

### परिचय:

- पेगासस स्पाइवेयर को NSO ग्रुप (जो वर्ष 2010 में स्थापित एक इज़रायली साइबर सुरक्षा फर्म है) द्वारा विकसित किया गया है। यह डेटा पर नज़र रखने, बातचीत रिकॉर्ड करने, फोटो कैप्चर करने एवं ऐप डेटा तक पहुँचने के लिये iOS एवं एंड्रॉइड डेवाइस को हैक करने में सक्षम है।
- स्पाइवेयर एक दुरभावनापूर्ण सॉफ्टवेयर है जिससे उपयोगकर्ता की सहमति के बिना गुप्त रूप से डेवाइस पर नज़र रखने के साथ जानकारी एकत्र की जाती है।

### वशिष्टताएँ:

- उन्नत उपयोग:** इसके तहत iOS डेवाइसों को दूरस्थ रूप से जेलब्रेक करने के लिये ज़ीरो-डे वलनरेबिलिटी का उपयोग किया जाता है जबकि एंड्रॉइड संस्करण डेवाइसों की नगिरानी के लिये फ़रामारूट जैसे सॉफ्टवेयर का उपयोग किया जाता है।
  - ज़ीरो-डे वलनरेबिलिटी इस सॉफ्टवेयर में एक गुप्त सक्रियरटी फ़्ला है जिसके लिये कोई डफ़ेंस या पैच उपलब्ध नहीं है।
  - रूटिंग का आशय किसी डेवाइस को अनलॉक या जेलब्रेक करने की प्रक्रिया है जैसे कि स्मार्टफोन या टैबलेट, ताकि इस पर नियंत्रण प्राप्त किया जा सके।
- इनवज़िबिलिटी:** इसका कार्य गोपनीय है तथा फशिगि लिकि पर क्लिक करने के बाद ब्राउज़र बंद होने के अलावा इसका कोई भी स्पष्ट संकेत दिखाई नहीं देता है।

### पेगासस क्लाइट और संबंधित विवाद:

- NSO समूह के अनुसार, पेगासस का उपयोग विश्व भर की सरकारों तक ही सीमित है।

- पेगासस विवादास्पद है क्योंकि इसका उद्देश्य आतंकवाद एवं अपराध को रोकने के बजाय सरकारों द्वारा पत्रकारों, वपिक्षी नेताओं, कार्यकर्ताओं एवं आलोचकों की जासूसी के लिये किया जा सकता है।

## भारत में पेगासस का उपयोग कैसे किया गया?

- **पेगासस परियोजना:** एक वैश्विक सहयोगी जाँच में बताया गया कि इज़रायली NSO समूह द्वारा वकिसति पेगासस स्पाइवेयर का उपयोग करके **300 से अधिक सत्यापित भारतीय मोबाइल नंबरों को लक्ष्यित** किया गया था।
  - इसमें **मंत्रियों, वपिकषी नेताओं, पत्रकारों, वकीलों, व्यापारियों, वैज्ञानिकों, मानवाधिकार कार्यकर्ताओं और सरकारी अधिकारियों** को नशाना बनाया गया था।
- **एमनेस्टी इंटरनेशनल रिसर्च:** एमनेस्टी इंटरनेशनल की **सकियोरटी लैब** द्वारा पुष्टि की गई कि पेगासस का इस्तेमाल **37 फोन को नशाना** बनाने के लिये किया गया था, जिनमें से **10 भारतीयों** के थे।
- **भीमा कोरेगाँव मामला:** वर्ष 2019 में, पेगासस का कथित तौर पर **भीमा कोरेगाँव मामले** और महाराष्ट्र तथा छत्तीसगढ़ में दलित अधिकार आंदोलनों से जुड़े **वकीलों एवं कार्यकर्ताओं के खिलाफ** इस्तेमाल किया गया था।
- **RTI प्रतिक्रिया:** केंद्र सरकार ने वर्ष 2013 में एक RTI अनुरोध के जवाब में **प्रत्येक महीने 7,500 से 9,000 टेलीफोन इंटरसेप्शन वारंट जारी** करने का खुलासा किया।
  - हालाँकि, अब ऐसी सूचना के लिये RTI अनुरोधों को राष्ट्रीय सुरक्षा और व्यक्तियों की शारीरिक सुरक्षा को खतरा बताते हुए अस्वीकार कर दिया जाता है।
- **व्हाट्सएप के आरोप:** व्हाट्सएप ने आरोप लगाया कि अप्रैल, 2018 और मई, 2020 के बीच, NSO ग्रुप द्वारा **"हेवन (Heaven)", "ईडन (Eden)" और "इराइज्ड (Erised)"** नामक इंस्टॉलेशन वैक्टर (प्रवेश बटु) वकिसति करने के लिये अपने सोर्स कोड को **रविरस-इंजीनियरिंग और डीकंपाइल** किया गया था, ये सभी **"हमगिबर्ड (Hummingbird)"** नामक एक परष्कृत हैकगि सूट का हिस्सा थे, जसिं NSO ग्रुप ने अपने सरकारी ग्राहकों को बेचा था।

