भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

राज्य सभा

अतारांकित प्रश्न संख्या 3443

जिसका उत्तर 01 अप्रैल, 2022 को दिया जाना है।

11 चैत्र, 1944 (शक)

साइबर हमलों संबंधी आँकड़ा

3443. श्री जी. सी. चन्द्रशेखर:
श्री कुमार केतकर:
श्रीमती फूलो देवी नेतम:
डा. एल. हनुमंतय्या:

क्या इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री यह बताने की कृपा करेंगे कि:

(क) क्या सरकार उन साइबर हमलों से संबंधित आँकड़े अनुरक्षित रखती है जो विदेशी और घरेलू संस्थानों द्वारा भारत सरकार तथा सरकारी-स्वायित्व वाली संस्थाओं के विरूद्ध हुए हैं;
(ख) यदि हां, तो मूल देश और पहचान तथा रोकथाम के बीच की औसत समयावधि सहित वर्ष 2016 से तत्संबंधी ब्यौरा क्या है, यदि नहीं, तो इसके क्या कारण हैं; और
(ग) क्या सरकार के पास हाइब्रिड वॉरफेयर की स्थिति से निपटने की क्षमता है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री राजीव चंद्रशेखर)

(क) और (ख): सरकार विभिन्न साइबर सुरक्षा खतरों से पूरी तरह परिचित और जागरूक है। भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) को भारत में साइबर सुरक्षा की घटनाओं पर नज़र रखने और निगरानी करने का काम सौंपा गया है।

सर्ट-इन ने सूचित किया है कि वर्ष 2016, 2017, 2018, 2019, 2020 और 2021 के दौरान सरकारी संगठनों से संबंधित क्रमशः कुल 5461, 33514, 70798, 85797, 54314 और 48285 साइबर सुरक्षा घटनाएं हुई हैं।

भारतीय साइबर स्पेस पर साइबर हमले करने के लिए समय-समय पर प्रयास किए जाते हैं। यह देखा गया है कि हमलावर दुनिया के विभिन्न हिस्सों में स्थित कंप्यूटर प्रणाली से छेड़छाड़ करते हैं और हमले करने के लिए उपयोग की जाने वाली वास्तविक प्रणाली की पहचान छिपाने के लिए छद्म तकनीक और छिपे हुए सर्वर का उपयोग करते हैं।

विश्लेषित और भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) को उपलब्ध कराए गए लॉग के अनुसार, उन कंप्यूटरों के इंटरनेट प्रोटोकॉल (आईपी) पते जहां से हमलों की उत्पत्ति हुई प्रतीत होती है में अल्जीरिया, ब्राजील, चीन, फ्रांस, जर्मनी, हांगकांग, इंडोनेशिया, नीदरलैंड, उत्तर कोरिया, पाकिस्तान, रूस, सर्बिया, दक्षिण कोरिया, ताइवान, थाईलैंड, ट्यूनीशिया, तुर्की, संयुक्त राष्ट्र अमेरिका, वियतनाम आदि जैसे विभिन्न देश शामिल हैं।

सर्ट-इन, अंतरराष्ट्रीय सर्ट, विदेशी संगठनों और सेवा प्रदाताओं के साथ-साथ कानून प्रवर्तन एजेंसियों के साथ सहयोग करता है, काम करता है और घटना प्रतिक्रिया उपायों का समन्वय करता है।

(ग): इस मंत्रालय के पास ऐसी कोई सूचना उपलब्ध नहीं है।

हालांकि, भारत सरकार ने हाइब्रिड खतरों सहित साइबर खतरों से प्रभावी ढंग से निपटने के लिए उपाय किए हैं, जिनमें अन्य बातों के साथ-साथ शामिल हैं:

i. सरकार ने केंद्र सरकार के सभी मंत्रालयों/विभागों, राज्य/संघ राज्य क्षेत्रों की सरकारों और उनके संगठनों द्वारा साइबर हमलों और साइबर आतंकवाद से निपटने के लिए साइबर संकट प्रबंधन योजना (सीसीएमपी) तैयार की है, इसमें साइबर चैनलों के माध्यम से हाइब्रिड खतरों और प्रभाव को भी शामिल किया गया है। इसके अलावा, क्षेत्रीय संकट प्रबंधन योजनाओं के विकास और कार्यान्वयन में सहायता के लिए दिशानिर्देश दस्तावेज और टेम्पलेट प्रकाशित किए जाते हैं। सीसीएमपी का उद्देश्य रणनीतिक ढांचे की स्थापना करना और किसी साइबर-संकट से उबरने हेतु तैयार करने, प्रतिक्रिया देने और क्षतिपूर्ति समन्वय करने के कार्यों संबंधी मार्गदर्शन करना है।

ii. सर्ट-इन मंत्रालयों, विभागों, राज्यों और संघ राज्य क्षेत्रों और महत्वपूर्ण संगठनों के लिए साइबर सुरक्षा खतरे के परिदृश्य के बारे में उन्हें संवेदनशील बनाने के लिए नियमित रूप से कार्यशालाओं का आयोजन करता है, जिसमें हाइब्रिड प्रभाव के साइबर वैक्टर शामिल हैं। यह उन्हें साइबर संकट प्रबंधन योजना तैयार करने और कार्यान्वित करने में सक्षम बनाता है अब तक कुल 128 कार्यशालाएं आयोजित की जा चुकी हैं इनमें से वर्ष 2021 के दौरान 31 सीसीएमपी कार्यशालाएं आयोजित की गई हैं।

iii. सरकारी और महत्वपूर्ण क्षेत्रों में संगठनों की साइबर सुरक्षा संबंधी स्थिति और तैयारी के आकलन को सक्षम करने के लिए साइबर सुरक्षा मॉक ड्रिल और टेबल टॉप अभ्यास नियमित रूप से आयोजित किए जाते हैं जिसमें हाइब्रिड इन्फ़्लुएन्सिन साइबर वैक्टर शामिल हैं। सर्ट-इन द्वारा ऐसे 64 अभ्यास आयोजित किए गए हैं जिनमें विभिन्न राज्यों और क्षेत्रों के 820 संगठनों ने भाग लिया।

****