पेगासस स्पाइवेयर एवं इसकी निगिरानी संबंधी चिंताएँ

प्रिलिम्स के लिये:

पेगासस स्पाइवेयर, स्पाइवेयर, ज़ीरो-डे वल्नरेबिलिटी, फिशिंग, RTI, भारतीय टेलीग्राफ अधिनियम 1885, भारतीय टेलीग्राफ नियम 2007, IT अधिनियम 2000, इंटरसेप्शन नियम 2009, निजता का अधिकार, अनुच्छेद 21, केएस पुट्टास्वामी केस 2017, वाक् और अभिव्यक्ति की स्वतंत्रता का अधिकार, संसदीय निरीक्षण, अनुच्छेद 32 और 226, सर्वोच्च न्यायालय, डिजिटल व्यक्तिगत डेटा संरक्षण अधिनियम 2023, एंड-टू-एंड एनक्रिप्शन।

मेन्स के लिये:

स्पाइवेयर एवं निजता संबंधी चिंताएँ, साइबर हमले।

स्रोत: इंडियन एक्सप्रेस

चर्चा में क्यों?

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

- हाल ही में एक अमेरिकी कोर्ट ने फैसला सुनाया कि **पेगासस स्पाइवेयर ने भारत के 300** उपयोगकर्त्ताओं सहित 1,400 व्हाट्सएप उपयोगकर्त्ताओं की निगिरानी 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** डिवाइस को हैक करने में सक्षम है।
  - स्पाइवेयर एक **दुर्भावनापूर्ण सॉफ्टवेयर** है जिससे **उपयोगकर्त्ता की सहमति के बिना गुप्त रूप से** डिवाइस **पर नज़र** रखने के साथ **जानकारी एकत्र** की जाती है।
- **विशेषताएँ:**
  - **उन्नत उपयोग:** इसके तहत iOS डिवाइसों को दूरस्थ रूप से जेलब्रेक करने के लिये ज़ीरो-डे वल्नरेबिलिटी का उपयोग किया जाता है जबकि एंड्रॉइड संस्करण डिवाइसों की निगिरानी के लिये **फ्रामारूट जैसे सॉफ्टवेयर** का उपयोग किया जाता है।
    - ज़ीरो-डे वल्नरेबिलिटी इस सॉफ्टवेयर में एक **गुप्त सिक्योरिटी फ्लॉ** है **जिसके लिये कोई डिफेंस या पैच** उपलब्ध नहीं है।
    - **रूटिंग का आशय किसी डिवाइस को अनलॉक या जेलब्रेक करने** की प्रक्रिया है जैसे कि स्मार्टफोन या टैबलेट, ताकि इस पर **नियंत्रण प्राप्त** किया जा सके।
  - **इनवेज़िबिलिटी:** इसका **कार्य गोपनीय** है तथा **फिशिंग लिंक** पर क्लिक करने के बाद ब्राउज़र बंद होने के अलावा इसका कोई भी **स्पष्ट संकेत** दिखाई नहीं देता है।
- **पेगासस क्लाइंट 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, विपक्षी नेताओं, कार्यकर्त्ताओं 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 विकसित पेगासस स्पाइवेयर का उपयोग करके **300 से अधिक सत्यापित भारतीय मोबाइल नंबरों को** लक्षित किया गया था।
  - इसमें **मंत्रियों, विपक्षी नेताओं, पत्रकारों, वकीलों, व्यापारियों, वैज्ञानिकों, मानवाधिकार कार्यकर्त्ताओं और सरकारी अधिकारियों** को निशाना बनाया गया था।
- **एमनेस्टी इंटरनेशनल रिसर्च:** एमनेस्टी इंटरनेशनल की **सिक्योरिटी लैब** द्वारा पुष्टि की गई कि पेगासस का इस्तेमाल **37 फोन को** निशाना 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 कार्यकर्त्ताओं 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 "इराइज़्ड (Erised)"** नामक इंस्टॉलेशन वैक्टर (प्रवेश बिंदु) विकसित करने के लिये अपने सोर्स कोड को **रिवर्स-इंजीनियरिंग और डीकंपाइल किया गया था, ये सभी "हमिंगबर्ड (Hummingbird)"** नामक एक परिष्कृत हैकिंग सूट का हिस्सा थे, जिसे NSO ग्रुप ने अपने सरकारी ग्राहकों को बेचा था।

