भारत सरकार
इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्रालय
लोक सभा
अतारांकित प्रश्न संख्या 1729
जिसका उत्तर 29 जुलाई, 2026 को दिया जाना है ।
7 श्रावण, 1948 (शक)

एआई-सक्षम साइबर खतरे

1729. श्री जी. एम. हरीश बालयोगीः

क्या **इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी मंत्री** यह बताने की कृपा करेंगे किः

(क) सरकार द्वारा एआई-संचालित मालवेयर, रैंसमवेयर और ऑटोनोमस साइबर अटैक टूल्स सहित पहचाने गए कृत्रिम बुद्धिमत्ता (एआई) आधारित साइबर खतरों का ब्यौरा क्या है;

(ख) क्या सरकार ने महत्वपूर्ण सूचना अवसंरचना, वित्तीय प्रणालियों और सरकारी नेटवर्क के लिए एआई-संचालित मालवेयर, रैंसमवेयर और ऑटोनोमस अटैक टूल्स द्वारा उत्पन्न जोखिमों का आकलन किया है और यदि हां, तो तत्संबंधी ब्यौरा क्या है;

(ग) एआई-संचालित साइबर खतरों की पहचान, रोकथाम और प्रतिक्रिया के लिए मौजूदा तंत्रों का ब्यौरा क्या है;

(घ) ऐसे खतरों में निपटने के लिए सरकारी एजेंसियों और महत्वपूर्ण क्षेत्रों के लिए की गई क्षमता-निर्माण और साइबर सुरक्षा तैयारी संबंधी उपायों का ब्यौरा क्या है;

(ङ) उभरते साइबर खतरों की पहचान और शमन के लिए एआई-आधारित साइबर सुरक्षा समाधानों के अनुसंधान, विकास और नियोजन का ब्यौरा क्या है; और

(च) एआई-संचालित साइबर हमलों के विरुद्ध भारत की तैयारियों, साइबर घटनाओं को रोकने की क्षमता और घटना के संबंध में प्रतिक्रिया क्षमताओं को मजबूत करने के लिए सरकार द्वारा क्या कदम उठाए गए हैं या उठाए जाने का प्रस्ताव है?

उत्तर

इलेक्ट्रॉनिकी और सूचना प्रौद्योगिकी राज्य मंत्री (श्री जितिन प्रसाद)

(क) से **(च):** सरकार आर्टिफिशियल इंटेलिजेंस (एआई) समर्थित साइबर खतरों से उत्पन्न होने वाले खतरों सहित उभरते साइबर सुरक्षा खतरों और चुनौतियों से अवगत है। एआई प्रौद्योगिकियां स्वचालित सर्वेक्षण, तीव्र सुभेद्यता शोषण, क्रेडेंशियल समझौता और अत्यधिक विश्वसनीय बहुभाषी सोशल इंजीनियरिंग अभियानों को सक्षम करके प्रणालीगत साइबर जोखिमों को बढ़ा सकती हैं। ये क्षमताएं हमले की लागत को कम करती हैं, हथियारीकरण में तेजी लाती हैं, और फ़िशिंग और प्रतिरूपण हमलों को अधिक मापनीय और पता लगाने में दुर्गम बनाती हैं।

सरकार एक खुला, सुरक्षित, विश्वसनीय और जवाबदेह साइबर स्पेस सुनिश्चित करने के लिए प्रतिबद्ध है। एआई-सक्षम साइबर खतरों से उत्पन्न जोखिमों को दूर करने, साइबर लचीलापन बढ़ाने और घटना प्रतिक्रिया क्षमताओं को सुदृढ़ करने के लिए कई कानूनी, तकनीकी और प्रशासनिक नीतिगत उपायों को लागू किया गया है, जिनमें अन्य बातों के साथ-साथ निम्नलिखित भी शामिल हैं:

1. भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल (सर्ट-इन) द्वारा अपेक्षित शमन के लिए दुर्भावनापूर्ण डोमेन और फिशिंग गतिविधियों का पता लगाने के लिए एआई-संचालित स्थितिजन्य जागरूकता प्रणाली नियोजित की जाती है।
2. सर्ट-इन ने सुभेद्यताओं का पता लगाने और उन्हें कम करने के लिए सैंडबॉक्स वातावरण में सार्वजनिक-सामना करने वाली डिजिटल एसेट्स के लिए एआई-सक्षम सुभेद्यता मूल्यांकन का विस्तार किया है।

