साइबर सुरक्षा चुनौतियों का सामना

यह एडिटोरियल 25/02/2023 को 'द हिंदू' में प्रकाशित "Cyberattacks are rising, but there is an ideal patch" लेख पर आधारित है। इसमें साइबर सुरक्षा से संबद्ध चुनौतियों पर प्रकाश डाला गया है और साइबर सुरक्षा पर आम सहमति के लिये G20 अध्यक्षता के माध्यम से भारत की वृहत भूमिका की परिकल्पना की गई है।

संदर्भ

हाल की कुछ घटनाओं ने तेज़ी से बढ़ते हमारे डिजिटल नेटवर्क की विभिन्न कमज़ोरियों को उजागर किया है। पहला दृष्टांत AIIMS के सर्वर पर हुए हमले का है जिससे लगभग 40 मिलियन स्वास्थ्य रिकॉर्ड की गोपनीयता भंग हुई और दो सप्ताह तक सिस्टम आउटेज की स्थिति बनी रही।

- एक अन्य हमले में एक रैंसमवेयर समूह 'ब्लैककैट' (BlackCat) शामिल था जिसने रक्षा मंत्रालय के गोला-बारूद और विस्फोटक निर्माता सोलर इंडस्ट्रीज लिमिटेड की मातृ कंपनी की सुरक्षा को भंग किया और 2 टेराबाइट से अधिक डेटा की चोरी कर ली।
- भविष्य में इस तरह के हमलों को रोकने के लिये साइबर सुरक्षा उपायों को बढ़ाने की तत्काल आवश्यकता पर प्रकाश पड़ता है।

साइबर सुरक्षा से संबद्ध चुनौतियाँ

- **हाल के साइबर हमले:**
  - रैंसमवेयर हमले अधिक बारंबार और नुकसानदेह होते जा रहे हैं, जहाँ 75% से अधिक भारतीय संगठनों ने इस तरह के हमलों का सामना किया है और ऐसे प्रत्येक उल्लंघन में औसतन 35 करोड़ रुपए का नुकसान हुआ है।
- **महत्त्वपूर्ण अवसंरचना की भेद्यता:**
  - भौतिक और डिजिटल क्षेत्रों के बीच की रेखाएँ तेजी से धुंधली होती जा रही हैं, जिससे महत्त्वपूर्ण अवसंरचनाएँ शत्रु राज्य और अराजक अभिकर्ताओं के हमलों के प्रति अत्यंत संवेदनशील हो गई हैं।
  - साइबर क्षमताओं का उपयोग महत्त्वपूर्ण अवसंरचनाओं, उद्योग और सुरक्षा को कमज़ोर करने के लिये किया जा सकता है, जैसा कि यूक्रेन में जारी संघर्ष में देखा गया है जहाँ हैकिंग एवं जीपीएस जैमिंग का उपयोग कर वॉरहेड्स, रडार और संचार उपकरणों में इलेक्ट्रॉनिक प्रणाली को निष्क्रिय कर देने की बात सामने आई।
- **अधूरी तैयारी:**
  - CERT-In ने संगठनों के लिये कुछ दिशानिर्देश प्रस्तुत किये हैं जिनका डिजिटल आयाम से संपर्क के दौरान अनुपालन किया जाना चाहिये, लेकिन अधिकांश संगठनों के पास साइबर हमलों की पहचान करने और उन्हें रोक सकने के साधनों का अभाव है।
  - इसके अतिरिक्त, भारत में साइबर सुरक्षा पेशेवरों की भारी कमी की स्थिति पाई जाती है ।
- **सीमित निजी क्षेत्र की भागीदारी:**
  - भारत की साइबर सुरक्षा संरचनाओं में निजी क्षेत्र की भागीदारी सीमित है, जबकि साइबर हमलों से उपयोगकर्त्ताओं एवं ग्राहकों की सुरक्षा के लिये समान विचारधारा वाले अंतर-सरकारी एवं राज्य ढाँचे के साथ सहयोग आवश्यक है।
- **अतिरिक्त जटिलता:**
  - आर्टिफिशियल इंटेलिजेंस (AI), मशीन लर्निंग (ML), डेटा एनालिटिक्स, क्लाउड कंप्यूटिंग और इंटरनेट ऑफ थिंग्स (IoT) के अधिक समावेशन के साथ साइबर स्पेस के और जटिल डोमेन बनने की संभावना है जो तकनीकी-कानूनी (techno-legal) प्रकृति की समस्याओं को जन्म देगा।
  - 5G की शुरुआत और क्वांटम कंप्यूटिंग के आगमन से दुर्भावनापूर्ण सॉफ्टवेयर की शक्ति में वृद्धि होगी।