निगरानी 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 नियंत्रण** लेने का अधिकार प्रदान करती है।
  - हालाँकि, भारतीय टेलीग्राफ नियम, 2007 **के नियम 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 नियम, 2009** सरकार को कंप्यूटर संसाधन के माध्यम से किसी भी सूचना की **निगरानी, अवरोधन या डिक्रिप्ट करने की** अनुमति प्रदान करते हैं।
- **डिजिटल व्यक्तिगत डेटा संरक्षण (DPDP) अधिनियम, 2023:** DPDP अधिनियम, 2023 एक व्यापक **गोपनीयता और डेटा संरक्षण कानून है जिसमें सहमति (Consent), वैध उपयोग (Legitimate Uses), उल्लंघन, डेटा न्यासीय (Data Fiduciary)** और **प्रोसेसर रिस्पान्सबिलिटी** और **अपने डेटा पर व्यक्तियों के अधिकारों** से संबंधित प्रावधान शामिल हैं।

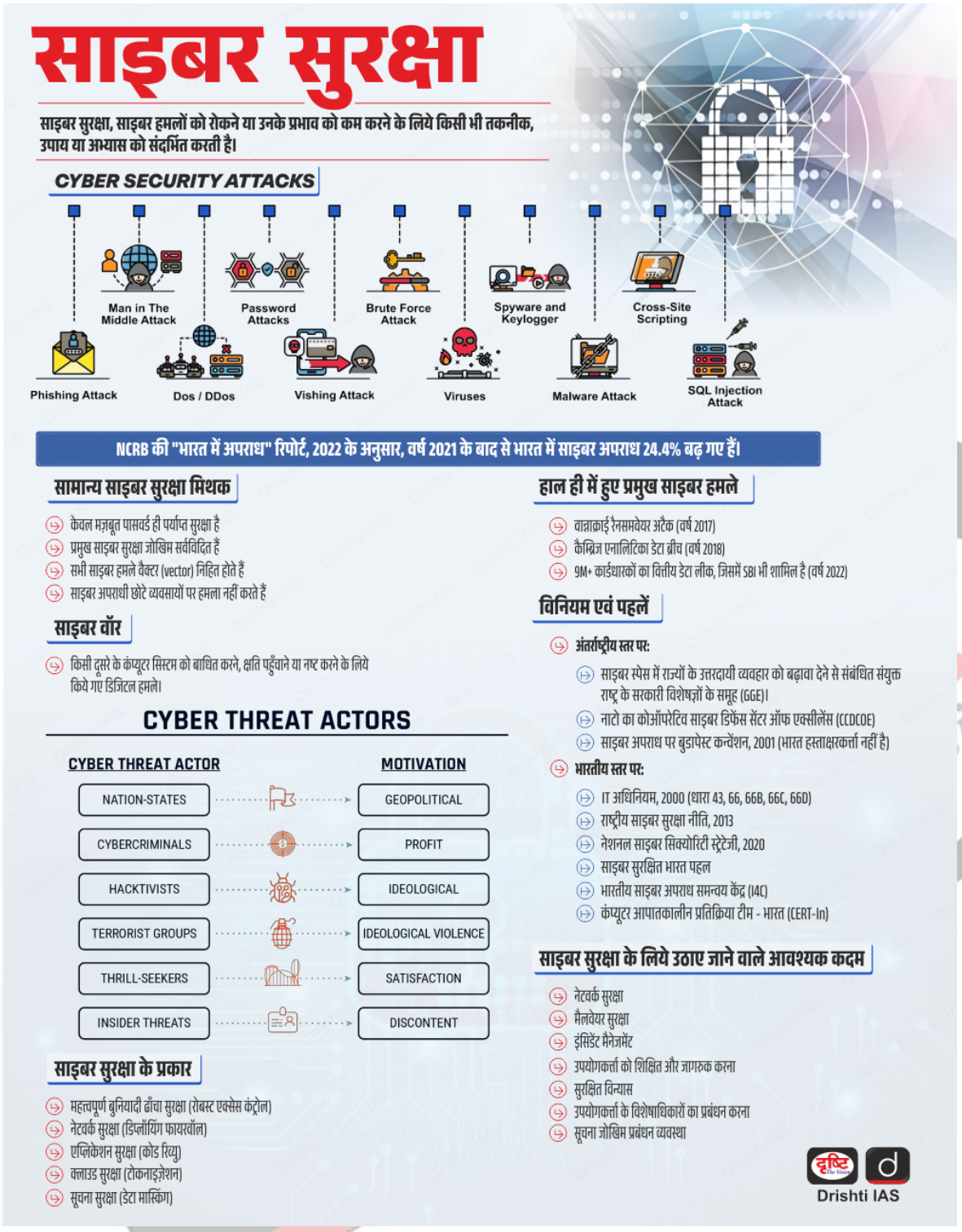
भारत में निगरानी से संबंधित क्या चुनौतियाँ हैं?

