राज्य प्रायोजित साइबर हमले

प्रिलिम्स के लिये:

राज्य प्रायोजित हमले, पेगासस स्पाइवेयर, साइबर हमला, गोपनीयता उल्लंघन, भारतीय साइबर अपराध समन्वय केंद्र (I4C), साइबर सुरक्षा

मेन्स के लिये:

पेगासस परियोजना और निगरानी में सुधार की आवश्यकता, सरकारी नीतियाँ और विभिन्न क्षेत्रों में विकास के लिये हस्तक्षेप और उनके डिज़ाइन एवं कार्यान्वयन से उत्पन्न होने वाले मुद्दे

स्रोत: द हिंदू

चर्चा में क्यों?

हाल ही में Apple Inc. ने विपक्षी नेताओं और पत्रकारों सहित व्यक्तियों को "राज्य-प्रायोजित हमलावरों के बारे में सूचित किया, जो **उनके iPhones को** दूरस्थ गतिविधियों के तहत **जोखिम में डालने की कोशिश कर रहे** हैं"।

- ऐसा दूसरी बार हुआ है कि भारत में विपक्षी राजनेताओं और नागरिक समाज के अभिकर्त्ताओं को चेतावनी दी गई है कि वे **जासूसी के प्रयासों का निशाना बने** हैं।
- वर्ष 2021 में पेरिस स्थित [illegible] ने बताया कि पेगासस स्पाइवेयर, जो केवल इज़रायली फर्म NSO ग्रुप द्वारा सरकारी एजेंसियों को बेचा गया था, का कथित तौर पर भारत में कई पत्रकारों, नागरिक समाज समूहों और राजनेताओं पर इस्तेमाल किया गया था।

नोट: साइबर हमला कंप्यूटर सिस्टम, नेटवर्क या डिजिटल उपकरणों की सुरक्षा में सेंध लगाने का एक दुर्भावनापूर्ण और जान-बूझकर किया गया प्रयास है, जिसका उद्देश्य संवेदनशील डेटा को चुराना, नुकसान पहुँचाना, बदलना या उस तक पहुँचना, संचालन में बाधा डालना या डिजिटल क्षेत्र में नुकसान पहुँचाना है।

राज्य प्रायोजित साइबर हमले:

- **परिचय:**
  - राज्य-प्रायोजित साइबर हमले, जिन्हें राष्ट्र-राज्य साइबर हमलों के रूप में भी जाना जाता है, **अन्य देशों, संगठनों या व्यक्तियों के खिलाफ सरकारों या सरकारी एजेंसियों द्वारा संचालित या समर्थित साइबर हमले** हैं।
  - चूँकि ये हमले किसी राष्ट्र-राज्य के विशाल संसाधनों और क्षमताओं द्वारा समर्थित होते हैं, इसलिये वे **अपने उच्च स्तर के संगठन, जटिलता और संसाधनशीलता से प्रतिष्ठित होते हैं।**
  - राज्य-प्रायोजित साइबर हमलों के उदाहरणों में स्टक्सनेट वर्म शामिल है, **जिसने ईरान के परमाणु कार्यक्रम को लक्षित किया, वर्ष 2016 के अमेरिकी राष्ट्रपति चुनाव में कथित रूसी हस्तक्षेप** एवं वर्ष 2017 वानाक्राई रैनसमवेयर हमला, जो उत्तर कोरिया से जुड़ा था।
- **राष्ट्रीय सुरक्षा पर प्रभाव:**
  - **डेटा चोरी:** राज्य-प्रायोजित हमलों से संवेदनशील राष्ट्रीय सुरक्षा जानकारी, गोपनीय सैन्य सूचना और **महत्त्वपूर्ण बुनियादी ढाँचा संबंधी डेटा की चोरी हो सकती है।** इस तरह के उल्लंघन किसी देश की रक्षा क्षमताओं से समझौता कर सकते हैं।
  - **आर्थिक प्रभाव:** प्रमुख उद्योगों और महत्त्वपूर्ण बुनियादी ढाँचे पर हमलों से आर्थिक नुकसान हो सकता है। उदाहरण के लिये ऊर्जा या वित्तीय प्रणालियों में व्यवधान के गंभीर आर्थिक परिणाम हो सकते हैं।
  - **राजनीतिक प्रभाव: साइबर हमलों का उपयोग जनता की राय में हेर-फेर करने, चुनावों को प्रभावित करने और राजनीतिक स्थिरता को कमज़ोर करने के लिये किया जा सकता है। दुष्प्रचार अभियान तथा हैकिंग के दूरगामी राजनीतिक प्रभाव हो सकते हैं।**

