राष्ट्रीय साइबर सुरक्षा रणनीति

प्रिलिम्स के लिये:

भारतीय डेटा सुरक्षा परिषद (DSCI), साइबर सुरक्षा के लिये सरकार की पहल, भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-In), संबंधित पहल।

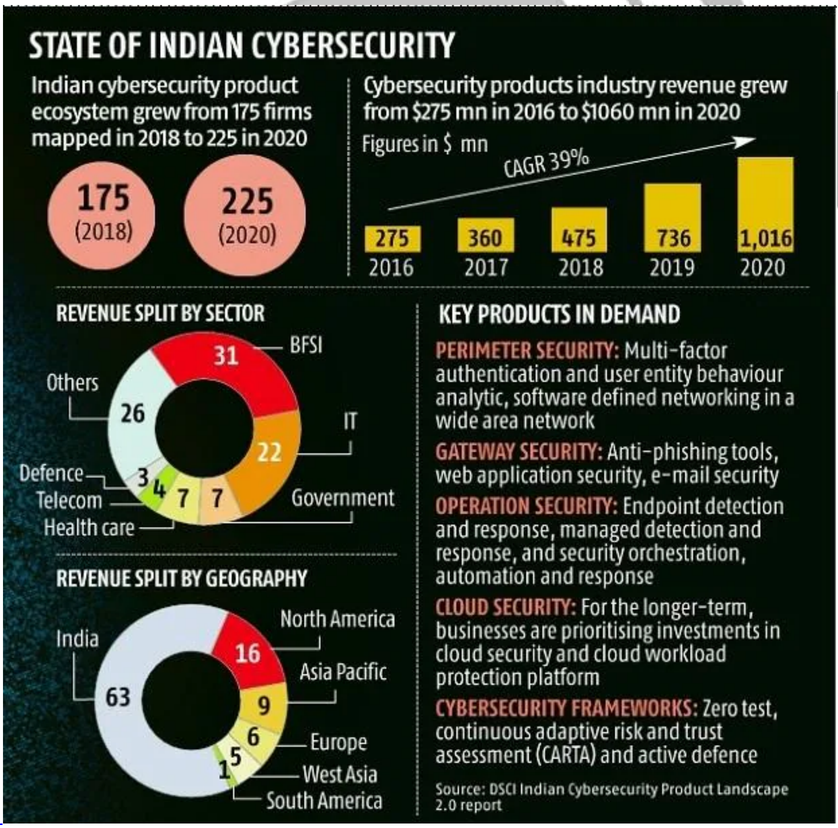
मेन्स के लिये:

संचार नेटवर्क, राष्ट्रीय साइबर सुरक्षा रणनीति, साइबर सुरक्षा के माध्यम से आंतरिक सुरक्षा के लिये चुनौतियाँ

चर्चा में क्यों?

वर्ष 2020 में, लेफ्टिनेंट **जनरल राजेश पंत** की अध्यक्षता में **भारतीय डेटा सुरक्षा परिषद (Data Security Council of India-DSCI)** द्वारा [राष्ट्रीय साइबर सुरक्षा रणनीति]() की अवधारणा की गई थी। रिपोर्ट में भारत के लिये एक सुरक्षित,सुदृढ़, भरोसेमंद, लचीला और जीवंत साइबर स्पेस सुनिश्चित करने के लिये 21 क्षेत्रों पर ध्यान केंद्रित किया गया है।

- हालाँकि भारत में [साइबर हमलों]() में वृद्धि के बीच, केंद्र ने अभी तक राष्ट्रीय साइबर सुरक्षा रणनीति लागू नहीं किया है।



//

राष्ट्रीय साइबर सुरक्षा रणनीति की क्या आवश्यकता है?

