भारत सरकार

**इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय**

**राज्य सभा**

**अतारांकित प्रश्न संख्या 2013**

जिसका उत्तर 23 दिसम्बर, 2022 को दिया जाना है।

2 पौष, 1944 (शक)

## महत्वपूर्ण आधारभूत अवसंरचनाओं पर साइबर हमले

**2013. श्री मल्लिकार्जुन खरगे**:

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

(क) विगत पांच वर्षों में देश में महत्वपूर्ण आधारभूत अवसंरचनाओं प्रणालियों पर हुए बड़े हमलों सहित साइबर हमलों की संख्या का वर्ष-वार ब्यौरा क्या है;

(ख) क्या सरकार के पास ऐसे साइबर हमलों की उत्पत्ति संबंधी कोई रिकॉर्ड है, यदि हां, तो तत्संबंधी ब्यौरा क्या है;

(ग) क्या सरकार को इस बात की जानकारी है कि कई महत्वपूर्ण अवसंरचना प्रणालियां साइबर हमलों के प्रति अत्यंत संवेदनशील हैं, जिससे देश की राष्ट्रीय सुरक्षा के लिए खतरा पैदा हो सकता है; और

(घ) यदि हां, तो ऐसे प्रतिष्ठानों पर साइबर सुरक्षा के संबंध में सर्वोत्तम तरीकों का अनुपालन सुनिश्चित करने के लिए सरकार ने क्या उपाय किए हैं?

उत्तर

## इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री राज्य मंत्री (श्री राजीव चंद्रशेखर)

**(क):** सरकार की नीतियों का उद्देश्य अपने उपयोगकर्ताओं के लिए एक खुला, सुरक्षित और भरोसेमंद और जवाबदेह इंटरनेट सुनिश्चित करना है। गुमनामी, इंटरनेट का तेजी से विकास, साइबर सुरक्षा की घटनाओं में वृद्धि के साथ मिलकर, एक सीमाविहीन साइबरस्पेस एक वैश्विक घटना है। सूचना प्रौद्योगिकी अधिनियम, 2000 ("आईटी अधिनियम") के अनुसार, महत्वपूर्ण सूचना अवसंरचना का अर्थ एक ऐसा कंप्यूटर संसाधन है जिसकी अक्षमता या विनाश का *अन्य बातों* के साथ-साथ राष्ट्रीय सुरक्षा पर दुर्बल प्रभाव पड़ता है। नेशनल क्रिटिकल इंफॉर्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर (एनसीआईआई पीसी) को आईटी अधिनियम के अंतर्गत क्रिटिकल इन्फॉर्मेशन इंफ्रास्ट्रक्चर प्रोटेक्शन के लिए राष्ट्रीय नोडल एजेंसी के रूप में अधिसूचित किया गया है। एनसीआईआईपीसी ने सूचित किया है कि इस तरह के बुनियादी ढांचे पर साइबर हमलों के बारे में खुलासा करना राष्ट्रीय सुरक्षा के हित में नहीं होगा।

**(ख):** समय-समय पर देश के बाहर की प्रणालियों से भारतीय साइबर स्पेस पर साइबर हमले शुरू करने के प्रयास किए गए हैं। यह देखा गया है कि हमलावर दुनिया के विभिन्न हिस्सों में स्थित कंप्यूटर सिस्टम से समझौता कर रहे हैं और हमलावरों की उत्पत्ति-पहचान को छिपाने के लिए परिष्कृत तकनीकों/प्रौद्योगिकियों और प्रॉक्सी सर्वर के नेटवर्क का उपयोग करते हैं।

**(ग) और (घ):** सरकार की नीतियों का उद्देश्य अपने उपयोगकर्ताओं के लिए एक खुला, सुरक्षित और भरोसेमंद और जवाबदेह इंटरनेट सुनिश्चित करना है। प्रौद्योगिकी के नवाचार और व्यवसायों और सेवाओं के लिए साइबरस्पेस और डिजिटल बुनियादी ढांचे के उपयोग में वृद्धि के साथ, साइबर हमले गोपनीयता, अखंडता और सूचना और सेवाओं की उपलब्धता के लिए खतरा पैदा करते हैं। सरकार महत्वपूर्ण अवसंरचना प्रणालियों सहित विभिन्न साइबर सुरक्षा खतरों से पूरी तरह परिचित और जागरूक है।

यह सुनिश्चित करने के लिए निम्नलिखित उपाय किए गए हैं ताकि महत्वपूर्ण सूचना अवसंरचना वाले प्रतिष्ठानों में साइबर सुरक्षा के संबंध में सर्वोत्तम प्रथाओं का पालन किया जाए :

