भारत सरकार

विद्युत मंत्रालय

....

लोक सभा

अतारांकित प्रश्न संख्या-4890

जिसका उत्तर 25 मार्च, 2021 को दिया जाना है।

साइबर हमले से पावरग्रिड की रक्षा

4890. श्री प्रवेश साहिब सिंह वर्मा:
श्री सुधाकर तुकाराम श्रंगरे:
श्री रवनीत सिंह:
सुश्री प्रतिमा भौमिक:
श्री प्रदीप कुमार सिंह:
श्री सुमेधानन्द सरस्वती:
श्री उत्तम कुमार रेड्डी:
श्री प्रताप सिन्हा:
श्री भगवंत खुबा:
श्री सय्यद ईमत्याज जलील:
श्री असादुद्दीन ओवैसी:
श्री डी.एम. कथीर आनन्द:

क्या **विद्युत** मंत्री यह बताने की कृपा करेंगे किः

(क) क्या सरकार ने साइबर हमलों से देश में ऊर्जा आपूर्ति ग्रिड की भेद्यताओं की पहचान करने के लिए कोई अध्ययन कराए हैं;

(ख) यदि हां, तो तत्संबंधी ब्यौरा क्या है और यदि नहीं, तो इसके क्या कारण हैं;

(ग) पिछले दो वर्षों तथा चालू वर्ष के दौरान पावरग्रिड पर साइबर हमलों और ऊर्जा आपूर्ति प्रणाली में पाए गए मैलवेयर के मामलों एवं स्रोतों की संख्या तथा ब्यौरा क्या है;

(घ) क्या देशभर में विद्युत आपूर्ति का प्रबंध देखने वाली ग्रिड पर उक्त साइबर हमलों के कारण कुछ राज्यों को बिजली के ब्लैक आउट अथवा व्यापक रूप से बिजली गुल होने का सामना करना पड़ा और यदि हां, तो इस संबंध मे तथ्यात्मक स्थिति क्या है;

(ड़) क्या सरकार ने इस संबंध में कोई जांच कराई है और भविष्य में इस प्रकार के साइबर हमलों से पावर ग्रिडों की सुरक्षा सुनिश्चित करने के लिए क्या उपाय किए गए हैं/किए जा रहे हैं;

(च) यदि हां, तो तत्संबंधी ब्यौरा क्या है और यदि नहीं, तो इसके क्या कारण हैं; और

(छ) क्या सरकार का विचार देश में ऊर्जा आपूर्ति अवसंरचना की साइबर सुरक्षा की निगरानी हेतु एक दल गठित करने का है और यदि हां, तो तत्संबंधी ब्यौरा क्या है?

उत्तर

विद्युत और नवीन एवं नवीकरणीय ऊर्जा राज्य मंत्री (स्वतंत्र प्रभार) तथा कौशल विकास एवं उद्यमशीलता राज्य मंत्री (श्री आर.के. सिंह)

(क) और (ख) : सूचना प्रौद्योगिकी संशोधन अधिनियम, 2008 के अनुसार, देश में साइबर घटनाओं की सूचना का संग्रहण, विश्लेषण और प्रसारण के लिए भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सीईआरटी-इन) को राष्ट्रीय एजेंसी

के रूप में नामित किया गया है। सीईआरटी-इन नवीनतम साइबर खतरों/अरक्षितताओं तथा नियमित आधार पर कम्प्यूटरों और नेटवर्कों को सुरक्षित रखने के लिए प्रत्युपायों से संबंधित चेतावनियों तथा एडवाईजरी भी जारी करते हैं। इसके अतिरिक्त, सूचना प्रौद्योगिकी (आईटी) अधिनियम, 2000 की धारा 70क के प्रावधानों के अनुसार, सरकार ने देश में महत्वपूर्ण सूचना अवसंरचना को सुरक्षित रखने के लिए राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केन्द्र (एनसीआईआईपीसी) की स्थापना की है। विद्युत मंत्रालय (एमओपी) ने देश में विद्युत प्रणाली के सुदृढ़ीकरण के लिए क्षेत्रीय कम्प्यूटर आपात प्रतिक्रिया दल (सीईआरटी) नामत: सीईआरटी-तापीय, सीईआरटी-जल, सीईआरटी-वितरण, सीईआरटी-पारेषण, सीईआरटी-ग्रिड संचालन आदि की स्थापना की है ताकि साइबर हमले इसे बाधित न कर सके और हमारे सिस्टमों पर साइबर हमले के किसी भी प्रकार का तुंरत पता लगाया तथा उसका मुकाबला किया जा सके।