साइबर सुरक्षा के संबंध में प्रमुख पहलें

- **वैश्विक पहलें:**
  - **साइबर अपराध पर बुडापेस्ट कन्वेंशन:** यह एक अंतर्राष्ट्रीय संधि है जो राष्ट्रीय कानूनों के सामंजस्य, जाँच तकनीकों में सुधार और राष्ट्रों के बीच सहयोग को बढ़ाकर इंटरनेट एवं कंप्यूटर संबंधी अपराध को संबोधित करने का प्रयास करती है। यह 1 जुलाई 2004 को लागू

हुआ। भारत इस अभिसमय का हस्ताक्षरकर्ता नहीं है।
    - इंटरनेट गवर्नेंस फोरम (IGF): यह इंटरनेट गवर्नेंस विमर्श पर सभी हितधारकों, यानी सरकार, निजी क्षेत्र और नागरिक समाज को एक साथ लाता है।
    - **UNGA संकल्प:** संयुक्त राष्ट्र महासभा (UNGA) ने सूचना एवं संचार प्रौद्योगिकी (ICT) वातावरण में सुरक्षा के मुद्दों पर दो प्रक्रियाओं की स्थापना की है।
        - रूस द्वारा संकल्प के माध्यम से ओपन-एंडेड वर्किंग ग्रुप (OEWG)।
        - संयुक्त राज्य अमेरिका द्वारा संकल्प के माध्यम से सरकारी विशेषज्ञ समूह (GGE)।
- **भारतीय पहलें:**
    - राष्ट्रीय साइबर सुरक्षा रणनीति 2020: यह अधिक कड़े ऑडिट के माध्यम से साइबर जागरूकता और साइबर सुरक्षा में सुधार लाने की इच्छा रखता है। पैनल में शामिल साइबर ऑडिटर अब कानूनी रूप से आवश्यक होने की तुलना में संगठनों की सुरक्षा सुविधाओं पर अधिक ध्यान देंगे।
    - राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC): सूचना प्रौद्योगिकी अधिनियम, 2000 के तहत स्थापित NCIIPC महत्त्वपूर्ण सूचना अवसंरचना के संरक्षण एवं प्रत्यास्थता के लिये नोडल एजेंसी के रूप में कार्य करता है।
    - भारतीय साइबर अपराध समन्वय केंद्र (I4C): व्यापक और समन्वित तरीके से सभी प्रकार के साइबर अपराधों से निपटने के लिये इसे वर्ष 2020 में स्थापित किया गया था।
    - साइबर सुरक्षित भारत पहल: इसे वर्ष 2018 में साइबर अपराध के बारे में जागरूकता का प्रसार करने और मुख्य सूचना सुरक्षा अधिकारियों (CISOs) तथा सभी सरकारी विभागों के आईटी कर्मचारियों के लिये सुरक्षा उपायों हेतु क्षमता निर्माण करने के उद्देश्य से शुरू किया गया था।
    - साइबर स्वच्छता केंद्र: इस प्लेटफॉर्म को वर्ष 2017 में इंटरनेट उपयोगकर्त्ताओं के लिये वायरस एवं मैलवेयर को हटाते हुए अपने कंप्यूटर एवं अन्य उपकरणों को 'क्लीन' करने के उद्देश्य से पेश किया गया था।
    - **सूचना प्रौद्योगिकी अधिनियम, 2000:** यह अधिनियम कंप्यूटर, कंप्यूटर सिस्टम, कंप्यूटर नेटवर्क और इलेक्ट्रॉनिक प्रारूप में डेटा एवं सूचना के उपयोग को नियंत्रित करता है।
    - **राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल:** यह एक नागरिक-केंद्रित पहल है जो नागरिकों को साइबर अपराधों की ऑनलाइन रिपोर्टिंग में सक्षम बनाएगी और ये शिकायतें विधि-सम्मत कार्रवाई के लिये संबंधित कानून प्रवर्तन एजेंसियों द्वारा अभिगम्य होंगी।
    - **कंप्यूटर इमरजेंसी रिस्पांस टीम - भारत (CERT-In):** यह इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय का एक संगठन है जो साइबर घटनाओं पर सूचनाओं के संग्रहण, विश्लेषण और प्रसार से संलग्न है तथा यह साइबर सुरक्षा संबंधी घटनाओं पर चेतावनी भी जारी करता है।
    - **साइबर सुरक्षा संबंधी संधियाँ:** भारत ने अमेरिका, रूस, ब्रिटेन, दक्षिण कोरिया और यूरोपीय संघ जैसे देशों/समूहों के साथ विभिन्न साइबर सुरक्षा संधियों पर हस्ताक्षर किये हैं।
    - **बहुपक्षीय ढाँचे:** क्वाड (Quad) और I2U2 जैसे बहुराष्ट्रीय ढाँचों में भी साइबर घटनाओं पर प्रतिक्रियाओं, प्रौद्योगिकी सहयोग, क्षमता निर्माण एवं साइबर प्रत्यास्थता में सुधार हेतु सहयोग बढ़ाने के प्रयास किये जा रहे हैं।
    - **डिजिटल व्यक्तिगत डेटा संरक्षण विधेयक 2022 का मसौदा:** यह केवल वैध उद्देश्यों के लिये व्यक्तिगत डेटा के उपयोग को सुनिश्चित करने का लक्ष्य रखता है और डेटा उल्लंघनों के लिये 500 करोड़ रुपए तक का जुर्माना प्रस्तावित करता है।
    - **डिफेंस साइबर एजेंसी (DCyA):** यह भारतीय सशस्त्र बलों द्वारा स्थापित की गई है और आक्रामक एवं रक्षात्मक कार्रवाइयों में सक्षम है।