(i) राष्ट्रीय सुरक्षा परिषद सचिवालय के अंतर्गत राष्ट्रीय साइबर सुरक्षा समन्वयक साइबर सुरक्षा मामलों के संबंध में राष्ट्रीय स्तर पर विभिन्न एजेंसियों के साथ समन्वय करता है।

(ii) केंद्र सरकार ने सूचना प्रौद्योगिकी (संरक्षित प्रणाली के लिए सूचना सुरक्षा प्रथाएं और प्रक्रियाएं) नियमावली, 2018 के माध्यम से इसके द्वारा अधिसूचित महत्वपूर्ण सूचना अवसंरचना के लिए प्रथाओं और प्रक्रियाओं को संरक्षित प्रणालियों के रूप में विहित किया है। इनके लिए ऐसी संरक्षित प्रणालियों वाले संगठनों को सूचना सुरक्षा ( आईएस) संचालन समिति का गठन करने की आवश्यकता होती है ताकि संरक्षित प्रणाली की आईएस नीतियों, इसके नेटवर्क विन्यास और अनुप्रयोगों में महत्वपूर्ण बदलाव को मंजूरी दी जा सके और साइबर घटनाओं के समय पर संचार के लिए एक तंत्र स्थापित किया जा सके । उन्हें संगठनों को एक मुख्य सूचना सुरक्षा अधिकारी (सीआईएसओ) नामित करने, एक आईएस प्रबंधन प्रणाली स्थापित करने, सिस्टम के नेटवर्क आर्किटेक्चर/अधिकृत कर्मियों/हार्डवेयर और सॉफ्टवेयर सूची/आईटी सुरक्षा सेवा स्तर के समझौतों का दस्तावेजीकरण करने, भेद्यता/खतरे/जोखिम विश्लेषण करने ,साइबर संकट प्रबंधन योजना तैयार करने , समय-समय पर आईएस ऑडिट करें, साइबर सुरक्षा और नेटवर्क संचालन केंद्र स्थापित करने और लॉग का नियमित बैकअप लेने की भी आवश्यकता होती है। सीआईएसओ को एनसीआईआईपीसी के साथ नियमित संपर्क बनाए रखना आवश्यक है, यह सुरक्षा उपायों को लागू करने के लिए जिम्मेदार है, और संरक्षित प्रणाली के लिए आईएस से संबंधित दस्तावेजों, योजनाओं आदि में एनसीआईआईपीसी के सुझावों को साझा करता है और शामिल करता है।

(iii) इंडियन कंप्यूटर इमरजेंसी रिस्पांस टीम ( सीईआरटी-इन) को साइबर सुरक्षा घटनाओं पर प्रतिक्रिया देने के लिए राष्ट्रीय एजेंसी के रूप में नामित किया गया है । सीईआरटी-इन सभी क्षेत्रों के संगठनों के साथ उनके द्वारा सक्रिय रूप से खतरे को कम करने की कार्रवाइयों के लिए सक्रिय रूप से छोटे छोटे एलर्ट को एकत्र करने, विश्लेषण करने और साझा करने के लिए एक स्वचालित साइबर खतरा विनिमय मंच संचालित करता है ।

(iv) सीईआरटी-इन ने मौजूदा और संभावित साइबर सुरक्षा खतरों के बारे में स्थितिजन्य जागरूकता उत्पन्न करने के लिए राष्ट्रीय साइबर समन्वय केंद्र की स्थापना की है।

(v) सीईआरटी-इन ने सूचना सुरक्षा सर्वोत्तम प्रथाओं के कार्यान्वयन का समर्थन और लेखापरीक्षा करने के लिए 150 सुरक्षा ऑडिटिंग संगठनों को सूचीबद्ध किया है।

(vi) केंद्र/राज्य सरकारों के सभी मंत्रालयों और विभागों और उनके संगठनों और महत्वपूर्ण क्षेत्रों द्वारा कार्यान्वयन के लिए सीईआरटी-इन द्वारा एक साइबर संकट प्रबंधन योजना तैयार की गई जो इन्हें साइबर हमलों और साइबर आतंकवाद का मुकाबला करने में मदद करती है।

(vii) वेबसाइटों को होस्ट करने से पूर्व सरकारी वेबसाइटों और अनुप्रयोगों की ,साइबर सुरक्षा और वेबसाइटों के लिए भारत सरकार के दिशानिर्देशों के अनुपालन के संबंध में लेखा परीक्षा की जाती है है। होस्टिंग के बाद भी नियमित आधार पर वेबसाइटों और एप्लिकेशन का ऑडिट किया जाता है।

******

*****