(ग) : हाल ही में, पावर सिस्टम ऑपरेशन कॉर्पोरेशन (पोसोको), के दक्षिण क्षेत्रीय भार प्रेषण केंद्र (एसआरएलडीसी), पश्चिमी क्षेत्रीय भार प्रेषण केंद्र (डब्ल्यूआरएलडीसी) तथा उत्तर-पूर्व क्षेत्रीय भार प्रेषण केंद्र (एनईआरएलडीसी) एनटीपीसी कुडगी और तेलंगाना राज्य ट्रांस्को द्वारा साइबर घटनाएं सूचित की गई हैं। इन संगठनों द्वारा आवश्यक पृथक्करण और अन्य सुरक्षा उपाय किए गए हैं। इसके अतिरिक्त, इन घटनाओं का विस्तृत विश्लेषण सीईआरटी-इन के मार्गदर्शन के तहत प्रक्रियाधीन है।

(घ) : जी नहीं।

(ङ) और (च) : साइबर हमले की घटनाओं की जांच की गई है। अतिरिक्त जांच तथा विश्लेषण प्रक्रियाधीन हैं। सरकार ने साइबर सुरक्षा की स्थिति को मजबूत करने तथा साइबर हमलों की रोकथाम करने के लिए निम्नलिखित उपाय किए हैं:

(i) भारतीय कम्प्यूटर आपात प्रतिक्रिया दल (सीईआरटी-इन) नवीनतम साइबर खतरों/अरक्षितताओं तथा नियमित आधार पर कम्प्यूटरों और नेटवर्कों को सुरक्षित रखने के लिए प्रत्युपायों से संबंधित चेतावनी तथा एडवाईजरी जारी करते हैं।

(ii) सरकार ने अनुप्रयोगों/अवसंरचना को सुरक्षित करने तथा उसके अनुपालन के लिए मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) के संबंध में उनकी प्रमुख भूमिकाओं और उत्तरदायित्वों से संबंधित दिशानिर्देश जारी किए हैं।

(iii) सभी सरकारी वेबसाइटों तथा अनुप्रयोगों का साइबर सुरक्षा के मद्देनजर उनकी आयोजना करने से पूर्व संपरीक्षा की जानी है। आयोजना करने के बाद भी वेबसाइटों तथा अनुप्रयोगों की संपरीक्षा नियमित आधार पर की जाएगी।

(iv) सरकार ने सूचना सुरक्षा के सर्वोत्तम प्रथाओं के संपरीक्षा कार्यान्वयन तथा समर्थन के लिए सुरक्षा संपरीक्षा संगठनों को पैनलबद्ध किया है।

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

(vi) सरकारी तथा महत्वपूर्ण क्षेत्रों में साइबर सुरक्षा मॉक ड्रिल नियमित आधार पर संचालित किए जाते हैं।

(vii) सीईआरटी-इन आईटी अवसंरचना को सुरक्षित बनाने तथा साइबर हमलों को कम करने हेतु सरकार तथा महत्वपूर्ण क्षेत्रीय संगठनों के नेटवर्क/सिस्टम प्रशासकों और मुख्य सूचना सुरक्षा अधिकारियों (सीआईएसओ) के लिए नियमित प्रशिक्षण कार्यक्रम संचालित करता है।

(viii) सरकार साइबर सुरक्षा केन्द्र (बोटनेट क्लीनिंग एंड मॉलवेयर एनालिसिस सेंटर) का संचालन कर रही है। केन्द्र द्वेषपूर्ण प्रोग्रामों का पता लगा रहा है और हटाने के लिए निःशुल्क उपस्कर प्रदान कर रहा है।