## नगिरानी और डेटा संरक्षण के लिये भारत का कानूनी ढाँचा क्या है?

- **दूरसंचार अधिनियम, 2023:** **दूरसंचार अधिनियम, 2023** की धारा 20(2) केंद्र या राज्यों को सार्वजनिक आपात स्थितियों, आपदाओं या सार्वजनिक सुरक्षा के दौरान दूरसंचार सेवाओं या नेटवर्क का अस्थायी रूप से **नयित्रण** लेने का अधिकार प्रदान करती है।
  - हालाँकि, **भारतीय टेलीग्राफ नयिम, 2007** के नयिम 419(ए) में वैध संचार अवरोधन के लिये सरकारी प्राधिकरण की आवश्यकता है।
- **सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000:** **सूचना प्रौद्योगिकी अधिनियम, 2000** की धारा 69 और **इंटरसेप्शन नयिम, 2009** सरकार को कंप्यूटर संसाधन के माध्यम से कसिं भी सूचना की नगिरानी, अवरोधन या **डकिरपिट** करने की अनुमति प्रदान करते हैं।
- **डजिटल व्यक्तगत डेटा संरक्षण (DPDP) अधिनियम, 2023:** **DPDP अधिनियम, 2023** एक व्यापक गोपनीयता और डेटा संरक्षण कानून है जसिमें **सहमति (Consent), वैध उपयोग (Legitimate Uses), उल्लंघन, डेटा न्यासीय (Data Fiduciary)** और **प्रोसेसर रसिपान्सबिलिटी** और अपने डेटा पर व्यक्तियों के अधिकारों से संबंधित प्रावधान शामिल हैं।

## भारत में नगिरानी से संबंधित क्या चुनौतियाँ हैं?

- **मौलिक अधिकारों पर प्रभाव:** नगिरानी प्रत्यक्ष रूप से संविधान के **अनुच्छेद 21** के तहत **नजिता के अधिकार का उल्लंघन** करती है, जैसा कि **के.एस पट्टस्वामी केस, 2017** में चर्चा की गई है।
  - नागरिकों की गतिविधियों पर नज़र रखने के लिये नगिरानी प्रणालियों का अस्तित्व ही **अनुच्छेद 19(1)(A)** के तहत मुक्त भाषण को हतोत्साहित करता है।
  - **अनुच्छेद 19(1)(A)** के अनुसार, सभी नागरिकों को **वाक एवं अभिव्यक्ति की स्वतंत्रता का अधिकार** होगा, जसिं कुछ शर्तों के तहत सीमति किया जा सकता है, हालाँकि आमतौर पर इसे **भारत की संप्रभुता, अखंडता या सार्वजनिक व्यवस्था** को प्रभावित करने के आधार पर अस्वीकार कर दिया जाता है।
- **पारदर्शिता का अभाव:** संसदीय या न्यायिक नयित्रण न होने के कारण नगिरानी गुप्त रूप से की जाती है।
  - कार्यपालिका के पास असंगत शक्ति है, जो संविधान में नहित शक्तियों के पृथक्करण के सिद्धांत को कमजोर करती है।
- **न्यायालय में जाने में असमर्थता:** नगिरानी के शकिकार व्यक्त न्यायालय में जाने या अपनी शकियात दर्ज कराने में सक्षम नहीं होते, क्योंकि उन्हें स्वयं ऐसी नगिरानी के बारे में जानकारी नहीं होती।
  - इससे **अनुच्छेद 32 और 226** कमजोर होते हैं जो नागरिकों को अपने मौलिक और अन्य अधिकारों के प्रवर्तन के लिये उपाय तलाशने का अधिकार देते हैं।
- **कार्यपालिका का अतिक्रमण:** संवैधानिक पदाधिकारियों, जैसे कि **सर्वोच्च न्यायालय** के वर्तमान न्यायाधीशों, की नगिरानी की रषिर्ट, कार्यपालिका के अतिक्रमण के वरिद्ध सुरक्षा उपायों के अभाव को उजागर करती है।
- **स्वतंत्र अभिव्यक्तिका दमन:** नगिरानी का भय **खुली चर्चा, रचनात्मकता और असहमतिको रोकता है**, जो एक जीवंत लोकतंत्र के लिये आवश्यक है।