- **मौलिक अधिकारों पर प्रभाव**: निगरानी प्रत्यक्ष रूप से संविधान के अनुच्छेद 21 के तहत **निजता के अधिकार का उल्लंघन** करती है, जैसा कि के.एस पुट्टस्वामी केस, 2017 में चर्चा की गई है।
  - **नागरिकों की गतिविधियों पर नज़र रखने** के लिये निगरानी 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 वाक् एवं अभिव्यक्ति की स्वतंत्रता का अधिकार होगा, जिसे कुछ शर्तों के तहत सीमित 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 नियंत्रण** न होने के कारण निगरानी गुप्त रूप से की जाती है।
  - कार्यपालिका के पास **असंगत शक्ति है,** जो संविधान में निहित **शक्तियों के पृथक्करण** के सिद्धांत को कमज़ोर करती है।
- **न्यायालय में जाने में असमर्थता:** निगरानी के शिकार व्यक्ति **न्यायालय में जाने या अपनी शिकायत दर्ज कराने में सक्षम नहीं होते,** क्योंकि उन्हें स्वयं **ऐसी निगरानी 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 निगरानी की रिपोर्ट, कार्यपालिका के अतिक्रमण के विरुद्ध सुरक्षा उपायों के अभाव को उज़ागर करती है।
- **स्वतंत्र अभिव्यक्ति का दमन:** निगरानी का भय **खुली चर्चा, रचनात्मकता और असहमति को रोकता है,** जो एक जीवंत लोकतंत्र के लिये आवश्यक हैं।

आगे की राह

- **न्यायिक निगरानी:** निगरानी गतिविधियों के लिये **न्यायिक निगरानी** शुरू करना महत्त्वपूर्ण है। न्यायालयों को यह समीक्षा करने का अधिकार दिया जाना चाहिये कि क्या निगरानी आवश्यक, आनुपातिक और संवैधानिक अधिकारों के अनुरूप है।
- **सामूहिक निगरानी को रोकना:** एक **आनुपातिकता परीक्षण** शुरू किया जाना चाहिये, जिससे यह सुनिश्चित हो सके कि निगरानी का उपयोग केवल तभी किया जाए जब बिल्कुल आवश्यक हो और कम आक्रामक विकल्प समाप्त हो जाएं।
- **स्पाइवेयर के उपयोग को सीमित करना:** वैश्विक स्तर पर, साइबर सुरक्षा और पेगासस जैसे **स्पाइवेयर निर्यात** के दुरुपयोग को रोकने के लिये सख्त दिशा-निर्देशों की आवश्यकता है। उपयोगकर्त्ताओं के डेटा को अनधिकृत निगरानी से बचाने के लिये एंड-टू-एंड एनक्रिप्शन और अन्य **सुरक्षा प्रोटोकॉल** को प्राथमिकता दी जानी चाहिये।

//



दृष्टि मेन्स प्रश्न:

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

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 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)