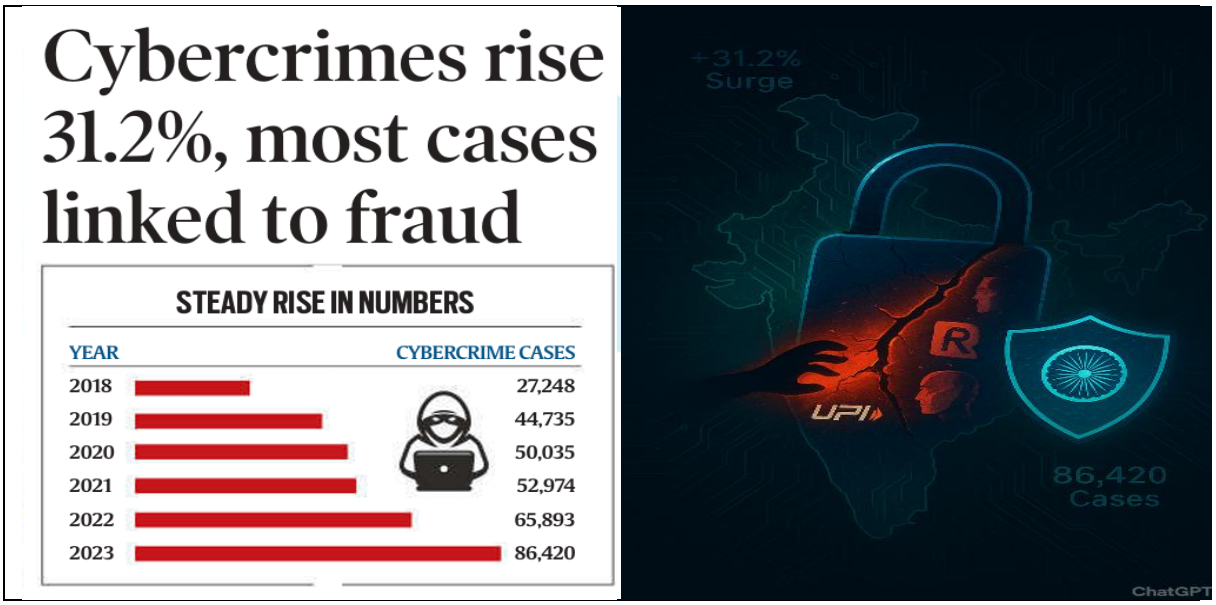
भारत में साइबर सुरक्षा और साइबर अपराध

समाचार में क्यों / संदर्भ

- एनसीआरबी की *भारत में अपराध 2023* रिपोर्ट साइबर अपराधों में 31.2% की वृद्धि दर्शाती है। मामले 2022 के 65,893 से बढ़कर 2023 में 86,420 तक पहुँच गए।
- लगभग 69% घटनाएँ धोखाधड़ी से जुड़ी थीं, इसके बाद यौन शोषण (4.9%) और जबरन वसूली (3.8%) के मामले सामने आए।
- कर्नाटक, तेलंगाना और उत्तर प्रदेश जैसे राज्यों में सबसे अधिक मामले दर्ज हुए, जो यह दर्शाता है कि भारत के बढ़ते डिजिटल विस्तार के साथ-साथ साइबर अपराधियों के नए-नए तरीकों और कमजोरियों में भी वृद्धि हो रही है।



साइबर अपराध क्या है?

- **परिभाषा:** साइबर अपराध उन अपराधों को कहा जाता है जहाँ कंप्यूटर, नेटवर्क या डिजिटल उपकरण अपराध का साधन होते हैं या स्वयं अपराध का निशाना बनते हैं।
- **प्रमुख प्रकार:**
  - **वित्तीय अपराध:** फ़िशिंग, यूपीआई/ऑनलाइन बैंकिंग धोखाधड़ी, पहचान की चोरी, निवेश और क्रिप्टो से जुड़े घोटाले।
  - **सामग्री अपराध:** अश्लील या अवैध सामग्री का प्रसार।
  - **साइबर स्टॉकिंग और ऑनलाइन उत्पीड़न।**
  - **जासूसी और साइबर युद्ध:** महत्वपूर्ण ढाँचों पर राज्य-प्रायोजित हमले।
  - **रैंसमवेयर और मैलवेयर हमले:** अक्सर डार्क वेब पर उपलब्ध "रैंसमवेयर-एज़-ए-सर्विस (RaaS)" नेटवर्क के ज़रिए।