- **राष्ट्रीय संप्रभुता: साइबर हमले किसी देश की संप्रभुता का उल्लंघन कर सकते हैं और अपने नागरिकों पर शासन करने तथा उनकी रक्षा करने की क्षमता से समझौता कर सकते हैं।**

?????? (Pegasus):

- **परिचय:**
  - यह एक **प्रकार का मैलेशियस सॉफ्टवेयर** या मैलवेयर है जिसे स्पाइवेयर के रूप में वर्गीकृत किया गया है।
    - यह उपयोगकर्त्ताओं की जानकारी के बिना उपकरणों तक पहुँच प्राप्त करने के लिये डिज़ाइन किया गया है और व्यक्तिगत जानकारी एकत्र करता है तथा इसे वापस रिले करने के लिये सॉफ्टवेयर का उपयोग किया जाता है।
  - पेगासस को **इज़रायली फर्म NSO ग्रुप द्वारा विकसित किया गया है जिसे वर्ष 2010** में स्थापित किया गया था।
    - पेगासस संक्रमण को ऑपरेटिंग सिस्टम की खामियों का फायदा उठाकर तथाकथित **"ज़ीरो-क्लिक" हमलों** के माध्यम से प्राप्त किया जा सकता है, जिसके सफल होने के लिये फोन के मालिक से किसी भी बातचीत की आवश्यकता नहीं होती है।
- **लक्ष्य:**
  - इज़रायल की निगरानी वाली फर्म द्वारा सत्तावादी सरकारों को बेचे गए एक फोन मैलवेयर के माध्यम से**दुनिया भर के मानवाधिकार कार्यकर्त्ताओं, पत्रकारों और वकीलों** को लक्षित किया गया है।
  - भारतीय मंत्री, सरकारी अधिकारी और विपक्षी नेता भी उन लोगों की सूची में शामिल हैं जिनके फोन पर इस स्पाइवेयर द्वारा छेड़छाड़ किये जाने की संभावना व्यक्त की गई है।
    - वर्ष 2019 में **व्हाट्सएप** ने इज़रायल के NSO ग्रुप के खिलाफ अमेरिकी न्यायालय में **एक मुकदमा दायर किया,** जिसमें आरोप लगाया गया था कि यह फर्म मोबाइल उपकरणों को दुर्भावनापूर्ण सॉफ्टवेयर से संक्रमित करके एप्लीकेशन पर साइबर हमलों को प्रेरित कर रही है।
- **साइबर सुरक्षा हेतु पहलें:**
  - **भारतीय पहलें:**
    - **साइबर सुरक्षित भारत पहल**
    - **राष्ट्रीय साइबर सुरक्षा समन्वय केंद्र (NCCC)**
    - साइबर स्वच्छता केंद्र
    - भारतीय साइबर अपराध समन्वय केंद्र (I4C)
    - भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम, सर्ट-इन (Indian Computer Emergency Response Team- CERT-In)
  - **वैश्विक पहलें:**
    - अंतर्राष्ट्रीय दूरसंचार संघ (ITU)
    - साइबर अपराध पर बुडापेस्ट अभिसमय

आगे की राह

- व्यापक राष्ट्रीय साइबर सुरक्षा नीतियों और रणनीतियों को विकसित करने तथा लागू करने की आवश्यकता है जो**साइबर क्षेत्र में रक्षा एवं अपराध दोनों का समाधान करेगी**।
- सरकारी एजेंसियों के लिये घुसपैठ पहचान हेतु उन्नत प्रणाली, सुरक्षित नेटवर्क और साइबर सुरक्षा प्रशिक्षण सहित साइबर सुरक्षा बुनियादी ढाँचे को मज़बूत करने के लिये संसाधन आवंटित करने की आवश्यकता है।
- खतरे की खुफिया जानकारी साझा करने और राज्य-प्रायोजित खतरों पर प्रतिक्रियाओं का समन्वय करने के लिये अन्य देशों तथा अंतर्राष्ट्रीय संगठनों के साथ सहयोग करना चाहिये।