भारत-ऑस्ट्रेलिया साइबर सुरक्षा संबंध

लेखक - बृजेश सिंह (वरिष्ठ आईपीएस अधिकारी)

यह आलेख सामान्य अध्ययन प्रश्न पत्र-II (अंतर्राष्ट्रीय संबंध) & III (साइबर सुरक्षा) से संबंधित है।

इंडियन एक्सप्रेस

27 अप्रैल, 2022

सहयोग को गहरा करने से आपसी समझ विकसित हो सकती है और साइबर उपकरणों तथा प्रौद्योगिकियों में पूरक बाज़ार बन सकते हैं, साथ ही दोनों महाद्वीपों पर द्विपक्षीय व्यापार और रणनीतिक प्रतिबद्धताओं को बढ़ावा मिल सकता है।

पश्चिमी देशों और मीडिया का ध्यान रूस और यूक्रेन के बीच संघर्ष पर केंद्रित है, लेकिन इन देशों ने हिंद-प्रशांत से अपनी नजरें नहीं हटाई हैं जहाँ बदलती विश्व व्यवस्था के स्पष्ट प्रमाण देखने को मिल जाएँगे। यह इस महीने की शुरुआत में वस्तुओं और सेवाओं में भारत-ऑस्ट्रेलिया आर्थिक सहयोग और व्यापार समझौते पर हस्ताक्षर में प्रकट होता है।

अफगानिस्तान से अमेरिका की असफल वापसी के बाद चीन ने नए आर्थिक, सैन्य और राजनीतिक गठबंधन बनाने में गंभीर रुचि ली और आसन्न ऊर्जा संकट की माँग है कि राष्ट्र अपने रणनीतिक और दीर्घकालिक हितों को फिर से संगठित करें। भारत-ऑस्ट्रेलिया ईसीटीए (ECTA) आम मूल्यों में द्विपक्षीय विश्वास का एक ठोस उदाहरण है। यह विश्वास व खतरों तथा लक्ष्यों की समझ का एक ठोस उदाहरण है और इसका एक प्रतिबिंब साइबर सुरक्षा में सहयोग है।

रूस-यूक्रेन संघर्ष ने दिखाया है कि साइबर खतरे के अभिनेता, राज्य और गैर-राज्य दोनों, हाइब्रिड या "अप्रतिबंधित" युद्ध में महत्वपूर्ण खिलाड़ी बन गए हैं। दोनों देशों ने सूचना के साथ-साथ परिचालन स्थान में दुर्भावनापूर्ण तत्वों को कमजोर कर दिया है, जबकि हैक्टिविस्ट समूह (अपराधियों का एक ऐसा समूह जो राजनीतिक कारणों के समर्थन में साइबर हमले करने के लिए एकजुट होते हैं) जैसे गैर-राज्य अभिनेताओं ने महत्वपूर्ण रूसी और बेलारूसी वित्तीय और सैन्य बुनियादी ढाँचे को महत्वपूर्ण नुकसान पहुँचाने का दावा किया है।

चीन पर बड़ी संख्या में साइबर हथियार जमा करने का आरोप है और उसने कथित तौर पर जासूसी, बौद्धिक संपदा की चोरी और कुछ देशों के इंटरनेट संसाधनों पर विनाशकारी हमलों के उद्देश्य से परिष्कृत ऑपरेशन किए हैं। ऑस्ट्रेलिया और भारत तथाकथित एडवांस्ड पर्सिस्टेंट थ्रेट (APT) समूहों द्वारा ऐसे कई अभियानों के निशानों पर रहे हैं, जो चीन द्वारा समर्थित या माना जाता है।

जून 2020 के आभासी द्विपक्षीय शिखर सम्मेलन में, प्रधानमंत्री नरेन्द्र मोदी और उनके ऑस्ट्रेलियाई समकक्ष स्कॉट मॉरिसन ने द्विपक्षीय संबंधों को एक व्यापक रणनीतिक साझेदारी तक बढ़ाया। नए साइबर ढाँचे में डिजिटल अर्थव्यवस्था, साइबर सुरक्षा और महत्वपूर्ण एवं उभरती प्रौद्योगिकियों पर एक साथ काम करने की पंचवर्षीय योजना शामिल है। इसे क्षेत्रीय साइबर में सुधार के लिए द्विपक्षीय अनुसंधान के लिए $ 9.7 मिलियन के फंड द्वारा समर्थित किया जाएगा।

