राष्ट्रीय साइबर सुरक्षा रणनीति 2020

चर्चा में क्यों?

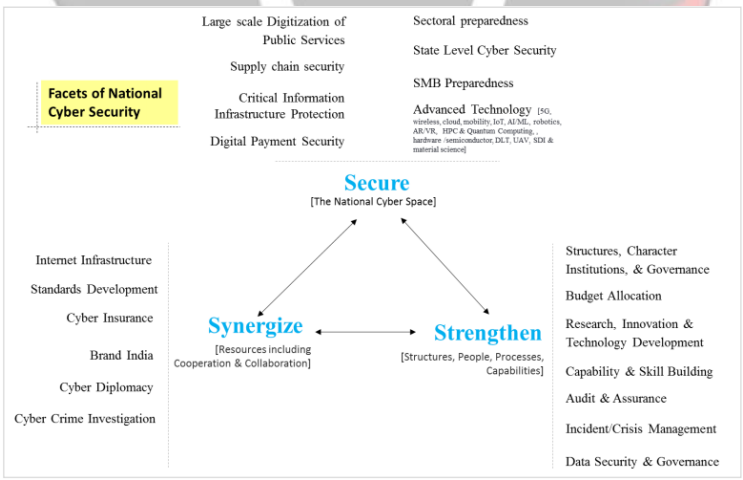
राष्ट्रीय सुरक्षा परिषद सचिवालय में राष्ट्रीय साइबर सुरक्षा समन्वयक कार्यालय द्वारा एक राष्ट्रीय साइबर सुरक्षा रणनीति 2020 तैयार की जा रही है।

- साइबर सुरक्षा का आशय किसी भी प्रकार के हमले, क्षति, दुरुपयोग और जासूसी से महत्त्वपूर्ण सूचना अवसंरचना सहित संपूर्ण साइबर स्पेस की रक्षा करने से है।
- राष्ट्रीय सुरक्षा परिषद (NSC) एक तीन-स्तरीय संगठन है, जो कि सामरिक चिंता वाले राजनीतिक, आर्थिक, ऊर्जा और सुरक्षा संबंधी मुद्दों को देखता है।

प्रमुख बिंदु

राष्ट्रीय साइबर सुरक्षा रणनीति 2020

- **उद्देश्य**
  - इसका प्राथमिक उद्देश्य बेहतर ऑडिट प्रणाली के माध्यम से साइबर सुरक्षा और साइबर जागरूकता में सुधार लाना है।
  - इसके तहत सूचीबद्ध साइबर ऑडिटर, विभिन्न संगठनों की सुरक्षा से संबंधित सुविधाओं और विशेषताओं पर बारीकी से नज़र रखेंगे, जो कि वर्तमान में कानूनी रूप से आवश्यक है।
- **परिचय**
  - नीति के तहत यह मानते हुए कि साइबर हमले नियमित आधार पर हो सकते हैं, नियमित तौर पर साइबर संकट प्रबंधन अभ्यास का आयोजन किया जाएगा।
  - इस नीति में एक साइबर तत्परता सूचकांक की बात की गई है, जो कि साइबर सुरक्षा तत्परता की निगरानी करेगा।
  - साइबर सुरक्षा के लिये एक अलग बजट का सुझाव दिया गया है, ताकि अपेक्षित डोमेन ज्ञान वाली विभिन्न एजेंसियों की भूमिका और कार्यों के मध्य तालमेल स्थापित किया जा सके।



//

आवश्यकता

- **साइबर वार**

- 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।
  - 'सोलरविंड' नामक साइबर अटैक ने अमेरिका के महत्त्वपूर्ण राष्ट्रीय बुनियादी अवसंरचना को प्रभावित किया था।
- **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।

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
- राष्ट्रीय साइबर नीति, 2013

आगे की राह

- भारत वैश्विक स्तर पर 17 सबसे अधिक डिजिटल अर्थव्यवस्थाओं में दूसरा सबसे तेज़ी से डिजिटल प्रौद्योगिकी अपनाने वाला देश है और तीव्र डिजिटलीकरण के मद्देनज़र साइबर सुरक्षा के लिये दूरदर्शी उपाय अपनाना काफी महत्त्वपूर्ण है।
- निजी और सार्वजानिक निगमों अथवा सरकारी विभागों के लिये यह महत्त्वपूर्ण है कि वे अपने संगठनों की डिजिटल अवसंरचना में मौजूद विभिन्न सुभेद्यता जानें और उन्हें दूर करने के लिये एक प्रणाली का विकास करें।
- विभिन्न एजेंसियों और मंत्रालयों के बीच परिचालन समन्वय सुनिश्चित करने के लिये एक सर्वोच्च निकाय की आवश्यकता है।
- साइबर अवरोध को साइबर हमलों को रोकने के लिये रणनीतिक अवरोध के रूप में देखा जा सकता है। हमें साइबर स्पेस सुरक्षा सुनिश्चित करने के लिये

आक्रामक क्षमता हासिल करने की आवश्यकता है।

स्रोत: इंडियन एक्सप्रेस