भारत सरकार

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय

लोक सभा

अतारांकित प्रश्न संख्या 3887

जिसका उत्तर 11 दिसम्बर, 2019 को दिया जाना है।

20 अग्रहायण, 1941 (शक)

भारतीय वेबसाइटों को हैक करना

3887. श्री भर्तृहरि महताब :

श्री राहुल रमेश शेवाले :

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

(क) क्या हाल ही के वर्षों में विदेशों में भारतीय वेबसाइटों से साइबर अपराधों और हैकिंग के मामलों में वृद्धि हुई है;

(ख) यदि हां, तो गत तीन वर्षों में प्रत्येक वर्ष और चालू वर्ष के दौरान दर्ज की गयी ऐसी घटनाओं की संख्या सहित तत्संबंधी देश-वार ब्यौरा क्या है और इसके क्या कारण हैं;

(ग) क्या उक्त अवधि के दौरान भारतीय शिष्टमंडलों ने संचार और आईटी के क्षेत्र में द्विपक्षीय सहयोग के तहत उक्त देशों का दौरा किया है;

(घ) यदि हां, तो तत्संबंधी ब्यौरा क्या है और इसके निष्कर्ष क्या रहे और इस तरह के संवाद में किन मुद्दों पर चर्चा की गई है; और

(ड.) साइबर अपराधों को रोकने के लिए और विदेशों द्वारा भारतीय वेबसाइटों की हैकिंग को रोकने और विदेशों की गतिविधियों पर नजर रखने के लिए क्या सुरक्षा उपाय मौजूद हैं और उसकी क्या उपलब्धियां रही हैं ?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री संजय धोत्रे)

(क) और **(ख) :** भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) को रिपोर्ट की गई और उसके द्वारा ट्रैक की गई सूचना के अनुसार केन्द्र सरकार के मंत्रालय/विभागों और राज्य सरकारों की कुल 33147, 30067, 17560 और 21467 भारतीय वेबसाइटों को क्रमश: वर्ष 2016, 2017, 2018 और 2019 (अक्टूबर तक) के दौरान हैक किया गया।

भारतीय साइबर स्पेस पर साइबर हमले शुरू करने के लिए समय-समय पर प्रयास किए गए हैं। ऐसा देखा गया है कि हमलावर विश्व के विभिन्न भागों में स्थित कम्प्यूटर प्रणालियों के साथ छेड-छाड़ कर रहे हैं तथा वास्तविक प्रणालियों, जिनसे हमले किए जा रहे की पहचान छिपाने के लिए छदम वेष तकनीक और अदृश्य सर्वरों का प्रयोग करते हैं।

विश्लेषित किए गए और सर्ट-इन को उपलब्ध कराए गए लॉग के अनुसार ऐसी प्रतीत होता है कि कम्प्यूटरों, जहां से हमले किए गए हैं, के इन्टरनेट प्रोटोकॉल (आईपी) अड्रेस चीन, पकिस्तान, नीदरलैंड, फ्रांस, ताइवान, टूनिशिया, रूस, अलजेरिया और सर्बिया सहित विभिन्न देशों से संबंधित हैं।

(ग), (घ) और **(ङ) :** देश के बाहर ऐसी घटनाओं में शामिल प्रणालियों के समाधान के लिए सर्ट-इन बाहर के देशों में अपनी समकक्ष एजेसियों के साथ समन्वय स्थापित कर प्रति उपाय करता है।

सरकार ने देश ने देश में साइबर सुरक्षा की घटनाओं को रोकने और साइबर सुरक्षा बढ़ाने के लिए कई उपाए किए हैं। इनमें अन्य बातों के साथ-साथ निम्नलिखित उपाय शामिल हैं :

(i) सरकार ने सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 70क के प्रावधानों के अनुसार देश में महत्वपूर्ण सूचना अवसंरचना के संरक्षण के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (एनसीआईआईपीसी) की स्थापना की है।