एनसीआरबी डेटा से प्रमुख रुझान

- **लगातार वृद्धि:** 2018 में 27,248 मामले →2023 में 86,420 मामले। यह बढ़ोतरी वास्तविक घटनाओं के साथ-साथ बेहतर रिपोर्टिंग तंत्र को भी दर्शाती है।

- **धोखाधड़ी का प्रभुत्व:** 2023 में 68.9% मामले फ़िशिंग, यूपीआई धोखाधड़ी और डिजिटल भुगतान से जुड़ी धोखाधड़ी से संबंधित रहे।
- **भौगोलिक संकेंद्रण:**
  - कर्नाटक: 21,889 मामले (2023)
  - तेलंगाना: 18,236 मामले
  - उत्तर प्रदेश: 10,794 मामले
    यह प्रवृत्ति आईटी हब वाले क्षेत्रों और मज़बूत रिपोर्टिंग प्रणाली दोनों की ओर इशारा करती है।
- **आर्थिक अपराधों से संबंध:** 2023 में कुल आर्थिक अपराधों (2.04 लाख) में साइबर धोखाधड़ी का बड़ा हिस्सा रहा।

साइबर अपराधों से निपटने की चुनौतियाँ

- **लाभ-प्रधान डिजिटल पारिस्थितिकी तंत्र:** कंपनियाँ अक्सर साइबर सुरक्षा की तुलना में मुनाफ़े और तेज़ विस्तार को प्राथमिकता देती हैं।
- **अंतर्राष्ट्रीय प्रकृति:** कई हमले विदेशी सर्वरों के माध्यम से होते हैं, जिससे जांच और साक्ष्य जुटाना कठिन हो जाता है।
- **तेज़ डिजिटलीकरण:** यूपीआई, आईओटी, 5जी और रिमोट ऐप्स ने हमलों की संभावनाएँ बढ़ा दी हैं।
- **क्षमता की कमी:** प्रशिक्षित पुलिस बल, फोरेंसिक विशेषज्ञ और मान्यता प्राप्त साइबर प्रयोगशालाओं की कमी।
- **पुराना कानूनी ढाँचा:** आईटी अधिनियम, 2000 अब मौजूदा चुनौतियों के लिए अपर्याप्त है।
- **पेशेवर साइबर अपराधी नेटवर्क:** डार्क वेब और RaaS प्लेटफ़ॉर्म अपराधियों को आसानी से उपकरण उपलब्ध कराते हैं।
- **क्रिप्टोकरेंसी और एआई का दुरुपयोग:** गुमनाम लेनदेन, एआई-आधारित फ़िशिंग (जैसे WormGPT), डीपफेक और स्वचालित मैलवेयर नए खतरे पैदा कर रहे हैं।
- **जागरूकता की कमी:** कम डिजिटल साक्षरता, खासकर ग्रामीण और बुज़ुर्ग आबादी में, साइबर धोखाधड़ी के मामलों को बढ़ाती है।

सरकारी उपाय

कानूनी ढाँचा

- आईटी अधिनियम (IT Act), 2000 – साइबर अपराधों से निपटने का प्राथमिक कानून।
- डिजिटल व्यक्तिगत डेटा संरक्षण (DPDP) अधिनियम, 2023 – व्यक्तिगत डेटा अधिकारों की सुरक्षा सुनिश्चित करता है।

संस्थागत तंत्र

- **I4C (भारतीय साइबर अपराध समन्वय केंद्र):** जांच, पीड़ित सहायता और समन्वय के लिए केंद्रीय केंद्र।
- **CERT-In:** खतरों की निगरानी और सुरक्षा सलाह जारी करता है।
- **NCIIPC:** महत्वपूर्ण बुनियादी ढाँचों की सुरक्षा।

- **रक्षा साइबर एजेंसी:** सैन्य तैयारी को सुनिश्चित करती है।
- **राष्ट्रीय साइबर फोरेंसिक प्रयोगशाला:** साक्ष्य विश्लेषण और जांच में सहयोग।

