भारत सरकार

**इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय**

**लोक सभा**

**अतारांकित प्रश्न संख्या 4694**

जिसका उत्तर 24 मार्च, 2021 को दिया जाना है।

2021/3 चैत्र, 1943 (शक)

**चीनी एजेंसियों द्वारा साइबर हमला**

**4694. श्री राजेन्द्र धेड्या गावित:**
**श्री सुब्रत पाठक:**
**श्री रविन्दर कुशवाहा:**
**श्री रवि किशन:**
**श्री सुधीर गुप्ता:**
**श्री श्रीरंग आप्पा बारणे:**
**श्री चंद्र शेखर साहू:**
**श्री बिद्युत बरन महतो:**
**श्री संजय सदाशिवराव मांडलिक:**

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

(क) क्या हाल में चीनी मालवेयर एजेंसियों द्वारा भारत के पावर ग्रिड और कोविड-19 टीके की विनिर्माता कंपनियों पर साइबर हमलों के मामले सरकार के संज्ञान में आए हैं तथा यदि हां, तो तत्संबंधी ब्यौरा क्या है एवं सरकार की इस पर क्या प्रतिक्रिया है और सरकार द्वारा इस संबंध में क्या कदम उठाए गए हैं;

(ख) क्या सरकार ने हाल में ऐसे विभिन्न साइबर हमलों की जांच की है एवं यदि हां, तो इसके क्या परिणाम रहे हैं;

(ग) क्या ऐसी कोई आंतरिक एजेंसी है जहां ऐसे मामलों की रिपोर्ट दर्ज की जाती है और जांच की जाती है एवं यदि हां, तो तत्संबंधी ब्यौरा क्या है; और

(घ) क्या सरकार ने अभी तक ऐसे मामलों को उक्त एजेंसी के समक्ष उठाया है एवं यदि हां, तो तत्संबंधी ब्यौरा क्या है और सरकार को इस संबंध में क्या प्रतिक्रिया प्राप्त हुई है?

उत्तर

**इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री संजय धोत्रे)**

**(क) और (ख) :** भारतीय कंप्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) सूचना प्रौद्योगिकी अधिनियम, 2000 की धारा 70(ख) के प्रावधानों के अनुसार साइबर सुरक्षा से संबंधित घटनाओं का जवाब देने के लिए राष्ट्रीय एजेंसी के रूप में सेवारत है। सर्ट-इन क्षेत्रों में निकायों के नेटवर्क में मालवेयर संक्रमणों के बारे में धमकी असूचना संसाधनों तथा अपने स्थिति जन्य जागरुकता से इनपुट प्राप्त करते हैं तथा उपचारात्मक उपायों के लिए संबंधित संगठनों तथा क्षेत्रीय सीईआरटी के लिए अलर्ट जारी करते हैं। ऐसा देखा गया है कि आक्रमणकर्ता विश्व के विभिन्न भागों में स्थिति कम्प्यूटर प्रणाली से छेड़-छाड़ कर रहे हैं और वास्तिविक प्रणाली जिससे हमले किए जा रहे हैं की पहचान को छिपाने के लिए छद्मवेष तकनीकों और हिडेन सर्वरों का प्रयोग कर रहे हैं।

उभरते साइबर हमलों के विरुद्ध जवाब देने और उपायों की रोकथाम के लिए प्रमुख संगठनों और क्षेत्रीय सीईआरटी के लिए अलर्ट और परामर्शी निर्देश जारी किए जाते हैं।

सरकार ने देश में साइबर सुरक्षा स्थिति को बढ़ाने और साइबर हमले को रोकने के लिए निम्नलिखित कदम उठायें हैं :-

i. भारतीय कंप्यूटर आपात प्रतिक्रिया दल (सर्ट-इन) नियमित आधार पर कंप्यूटर को सुरक्षित करने के लिए नवीनतम साइबर खतरों/सुभेद्यताओं और प्रति उपाय के संबंध में चेतावनी और परामर्शी निदेश जारी करता है।

ii. सरकार ने अनुप्रयोगों/अवसंरचना और अनुपालन 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।

iii. 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।

iv. सरकार ने सूचना सुरक्षा श्रेष्ठ पद्धतियों के कार्यान्वयन में सहायता देने और लेखापरीक्षा करने के लिए साइबर सुरक्षा लेखापरीक्षा संगठनों को पैनलबद्ध किया है।

v. 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 (सीसीएमपी) तैयार की है।

vi. सरकारी और महत्वपूर्ण क्षेत्रों में साइबर सुरक्षा अभ्यासों (मॉक ड्रिल) का संचालन नियमित रूप से किया जा रहा है।

vii. सर्ट-इन आईटी अवसंरचना को सुरक्षित करने और साइबर हमले को कम करने के संबंध में 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।

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

ix. सरकार ने विद्यमान और संभावित साइबर सुरक्षा खतरों के बारे में आवश्यक परिस्थितिजन्य जागरूकता पैदा करने के लिए राष्ट्रीय साइबर समन्वय केन्द्र (एनसीसीसी) की स्थापना की है। एनसीसीसी के चरण-I को प्रचालनरत किया गया है।

**(ग) और (घ) :** इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय (एमईआईटीवाई) के पास इस तरह की कोई जानकारी उपलब्ध नहीं है।

********