(ix) सरकार ने मौजूदा और संभावित साइबर सुरक्षा खरतों के संबंध में आवश्यक स्थितिपरक जागरूकता उत्पन्न करने के लिए राष्ट्रीय साइबर समन्वय केन्द्र (एनसीसीसी) की स्थापना की है। एनसीसीसी का चरण-I प्रचालन में है।

(छ) : विद्यत मंत्रालय (एमओपी) के स्तर पर, मार्च, 2017 में भारतीय विद्युत पारेषण क्षेत्र में प्रवेश चाहने वाली विद्युत फर्मों तथा साइबर सुरक्षा से संबंधित मुद्दों पर विचार करने के लिए एक समिति का गठन किया गया है। तदनुसार, अगस्त, 2019 में अपनी पारेषण प्रणालियों में सिस्टम सुरक्षा बढ़ाने के लिए तरीकों तथा साधनों की जांच हेतु एक समिति का गठन किया गया था।

उपर्युक्त के साथ-साथ, मार्च, 2020 में अधिकारियों के एक समूह को विद्युत क्षेत्र में साइबर हमले के संबंध में संविदात्मक तथा विधायी मुद्दों के अध्ययन के लिए गठित किया गया था। समिति की रिपोर्ट प्राप्त हो गई है और यह विद्युत क्षेत्र में साइबर सुरक्षा को और अधिक सुदृढ़ बनाने हेतु उपाय करने के लिए जांच/विचार-विमर्श के अधीन है। सितंबर, 2020 में, आयातित उपकरणों के लिए प्रयोगशालाओं तथा जांच नयाचारों पर निर्णय लेने के लिए एक समिति गठित की गई है।

हाल ही में, एमओपी ने विद्युत क्षेत्र की साइबर सुरक्षा तैयारियों की समीक्षा करने के लिए सचिव (विद्युत) की अध्यक्षता में एक अधिकार प्राप्त समिति और अपर सचिव (विद्युत) की अध्यक्षता में स्थायी समिति गठित की है।

एमओपी ने राज्यों/संघ राज्य क्षेत्रों से भी अपने संबंधित राज्य/संघ राज्य क्षेत्र में विद्युत प्रणाली उपकरणों को सुरक्षित रखने के लिए विभिन्न कार्य करने का अनुरोध किया है।

इसके अलावा, देश में रणनीतिक रूप से महत्वपूर्ण तथा प्रमुख विद्युत आपूर्ति प्रणाली एवं नेटवर्क की सुरक्षा, सत्यनिष्ठा और विश्वसनीयता की सुरक्षा करने के लिए निम्नलिखित दिशा-निर्देश जारी किए गए हैं:

(i) विद्युत आपूर्ति प्रणाली एवं नेटवर्क में उपयोग किए जाने के लिए आयात किए गए सभी उपस्कर, घटक और कलपुर्जों की किसी भी प्रकार के अंतर्निहित मालवेयर/ट्रोजन/साइबर खतरे की जांच और भारतीय मानकों की अनुपालना के लिए देश में जांच की जाएगी।
(ii) ऐसी सभी जांच एमओपी द्वारा अभिचिन्हित प्रमाणित प्रयोगशालाओं में की जाएंगी।
(iii) यथा विनिर्दिष्टित "पूर्व संदर्भ" देशों से अथवा इन "पूर्व संदर्भ" देशों के स्वामित्व द्वारा नियंत्रित अथवा उनके कार्यक्षेत्र अथवा निदेशों के अधीन व्यक्तियों द्वारा प्रमुख पारेषण प्रणाली के लिए संवेदनशील उपस्करों/घटकों/कलपुर्जों के किसी भी आयात के लिए भारत सरकार की पूर्व अनुमति अपेक्षित होगी।
(iv) जहां ऐसे संवेदनशील उपकरण/घटकों/कलपुर्जों का आयात "पूर्व संदर्भ" देशों से, विशेष अनुमति के साथ, किया जाता है, प्रमाणित एवं अभिचिन्हित प्रयोगशालाओं में उनकी जांच के लिए नयाचार एमओपी द्वारा अनुमोदित किए जाएंगे।

****