- **साइबर हमलों की बढ़ती संख्या:** अमेरिकी साइबर सुरक्षा **फर्म पालो ऑल्टो नेटवर्क्स** की वर्ष 2021 की रिपोर्ट के अनुसार, महाराष्ट्र भारत में सबसे अधिक लक्षित (सभी **रैंसमवेयर हमलों का 42% सामना** करने वाला) राज्य था
    - रिपोर्ट में कहा गया है कि भारत हैकर समूहों के लिये अधिक **आर्थिक रूप से लाभदायक क्षेत्रों में से एक है** और इसलिये हैकर भारतीय फर्मों की डेटा तक पहुँच प्राप्त करके आमतौर पर क्रिप्टोकरेंसी का उपयोग फिरौती का भुगतान करने के लिये करते हैं।
    - चार भारतीय संगठनों में से एक को वर्ष 2021 में रैंसमवेयर हमले का सामना करना पड़ा, जो **वैश्विक औसत के स्तर से 21%** अधिक है।
- **साइबर युद्ध के अपराध:**
    - संयुक्त राज्य अमेरिका उन चुनिंदा देशों में से एक है, जिसने न केवल साइबर हमले से बचाव की रणनीति विकसित करने में काफी अधिक धनराशि का निवेश किया है, बल्कि उसके पास साइबर युद्ध अपराधियों से निपटने के लिये आवश्यक क्षमता भी मौजूद है।
    - जिन देशों की साइबर युद्ध क्षमता सबसे अधिक है उनमें संयुक्त राज्य अमेरिका, चीन, रूस, इज़रायल और यूनाइटेड किंगडम आदि शामिल हैं।
- **महामारी के बाद डिजिटलीकरण में बढ़ोतरी:**
    - कोरोना वायरस महामारी के बाद से महत्त्वपूर्ण अवसंरचना का तेज़ी से डिजिटलीकरण किया जा रहा है, जिसमें वित्तीय सेवाएँ, बैंक, बिजली, विनिर्माण, परमाणु ऊर्जा संयंत्र आदि शामिल हैं।
- **महत्त्वपूर्ण क्षेत्रों की सुरक्षा:**
    - विभिन्न आर्थिक क्षेत्रों की बढ़ती परस्परता और 5G के साथ इंटरनेट के प्रयोग में होने वाली बढ़ोतरी के मद्देनज़र यह काफी महत्त्वपूर्ण हो गया है।
    - भारतीय कंप्यूटर इमरजेंसी रिस्पांस टीम (CERT-In) द्वारा प्रस्तुत आँकड़ों की मानें तो केवल वर्ष 2020 के प्रारंभिक आठ महीनों में ही कुल 6.97 लाख साइबर सुरक्षा संबंधी घटनाएँ दर्ज हुई थीं, जो कि पिछले चार वर्षों में हुई कुल साइबर घटनाओं के बराबर हैं।
- **हालिया साइबर घटनाएँ:**
    - भारत के बिजली क्षेत्र को व्यापक पैमाने पर लक्षित करने के लिये 'रेड इको' नामक चीन के एक समूह द्वारा मैलवेयर आदि के उपयोग में वृद्धि देखी गई है।
        - 'रेड इको' द्वारा 'शैडोपैड' (ShadowPad) नामक नए मैलवेयर का उपयोग किया जाता है, जिसमें सर्वर तक पहुँच प्राप्त करने के लिये बैकडोर का प्रयोग शामिल है।
    - 'स्टोन पांडा' नाम से प्रचलित चीन के एक हैकर समूह द्वारा 'भारत बायोटेक' और 'सीरम इंस्टीट्यूट' की सूचना प्रौद्योगिकी अवसंरचना एवं सप्लाई चेन सॉफ्टवेयर में कई सुभेद्यताएँ खोजी गई थीं।
- **सरकार के लिये:**
    - एक स्थानीय, राज्य या केंद्र सरकार देश (भौगोलिक, सैन्य रणनीतिक संपत्ति आदि) एवं नागरिकों से संबंधित विभिन्न गोपनीय डेटा एकत्रित करती है और इस डेटा की सुरक्षा काफी महत्त्वपूर्ण होती है।
- **आम लोगों के लिये:**
    - सोशल नेटवर्किंग साइटों पर किसी व्यक्ति द्वारा साझा की गई तस्वीरों, वीडियो और अन्य व्यक्तिगत जानकारी को अनुचित रूप से किसी अन्य व्यक्ति द्वारा प्रयोग किया जा सकता है, जिससे गंभीर, यहाँ तक कि जानलेवा घटनाएँ भी हो सकती हैं।
- **व्यवसायों के लिये:**
    - कंपनियों के पास उनके सिस्टम में बहुत सा डेटा और जानकारी मौजूद होती है। साइबर हमले के माध्यम से किसी भी प्रकार की प्रतिस्पर्द्धी सूचनाओं (जैसे-पेटेंट और मूल कार्य) और कर्मचारियों/ग्राहकों के निजी डेटा की चोरी होने का खतरा रहता है, जिसके परिणामस्वरूप भारी नुकसान का सामना करना पड़ सकता है।

राष्ट्रीय साइबर सुरक्षा रणनीति के मुख्य घटक क्या हैं?