एक वार्षिक साइबर नीति संवाद, साइबर सुरक्षा सहयोग पर एक नया संयुक्त कार्य समूह और आईसीटी पर एक संयुक्त कार्य समूह स्थापित किया गया है। साथ ही एक वार्षिक भारत-ऑस्ट्रेलिया विदेश मंत्री साइबर फ्रेमवर्क वार्ता आयोजित की जाएगी। भारत को अब अंतर्राष्ट्रीय साइबर रणनीति नामक एक प्रमुख ऑस्ट्रेलियाई पहल में शामिल किया जाएगा, जो 2017 में इंडोनेशिया, सिंगापुर और थाईलैंड में सक्रिय रूप से क्षमता निर्माण व्यवस्था का संचालन करने और मलेशिया, वियतनाम और कंबोडिया में इसी तरह की गतिविधियों का समर्थन करने के लिए शुरू हुआ था। वर्ष 2021 में ऑस्ट्रेलिया ने इस पहल में महत्वपूर्ण तकनीकों को जोड़ा, जिससे यह भारत और क्वाड के साथ द्विपक्षीय साझेदारी के लिए महत्वपूर्ण हो गया।

भारत को ऑस्ट्रेलिया की कम महत्वपूर्ण लेकिन स्मार्ट साइबर विशेषज्ञता से बहुत कुछ सीखना है। कैनबरा में ऑस्ट्रेलियाई साइबर सुरक्षा केन्द्र (एसीएससी) देश की साइबर सुरक्षा सूचना, सलाह और सहायता प्रयासों का भंडार है। यह राष्ट्रीय कानून प्रवर्तन, खुफिया एजेंसियों, अपराध जाँच और राष्ट्रीय सुरक्षा निकायों से विशेषज्ञता प्राप्त करता है। ACSC का कॉर्पोरेट जगत के साथ एक साझेदारी कार्यक्रम है ताकि खतरों पर खुफिया जानकारी साझा की जा सके। एक अन्य सरकारी प्रयास, ऑस्टसाइबर का उद्देश्य अंतर्राष्ट्रीय स्तर पर प्रतिस्पर्धी घरेलू साइबर सुरक्षा उद्योग स्थापित करना है।

भारत ने राष्ट्रीय साइबर सुरक्षा समन्वयक, एक राष्ट्रीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सीईआरटी-आईएन), एक राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण एजेंसी (एनसीआईआईपीसी) का कार्यालय स्थापित किया है और अपने साइबर को बढ़ाने के लिए सूचना प्रौद्योगिकी अधिनियम और नियमों में उचित संशोधन किए हैं। इसने वैश्विक साइबर सुरक्षा सूचकांक (GCI) 2020 में भारत की रैंक को 10वें स्थान पर पहुँचा दिया है, जो सिर्फ दो साल पहले 47वें स्थान पर था। भारत के पास सक्षम साइबर सुरक्षा पेशेवर हैं।

फरवरी में, भारत और ऑस्ट्रेलिया के विदेश मंत्रियों ने साइबर प्रशासन, साइबर सुरक्षा, क्षमता निर्माण, नवाचार, डिजिटल अर्थव्यवस्था, साइबर और महत्वपूर्ण प्रौद्योगिकियों में सहयोग को दोनों देशों के बीच संबंधों के एक आवश्यक स्तंभ के रूप में मान्यता दी है। महत्वपूर्ण और उभरती प्रौद्योगिकी नीति के लिए एक संयुक्त उत्कृष्टता केन्द्र, बेंगलुरु में स्थापित किया जाएगा।

भारत और ऑस्ट्रेलिया 5G रोलआउट, APT समूहों द्वारा खतरे, साइबर अपराध, सूचना संग्राम (information warfare) और एक लोकतांत्रिक व्यवस्था के लिए खतरों के बारे में समान चिंताओं को साझा करते हैं। सहयोग को गहरा करने से आपसी समझ विकसित हो सकती है और साइबर उपकरणों और प्रौद्योगिकियों में पूरक बाज़ार बन सकते हैं, साथ ही दोनों महाद्वीपों पर द्विपक्षीय व्यापार और रणनीतिक प्रतिबद्धताओं को बढ़ावा मिल सकता है।

GS World
Committed To Excellence

जीएस वर्ल्ड टीम इनपुट

IN THE NEWS

क्या है साइबर सुरक्षा?