साइबर सुरक्षा पर आम सहमति के निर्माण लिये भारत G20 शिखर सम्मेलन का उपयोग कैसे कर सकता है?

- **G20 शिखर सम्मेलन के अवसर का उपयोग करना:** G20 शिखर सम्मेलन के मेजबान राष्ट्र के रूप में भारत इस अवसर का उपयोग साइबर सुरक्षा पर चर्चा करने के लिये शक्ति के वैश्विक साधन को संचालित करने वाले सभी हितधारकों को साथ लाने के लिये कर सकता है ।
- **एक वैश्विक ढाँचे का निर्माण:** भारत साइबर सुरक्षा के लिये साझा न्यूनतम स्वीकार्यता (common minimum acceptance) के वैश्विक ढाँचे की संकल्पना तैयार करने में अग्रणी भूमिका निभा सकता है। यह सामूहिक सुरक्षा में एक महत्त्वपूर्ण योगदान होगा और साइबर सुरक्षा पर आम सहमति बनाने की दिशा में एक महत्त्वपूर्ण कदम होगा ।
- जागरूकता का प्रसार: भारत साइबर सुरक्षा संबंधी मुद्दों के बारे में जागरूकता के प्रसार, निवारक उपाय करने के महत्त्व पर बल देने और प्रभावी साइबर सुरक्षा नीतियों को विकसित करने के लिये G20 शिखर सम्मेलन का उपयोग कर सकता है।