- **सार्वजनिक सेवाओं का बड़े पैमाने पर डिजिटलीकरण:** सभी डिजिटलीकरण पहलों में डिज़ाइन के शुरुआती चरणों में ही सुरक्षा पर ध्यान देना।
    - मूल उपकरणों के मूल्यांकन, प्रमाणन और रेटिंग के लिये संस्थागत क्षमता का विकास करना।
    - सुभेद्यता और घटनाओं की समय-समय पर रिपोर्टिंग।
- **आपूर्ति शृंखला सुरक्षा:** इंटीग्रेटेड सर्किट और इलेक्ट्रॉनिक्स उत्पादों की आपूर्ति शृंखला की निगरानी तथा मैपिंग।
    - सामरिक और तकनीकी स्तरों पर वैश्विक स्तर पर देश की **सेमीकंडक्टर** डिज़ाइन क्षमताओं का लाभ उठाना।
- **महत्त्वपूर्ण सूचना अवसंरचना संरक्षण: पर्यवेक्षी नियंत्रण और डेटा अधिग्रहण (SCADA) सुरक्षा को एकीकृत करना**
    - सुभेद्यता को सुरक्षित बनाए रखना।
    - क्षेत्रक की समग्र स्तर की सुरक्षा आधार रेखा तैयार करना और उसके नियंत्रणों पर नज़र रखना।
    - खतरे की तैयारी और साइबर-बीमा उत्पादों के विकास के लिये ऑडिट पैरामीटर तैयार करना।
- **डिजिटल भुगतान:** तैनात उपकरणों और प्लेटफार्मों की मैपिंग तथा मॉडलिंग, आपूर्ति शृंखला, लेनदेन करने वाली संस्थाएँ, भुगतान प्रवाह, इंटरफेस एवं डेटा एक्सचेंज को मज़बूती प्रदान करना।
- **राज्य स्तरीय साइबर सुरक्षा:** राज्य स्तरीय साइबर सुरक्षा नीतियाँ विकसित करना,
    - समर्पित धन का आवंटन,
    - डिजिटलीकरण योजनाओं की गंभीर जाँच,
    - सुरक्षा संरचना, संचालन और शासन के लिये दिशानिर्देश।
- **छोटे और मध्यम व्यवसायों की सुरक्षा:** साइबर सुरक्षा तैयारियों के उच्च स्तर के प्रोत्साहन देने के लिये साइबर सुरक्षा में नीतिगत हस्तक्षेप।
    - **इंटरनेट ऑफ थिंग्स (IoT)** और औद्योगीकरण को अपनाने के लिये सुरक्षा मानकों, ढाँचे और संरचना का विकास करना।