- साइबर सुरक्षा से अभिप्राय एक तरह की इंटरनेट सिक्योरिटी से है, जो आपको मैलवेयर, ब्लैक हैट हैकर्स या किसी अन्य तरह के साइबर हमलों से बचाती है।
- अगर आप इंटरनेट का उपयोग बैंकिंग से जुड़ी गतिविधियों को अंजाम देने के लिए करते हैं, तो आपको अपने डिवाइस में साइबर सिक्योरिटी को ध्यान में रखते हुए एंटीवायरस को जरूर इंस्टॉल करना चाहिए।

साइबर अपराध क्या है?

- साइबर अपराध को साइबर क्राइम या कंप्यूटर क्राइम भी कहा जाता है। साइबर अपराध एक प्रकार की गैर कानूनी गतिविधि है, जिसे इंटरनेट या डिजिटल माध्यमों की सहायता से अंजाम दिया जाता है। सामान्य शब्दों में डिजिटल या इंटरनेट माध्यमों से होने वाला कोई भी अपराध साइबर अपराध कहलाता है।

साइबर अपराध के विभिन्न रूप

- साइबर अपराध इंटरनेट कंप्यूटर या किसी अन्य इंटर-कनेक्टेड बुनियादी ढाँचे सहित आपराधिक गतिविधि को दर्शाता है। यह इ-क्रेडिट कार्ड धोखाधड़ी, अवैध डाउनलोडिंग, औद्योगिक जासूसी चाइल्ड, पोर्नोग्राफी घोटाले, साइबर आतंकवाद सृजन वायरस के वितरण स्पैम जैसे अपराधों को कवर करता है।

राष्ट्रीय साइबर सुरक्षा रणनीति 2020

- कड़े ऑडिट के माध्यम से साइबर जागरूकता और साइबर सुरक्षा में सुधार के उद्देश्य से राष्ट्रीय साइबर सुरक्षा रणनीति 2020 का मसौदा तैयार किया गया था। इस नीति के तहत, पैनल में शामिल साइबर ऑडिटर संगठनों की सुरक्षा विशेषताओं को ध्यान से देखेंगे।

Committed To Excellence

संभावित प्रश्न (प्रारंभिक परीक्षा)

प्र. निम्नलिखित कथनों पर विचार कीजिए-

1. वैश्विक साइबर सुरक्षा सूचकांक (GCI) 2020 में भारत की रैंक 10वें स्थान पर थी।
2. वैश्विक साइबर सुरक्षा सूचकांक (GCI) अंतर्राष्ट्रीय दूरसंचार संघ (ITU) द्वारा जारी की जाती है।

उपर्युक्त में से कौन-सा/से कथन सही नहीं है/हैं?

(क) केवल 1
(ख) केवल 2
(ग) 1 और 2 दोनों
(घ) न तो 1, न ही 2

Expected Question (Prelims Exams)

Q. Consider the following statements:-

1. India was ranked 10th in the Global Cyber Security Index (GCI) 2020.
2. The Global Cyber Security Index (GCI) is released by the International Telecommunication Union (ITU).

Which of the above statement (s) is/are not correct?

(a) 1 only
(b) 2 only
(c) Both 1 and 2
(d) Neither 1 nor 2

संभावित प्रश्न (मुख्य परीक्षा)

प्र. साइबर खतरा क्या है? विभिन्न प्रकार के साइबर अपराधों का उल्लेख करते हुए सरकार द्वारा साइबर अपराधों के समाधान हेतु उठाए गए विभिन्न कदमों का विश्लेषण करें। (250 शब्द)

Q. What is Cyber Threat? While mentioning different types of cyber-crimes, analyze the various steps taken by the government to prevent cyber-crimes. (250 Words)

World
Committed To Excellence

नोट :- अभ्यास के लिए दिया गया मुख्य परीक्षा का प्रश्न आगामी UPSC मुख्य परीक्षा को ध्यान में रख कर बनाया गया है। अतः इस प्रश्न का उत्तर लिखने के लिए आप इस आलेख के साथ-साथ इस टॉपिक से संबंधित अन्य स्त्रोतों का भी सहयोग ले सकते हैं।