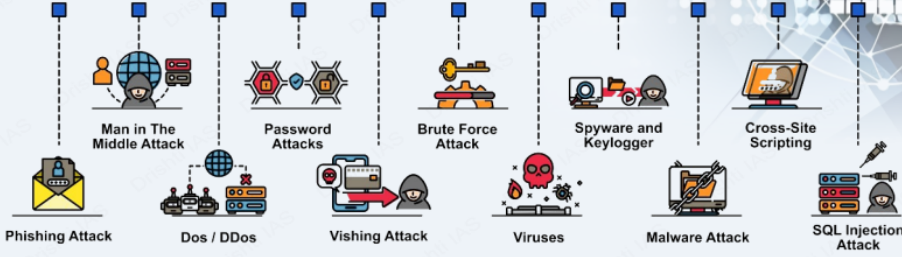
## आगे की राह

- **न्यायिक नगिरानी:** नगिरानी गतिविधियों के लिये **न्यायिक नगिरानी** शुरू करना महत्वपूर्ण है। न्यायालयों को यह समीक्षा करने का अधिकार दिया जाना चाहिये कि क्या नगिरानी आवश्यक, आनुपातिक और संवैधानिक अधिकारों के अनुरूप है।
- **सामूहिक नगिरानी को रोकना:** एक **आनुपातिकता परीक्षण** शुरू किया जाना चाहिये, जसिसे यह सुनिश्चित हो सके कि नगिरानी का उपयोग केवल तभी किया जाए जब बलिकुल आवश्यक हो और कम आक्रामक विकल्प समाप्त हो जाएं।
- **स्पाइवेयर के उपयोग को सीमति करना:** वैश्विक स्तर पर, **साइबर सुरक्षा** और पेगासस जैसे **स्पाइवेयर नरियात** के दुरुपयोग को रोकने के लिये सख्त दशिया-नरिदेशों की आवश्यकता है। उपयोगकर्ताओं के डेटा को अनधिकृत नगिरानी से बचाने के लिये **एंड-टू-एंड एन्क्रिप्शन** और अन्य **सुरक्षा प्रोटोकॉल** को प्राथमिकता दी जानी चाहिये।

# 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 मजबूत पासवर्ड ही पर्याप्त सुरक्षा है
- प्रमुख साइबर सुरक्षा जोखिम सर्वविधित 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

NATION-STATES



### MOTIVATION

GEOPOLITICAL

CYBERCRIMINALS



PROFIT

HACKTIVISTS



IDEOLOGICAL

TERRORIST GROUPS



IDEOLOGICAL VIOLENCE

THRILL-SEEKERS



SATISFACTION

INSIDER THREATS



DISCONTENT

### साइबर सुरक्षा के प्रकार

- महत्वपूर्ण बुनियादी ढाँचा सुरक्षा (रोबर एक्सेस कंट्रोल)
- नेटवर्क सुरक्षा (डिप्लॉयिंग फायरवॉल)
- एप्लिकेशन सुरक्षा (कोड रिव्यू)
- क्लाउड सुरक्षा (टोकनाइजेशन)
- सूचना सुरक्षा (डेटा मार्किंग)

### हाल ही में हुए प्रमुख साइबर हमले

- वाशाकाई नैसमवेयर अटैक (वर्ष 2017)
- कैम्ब्रिज एनालिटिक्स 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 हस्ताक्षरकर्ता नहीं है)
- भारतीय स्तर पर:**
  - IT अधिनियम, 2000 (धारा 43, 66, 66B, 66C, 66D)
  - राष्ट्रीय साइबर सुरक्षा नीति, 2013
  - नेशनल साइबर सिक््योरिटी स्ट्रेजी, 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
- उपयोगकर्ता को शिक्षित और जागरूक करना
- सुरक्षित विन्यास
- उपयोगकर्ता के विशेषाधिकारों का प्रबंधन करना
- सूचना जोखिम प्रबंधन व्यवस्था



### दृष्टि भिन्स प्रश्न:

**प्रश्न:** भारत में नगिरानी कानूनों पर चर्चा कीजिये। पेगासस जैसी आधुनिक नगिरानी तकनीकों द्वारा उत्पन्न चुनौतियों का समाधान करने के लिये कनि सुधारों की आवश्यकता है?

## UPSC सविलि सेवा परीक्षा, वगित वर्ष के प्रश्न

????????????

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

1. यदि कोई किसी मैलवेयर कंप्यूटर तक उसकी पहुँच को बाधति कर देता है तो कंप्यूटर प्रणाली को पुनः प्रचालति करने में लगने वाली लागत
2. यदि यह प्रमाणति 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 हाना को न्यूनतम करने के लिये विशेष परामर्शदाता 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 नमिनलखिति में से किसके/कनिके लिये वधिति: अधदिशात्मक है? (2017)**

1. सेवा प्रदाता
2. डेटा सेंटर
3. कॉर्पोरेट नकिय

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 वभिनिन तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतियों को ध्यान में रखते हुए समीक्षा कीजिये कि भारत ने कसि हद तक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीता सिफलतापूर्वक वकिसति की है। (2022)**