रिपोर्ट के सुझाव

- **बजटीय प्रावधान:** इस क्षेत्र में वर्तमान वार्षिक बजट आवंटन 0.25% के स्तर से बढ़ाकर 1% तक किया जाना चाहिये इसके अतिरिक्त साइबर सुरक्षा के लिये अलग बजट की सिफारिश की गई है।
    - अलग मंत्रालयों और एजेंसियों के संदर्भ में आईटी/प्रौद्योगिकी व्यय का 15-20% साइबर सुरक्षा के लिये निर्धारित किया जाना चाहिये।
    - यह साइबर सुरक्षा के लिये कोष स्थापित करने और उसी क्षेत्र में क्षमताओं के निर्माण हेतु राज्यों को केंद्रीय वित्त पोषण प्रदान करने का भी सुझाव देता है।
- **अनुसंधान, नवाचार, कौशल-निर्माण और प्रौद्योगिकी विकास:** रिपोर्ट आईसीटी के आधुनिकीकरण और डिजिटलीकरण में निवेश करने, परिणाम-आधारित कार्यक्रमों के माध्यम से साइबर सुरक्षा के लिये एक लघु तथा दीर्घकालिक एजेंडा स्थापित करने एवं डीप-टेक साइबर सुरक्षा नवाचार में निवेश प्रदान करने का सुझाव देती है।
    - DSCI भारतीय इंजीनियरिंग सेवाओं से चुने गए संवर्गों के साथ एक 'साइबर सुरक्षा सेवाएँ' बनाने की सिफारिश करता है।
- **संकट प्रबंधन:** किसी संकट से निपटने के लिये पर्याप्त तैयारी के लिये, DSCI साइबर सुरक्षा अभ्यास आयोजित करने की सिफारिश करता है जिसमें वास्तविक जीवंत परिदृश्य उनके प्रभाव के साथ शामिल हैं।
- **साइबर बीमा:** साइबर बीमा पर अभी शोध किया जाना बाकी है इसलिये व्यापार और प्रौद्योगिकी परिदृश्यों में साइबर सुरक्षा जोखिमों को संबोधित करने के साथ-साथ खतरे के जोखिम की गणना करने के लिये एक बीमांकिक विज्ञान होना चाहिये।
- **साइबर कूटनीति:** साइबर कूटनीति भारत के वैश्विक संबंधों को आकार देने में बहुत बड़ी भूमिका निभाती है। इसलिये **बंगाल की खाड़ी बहु-क्षेत्रीय तकनीकी और आर्थिक सहयोग पहल (बिम्सटेक)** और **शंघाई सहयोग संगठन (एससीओ)** जैसे प्रमुख क्षेत्रीय ब्लॉकों की साइबर सुरक्षा तैयारियों को कार्यक्रमों, आदान-प्रदान तथा औद्योगिक समर्थन के माध्यम से सुनिश्चित किया जाना चाहिये।
    - बेहतर कूटनीति के लिये, सरकार को साइबर सुरक्षा में एक ज़िम्मेदार प्लेयर के रूप में ब्रांड इंडिया को बढ़ावा देना चाहिये और प्रमुख देशों/क्षेत्रों के लिये 'साइबर दूत' भी बनाना चाहिये।
- **साइबर अपराध जाँच:** दुनिया भर में साइबर अपराध में वृद्धि के साथ, रिपोर्ट स्पैमिंग और फेक न्यूज को रोकने के लिये कानून बनाकर न्यायिक प्रणाली को कम करने की सिफारिश करती है।
    - यह संभावित प्रौद्योगिकी परिवर्तन को ध्यान में रखते हुए 5 वर्ष का रोडमैप तैयार करने, साइबर अपराधों से निपटने के लिये विशेष न्यायालयों की स्थापना और साइबर अपराध के बैकलॉग को दूर करने का भी सुझाव देती है।
    - इसके अलावा DSCI एजेंसियों को AI/ML, **ब्लॉकचैन**, IoT, क्लाउड, ऑटोमेशन आदि के युग में उन्नत फोरेंसिक प्रशिक्षण का सुझाव देती है।

सरकार द्वारा शुरू की गई पहलें

- ‘साइबर सुरक्षित भारत’ पहल
- साइबर स्वच्छता केंद्र
- राष्ट्रीय साइबर क्राइम रिपोर्टिंग पोर्टल
- भारतीय साइबर अपराध समन्वय केंद्र (I4C)
- नेशनल क्रिटिकल इन्फॉर्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर (NCIIPC)
- सूचना प्रौद्योगिकी अधिनियम, 2000

यूपीएससी सिविल सेवा परीक्षा, विगत वर्षों के प्रश्न (PYQs):

हाल ही में कभी-कभी खबरों में आने वाले शब्द 'वानाक्राई, पेट्या और इंटर्नलब्लू' निम्नलिखित में से किससे संबंधित हैं (2018)

(a) एक्सोप्लैनेट
(b) क्रिप्टोकरेंसी
(c) साइबर हमले
(d) मिनी उपग्रह

उत्तर: (c)

- रैंसमवेयर दुर्भावनापूर्ण सॉफ्टवेयर (या मैलवेयर) का एक रूप है। एक बार जब यह कंप्यूटर में प्रवेश कर लेता है, तो यह आमतौर पर डेटा तक पहुँच कर उपयोगकर्त्ताओं को नुकसान पहुँचाता है। भुगतान करने पर डेटा तक पहुँच बहाल करने का वादा करते हुए हमलावर पीड़ित से फिरौती की मांग करते है।
- **'वानाक्राई, पेट्या और इंटर्नलब्लू** कुछ रैनसम वेयर हैं, जिन्होंने बिटकॉइन (क्रिप्टोकरेंसी) में फिरौती के भुगतान की मांग की थी।

स्रोत: द हिंदू

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/national-cyber-security-strategy-2