आगे की राह

- **अंतरराष्ट्रीय सहयोग:** साइबर सुरक्षा अनुसंधान एवं विकास में संयुक्त प्रयासों को सबल करने के माध्यम से वैश्विक सहयोग सुनिश्चित करना महत्त्वपूर्ण है, क्योंकि अधिकांश साइबर हमले सीमाओं से परे उत्पन्न होते हैं।
    - भारत क्वाड जैसे बहुपक्षीय पहलों के साथ ही बुडापेस्ट कन्वेंशन में शामिल होने पर विचार कर सकता है।
- **कमियों को दूर करना:** कॉर्पोरेट्स या संबंधित सरकारी विभागों के लिये यह महत्त्वपूर्ण है कि वे अपने संगठनों में कमियों का पता लगाएँ और उन कमियों को दूर करें तथा वहाँ एक स्तरित सुरक्षा प्रणाली का निर्माण करें जहाँ विभिन्न स्तरों के बीच सुरक्षा खतरे के संबंध में खुफिया जानकारी साझा की जा रही हो।
- **एक वास्तविक वैश्विक ढाँचे का निर्माण:** इसकी आवश्यकता है क्योंकि मौजूदा प्रयास 'साइलो' में चल रहे हैं (यानी विभिन्न संस्थाएँ एक ही ओर लक्षित हैं लेकिन आपस में सूचनाएँ साझा नहीं करतीं)। एक शीर्ष निकाय विभिन्न एजेंसियों के बीच परिचालन समन्वय सुनिश्चित करने में सक्षम होगा।

- **समन्वय और सूचना प्रसार:** इसके अतिरिक्त, साइबर सुरक्षा अनुसंधान एवं विकास गतिविधियों के समन्वयन और प्राथमिकीकरण को औपचारिक रूप देने और भेद्यता संबंधी सलाह एवं खतरे की चेतावनी को समयोचित रूप से प्रसारित करने की भी आवश्यकता है।

अभ्यास प्रश्न: महामारी के समय से ही भारत साइबर अपराधों के बढ़ते खतरे का सामना कर रहा है। भारत इन खतरों से कैसे निपट सकता है और साइबर सुरक्षा पर वैश्विक सहमति का विकास कैसे कर सकता है? भारत की G20 अध्यक्षता के संदर्भ में विश्लेषण कीजिये।

यूपीएससी सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न (PYQ)

[illegible]

Q.1 भारत में व्यक्तियों के लिये साइबर बीमा के तहत धन की हानि और अन्य लाभों के भुगतान के अलावा, निम्नलिखित में से कौन से लाभ आम तौर पर कवर किये जाते हैं? (वर्ष 2020)

1. किसी के कंप्यूटर तक पहुँच को बाधित करने वाले मैलवेयर के मामले में कंप्यूटर सिस्टम की बहाली की लागत।
2. एक नए कंप्यूटर की लागत अगर ऐसा साबित हो जाता है कि कुछ असामाजिक तत्त्वों ने जानबूझकर इसे नुकसान पहुँचाया है।
3. साइबर जबरन वसूली के मामले में नुकसान को कम करने के लिए एक विशेष सलाहकार को काम पर रखने की लागत।
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव की 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)

Q.2 भारत में निम्नलिखित में से किसके लिये साइबर सुरक्षा घटनाओं पर रिपोर्ट करना कानूनी रूप से अनिवार्य है? (वर्ष 2017)

1. सेवा प्रदाता
2. डेटा केंद्र
3. निगमित 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)

[illegible]

साइबर सुरक्षा के विभिन्न घटक क्या हैं? साइबर सुरक्षा में चुनौतियों को ध्यान में रखते हुए जाँच करें कि भारत ने व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति को किस हद तक सफलतापूर्वक विकसित किया है। (वर्ष 2022)

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/rising-up-to-cyber-security-challenges