क्षमता निर्माण

- **CyTrain पोर्टल:** पुलिस और न्यायपालिका के लिए ऑनलाइन प्रशिक्षण।
- **राज्य साइबर प्रयोगशालाएँ:** अधिक संख्या में स्थापित करने और मान्यता की आवश्यकता।
- **राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल** (cybercrime.gov.in) और**वित्तीय धोखाधड़ी हेल्पलाइन।**

जागरूकता अभियान

- महिलाओं और बच्चों के खिलाफ साइबर अपराध रोकथाम (CCPWC)।
- **साइबर स्वच्छता केंद्र:** बॉटनेट सफाई और मैलवेयर हटाना।
- नियमित सलाह और डिजिटल साक्षरता पहल।

आगे की राह

- **व्यापक साइबर सुरक्षा कानून:** राष्ट्रीय स्तर पर कानून जो AI दुरुपयोग और त्वरित घटना-प्रतिक्रिया जैसी चुनौतियों को संबोधित करे।
- **विशेष साइबर पुलिस और फोरेंसिक ढाँचा:** राज्य स्तर पर साइबर प्रयोगशालाओं को उन्नत करना और इलेक्ट्रॉनिक साक्ष्य परीक्षण को औपचारिक मान्यता देना।
- **अंतर्राष्ट्रीय सहयोग:** तेज़ MLAT प्रक्रियाएँ, RaaS समूहों पर संयुक्त कार्रवाई और द्विपक्षीय समझौते।
- **जन-जागरूकता:** फ़िशिंग, यूपीआई सुरक्षा, दो-कारक प्रमाणीकरण और सिम-स्वैप धोखाधड़ी पर व्यापक अभियान।
- **साइबर बीमा और PPP मॉडल:** साइबर बीमा अपनाने को प्रोत्साहित करना और निजी क्षेत्र के निवेश को बढ़ावा देना।
- **क्षेत्रीय लचीलापन:** वित्त, स्वास्थ्य और ऊर्जा जैसे क्षेत्रों में अलग CERT इकाइयाँ बनाना और नियमित ऑडिट करना।
- **ख़ुफ़िया जानकारी साझा करना:** सार्वजनिक-निजी क्षेत्र में समझौते के संकेतकों (IoC) के सुरक्षित साझा ढाँचे।

निष्कर्ष (Conclusion)

एनसीआरबी 2023 की रिपोर्ट से स्पष्ट है कि भारत का डिजिटल विस्तार साइबर अपराधों की चुनौती के साथ तेज़ी से बढ़ रहा है। CERT-In, I4C और DPDP अधिनियम जैसी संस्थाएँ और क़ानून एक आधार तो प्रदान करते हैं, लेकिन मौजूदा कानूनी ढाँचे, क्षमता निर्माण और अंतर्राष्ट्रीय सहयोग में अभी भी खामियाँ हैं। स्थायी डिजिटल विश्वास और सुरक्षा सुनिश्चित करने के लिए भारत को बहु-स्तरीय रणनीति अपनानी होगी जिसमें कानूनी सुधार, तकनीकी ढाँचा, जन-जागरूकता और वैश्विक साझेदारी शामिल हों।

UPSC पिछले वर्ष के प्रश्न (Previous Year Questions):