(ii) भारतीय कंप्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) कम्प्यूटर और नेटवर्कों का सुरक्षित इस्तेमाल सुनिश्चित करने के लिए नियमित आधार पर नवीनतम साइबर खतरों / सुभेदताओं और प्रतिउपाय के संबंध में चेतावनी और परामर्शी निदेश जारी करता है।

(iii) सरकार ने अनुप्रयोगों/अवसंरचना की सुरक्षा के लिए मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) के लिए दिशानिर्देश और अनुपालन के लिए उनकी प्रमुख भूमिकाओं तथा जिम्मेदारियों से संबंधित निर्देश जारी किए हैं।

(iv) सभी सरकारी वेबसाइटों और एप्लीकेशनों को उनकी होस्टिंग के पहले साइबर सुरक्षा के संदर्भ में लेखापरीक्षित किया जाना है। होस्टिंग के बाद भी नियमित आधार पर वेबसाइटों और अनुप्रयोगों की लेखापरीक्षा की जाती है

(v) सरकार ने सूचना सुरक्षा श्रेष्ठ पद्धतियों के कार्यान्वयन में सहायता देने और लेखापरीक्षा करने के लिए 90 साइबर सुरक्षा लेखापरीक्षा संगठनों की पैनलबद्ध किया है।

(vi) केन्द्र सरकार के सभी मंत्रालयों/विभागों, राज्य सरकारों/संघ राज्य क्षेत्रों और उनके संगठनों तथा महत्वपूर्ण क्षेत्रों द्वारा कार्यान्वयन के लिए सरकार ने साइबर हमलों से निपटने के लिए साइबर आपदा प्रबंधन योजना तैयार की है।

(vii) सरकारी और महत्वपूर्ण क्षेत्रों के संगठनों की साइबर सुरक्षा की स्थिति और तैयारी का मूल्यांकन करने में उन्हें सक्षम बनाने के लिए नियमित रूप से साइबर सुरक्षा अभ्यासों (मॉक ड्रिल) का संचालन किया जा रहा है। अब तक भारतीय कंप्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) द्वारा इस प्रकार के 44 अभ्यास संचालित किए हैं जिनमें वित्त, रक्षा, विद्युत, दूरसंचार, परिवहन, ऊर्जा, अंतरिक्ष आईटी/आईटीईएस इत्यादि क्षेत्रों जैसे विभिन्न राज्यों और क्षेत्रों के 265 संगठनों के प्रतिभागियों ने भाग लिया

(viii) सर्ट-इन सरकार और महत्वपूर्ण क्षेत्र के संगठनों के मुख्य सुरक्षा अधिकारी (सीआईएसओ) और नेटवर्क/प्रणाली प्रशासकों के लिए आईटी अवसंरचना को सुरक्षित करने और साइबर हमलों के उन्मूलन के लिए नियमित रूप से प्रशिक्षण कार्यक्रम आयोजित करता है। वर्ष 2019 (अक्टूबर तक) में ऐसे उन्नीस (19) प्रशिक्षण कार्यक्रमों का आयोजन किया गया जिसमें 515 भागीदारों ने हिस्सा लिया।

(ix) सरकार ने साइबर स्वच्छता केंद्र (बोटनेट क्लीनिंग और मालवेयर एनालिसिस सेंटर) स्थापित किया है। यह केंद्र मैलीशियस प्रोग्रामों का पता लगाने और उन्हें हटाने के लिए नि:शुल्क टूल उपलब्ध करा रहा है।

(x) सरकार ने विद्यमान और संभावित साइबर सुरक्षा खतरों के बारे में आवश्यक परिस्थितिजन्य जागरूकता पैदा करने और अलग-अलग इकाइयों द्वारा सक्रिय, निवारक और सुरक्षात्मक कार्रवाई करने के लिए समय पर सूचना साझा करने के लिए राष्ट्रीय साइबर समन्वय केन्द्र (एनसीसीसी) की स्थापना शुरू की है। एनसीसीसी के चरण-I को प्रचालनरत किया गया है।

*****