Question	Marks	Words	Year
What are the different elements of cyber security? Keeping in view the challenges in cyber security examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. साइबर सुरक्षा के विभिन्न तत्त्व क्या हैं ? साइबर सुरक्षा की चुनौतियों को ध्यान में रखते हुए समीक्षा कीजिए कि भारत ने किस हद तक एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक विकसित की है।	15 Marks	250 Marks	2022
Keeping in view India's internal security, analyses the impact of cross-border cyber-attacks. Also discuss defensive measures against these sophisticated attacks. भारत की आन्तरिक सुरक्षा को ध्यान में रखते हुए, सीमा-पार से होने वाले साइबर हमलों के प्रभाव का विश्लेषण कीजिए। साथ ही, इन परिष्कृत हमलों के विरुद्ध रक्षात्मक उपायों की चर्चा कीजिए।	10 Marks	150 Marks	2021
Discuss different types of Cyber crimes and measures required to be taken to fight the menace. साइबर अपराध के विभिन्न प्रकारों और इस ख़तरे से लड़ने के आवश्यक उपायों की विवेचना कीजिए।	10 Marks	150 Marks	2020
What is the CyberDome Project? Explain how it can be useful in controlling internet crimes in India. साइबर डोम परियोजना क्या है? स्पष्ट कीजिए कि भारत में इंटरनेट अपराधों को नियंत्रित करने में यह किस प्रकार उपयोगी हो सकता है।	10 Marks	150 Marks	2019
Data security has assumed significant importance in the digitized world due to rising cyber crimes. The Justice B.N. Srikrishna Committee Report addresses issues related to data security. What, in your view, are the strengths and weaknesses of the Report relating to protection of personal data in cyber space? अंकीयकृत (डिजिटाइज़्ड) दुनिया में बढ़ते हुए साइबर अपराधों के कारण डाटा सुरक्षा का महत्त्व बहुत बढ़ गया है। जस्टिस बी०एन० श्री कृष्णा समिति रिपोर्ट में डाटा की सुरक्षा से संबंधित मुद्दों पर सोच-विचार किया गया है। आपके विचार में साइबर स्पेस में निजी डाटा की सुरक्षा से संबंधित इस रिपोर्ट की खूबियाँ और खामियाँ क्या-क्या हैं?	15 Marks	250 Marks	2018
Discuss the potential threats of Cyber attack and the security framework to prevent it. साईबर आक्रमण के सम्भावित खतरों की एवम् इन्हें रोकने के लिए सुरक्षा ढांचे की विवेचना कीजिए।	10 Marks	150 Marks	2017

Considering the threats cyberspace poses for the country, India needs a "Digital Armed Forces" to prevent crimes. Critically evaluate the National Cyber Security Policy, 2013 outlining the challenges perceived in its effective implementation. विचार करते हुए कि साइबर स्पेस देश के लिए ख़तरा प्रस्तुत करता है, भारत को ऐसे अपराधों को रोकने के लिए एक "डिजिटल सशस्त्र बल" की आवश्यकता है। राष्ट्रीय साइबर सुरक्षा नीति, 2013 के प्रभावी कार्यान्वयन में दिखाई देने वाली चुनौतियों की रूपरेखा प्रस्तुत करते हुए, इस नीति का समालोचनात्मक मूल्यांकन कीजिए।	12.5 Marks	200 Marks	2015
Discuss the advantages and security implications of cloud hosting of servers vis-a-vis in-house machine-based hosting for government businesses. सरकारी कार्यकलापों के लिए, सर्वरों की क्लाउड होस्टिंग बनाम स्वसंस्थागत मशीन-आधारित होस्टिंग के लाभों और सुरक्षा निहितार्थों पर चर्चा कीजिए।	12.5 Marks	200 Marks	2015
Cyber warfare is considered by some defense analysts to be a larger threat than even Al Qaeda or terrorism. What do you understand by Cyber warfare? Outline the cyber threats which India is vulnerable to and bring out the state of the country's preparedness to deal with the same. कुछ रक्षा विश्लेषक इलेक्ट्रानिकी संचार माध्यम द्वारा युद्ध को अलकायदा और आतंकवाद से भी बड़ा खतरा मानते हैं। आप 'इलेक्ट्रानिकी संचार माध्यम युद्ध' (Cyber warfare) से क्या समझते हैं ? भारत ऐसे जिन खतरों के प्रति संवेदनशील है उनकी रूप-रेखा खींचिए और देश की उनसे निपटने की तैयारी को भी स्पष्ट कीजिए।	10 Marks	200 Marks	2013
What is digital signature? What does its authentication mean? Giver various salient built in features of a digital signature. 'आंगुलिक हस्ताक्षर' (digital signature) क्या होता है ? उसकेद्वारा प्रमाणीकरण का क्या अर्थ है ? 'आंगुलिक हस्ताक्षर' की प्रमुख विविध अंतस्थ विशेषताएं बताइए।	10 Marks	100 Marks	2013
What are social networking sites and what security implications do these sites present? 'सामाजिक संजाल स्थल' (Social Networking Sites) क्या होती हैं और इन स्थलों से क्या सुरक्षा उलझनें प्रस्तुत होती हैं?	10 Marks	200 Marks	2013