3. सर्ट-इन सक्रिय खतरे को कम करने की कार्रवाई के लिए सभी क्षेत्रों के संगठनों के साथ अनुरूप अलर्ट साझा करने के लिए एक स्वचालित साइबर थ्रेट इंटेलिजेंस एक्सचेंज प्लेटफॉर्म संचालित करता है।
4. सर्ट-इन ने जून-जुलाई 2026 के दौरान "फ्रंटियर एआई-संचालित साइबर खतरों के विरुद्ध लचीलापन का निर्माण" विषय पर 10 अनुकूलित साइबर सुरक्षा अभ्यास और ड्रिल आयोजित किए हैं। इन अभ्यासों में बिजली, दूरसंचार, बैंकिंग, वित्तीय सेवाओं और बीमा (बीएफएसआई), परिवहन, शिक्षा, स्वास्थ्य और अंतरिक्ष जैसे क्षेत्रों में 345 सरकारी और निजी संगठनों के 1,470 प्रतिभागियों ने भाग लिया।
5. सर्टिफाइड सिक्योरिटी प्रोफेशनल इन आर्टिफिशियल इंटेलिजेंस (सीएसपीएआई) प्रोग्राम सितंबर 2024 में सर्ट-इन और एसआईएसए द्वारा लॉन्च किया गया था। इस अमेरिकन नेशनल स्टैंडर्ड्स इंस्टीट्यूट (एएनएसआई) नेशनल एक्रिडिटेशन बोर्ड (एएनएबी) द्वारा अनुमोदित कार्यक्रम का उद्देश्य साइबर सुरक्षा पेशेवरों को एआई सिस्टम को सुरक्षित करने, एआई से संबंधित खतरों को सक्रिय रूप से संबोधित करने और व्यावसायिक वातावरण में भरोसेमंद एआई नियोजन सुनिश्चित करने के कौशल से लैस करना है।
6. सर्ट-इन सरकारी, सार्वजनिक और निजी क्षेत्रों में साइबर सुरक्षा कार्यबल को कौशल प्रदान करने के लिए उद्योग भागीदारों के सहयोग से साइबर सुरक्षा प्रशिक्षण कार्यक्रम आयोजित करता है।
7. सर्ट-इन फरवरी 2025 में फ्रांस राष्ट्रीय साइबर सुरक्षा एजेंसी (एएनएसएसआई) द्वारा प्रकाशित आर्टिफिशियल इंटेलिजेंस (एआई) पर संयुक्त उच्च-स्तरीय जोखिम विश्लेषण रिपोर्ट पर सह-हस्ताक्षर करने वाले अंतरराष्ट्रीय भागीदारों में से एक है, जिसका शीर्षक "साइबर-जोखिम-आधारित दृष्टिकोण के माध्यम से एआई में विश्वास का निर्माण" है।
8. परामर्शी निदेश और दिशानिर्देश:
   i. सर्ट-इन कंप्यूटर, नेटवर्क और डेटा की सुरक्षा के लिए नवीनतम साइबर खतरों, सुभेद्धताओं और प्रतिउपायों के बारे में अलर्ट और परामर्शी निदेश जारी करता है।
   ii. सर्ट-इन ने जून 2026 में दिशानिर्देश जारी किए हैं, जिसमें सभी मूल उपकरण निर्माताओं (ओईएम) और प्रौद्योगिकी प्रदाताओं को एआई-त्वरित सुभेद्यता सुरक्षा को लागू करने की आवश्यकता है, जिसके लिए एआई-समर्थित सुरक्षा परीक्षण, निरंतर निगरानी, पैच प्रबंधन और एआई-संचालित साइबर खतरों से बचाव के लिए घटना प्रतिक्रिया ढांचे की आवश्यकता होती है।
   iii. सर्ट-इन ने मई 2026 में "डिजिटल अवसरंचना में एआई-सहायता प्राप्त सुभेद्धताओं के शोषण के विरुद्ध जोखिम को कम करने और बचाव के लिए ब्लूप्रिंट" जारी किया है, जिसका उद्देश्य तेजी से विकसित हो रहे एआई-संचालित साइबर खतरों के विरुद्ध डिजिटल अवसरंचना की रक्षा करना है।
   iv. सर्ट-इन ने अप्रैल 2026 में "फ्रंटियर एआई संचालित साइबर जोखिमों से बचाव" शीर्षक से एक परामर्शी निदेश जारी किया है, जिसमें उन्नत एआई-सक्षम खतरों के विरुद्ध सुरक्षा को सुदृढ़ करने के लिए संगठनों, एमएसएमई और व्यक्तियों के लिए व्यापक उपायों की रूपरेखा तैयार की गई है।
   v. सर्ट-इन ने आपूर्ति श्रृंखलाओं की सुरक्षा और पारदर्शिता बढ़ाने के लिए सॉफ्टवेयर, हार्डवेयर, आर्टिफिशियल इंटेलिजेंस, क्वांटम कंप्यूटिंग और क्रिप्टोग्राफी आवश्यकताओं के लिए बिल ऑफ मैटेरियल्स (बीओएम) के लिए जुलाई 2025 में तकनीकी दिशानिर्देश जारी किए हैं।
   vi. सर्ट-इन ने मार्च 2025 में एक परामर्शी निदेश जारी किया है जिसमें जनरेटिव एआई समाधानों के प्रभावी और जिम्मेदार उपयोग के लिए सर्वोत्तम पद्धतियों को दर्शाया गया है।
   vii. सर्ट-इन ने फरवरी 2025 में "स्मार्ट सिटी इन्फ्रास्ट्रक्चर के लिए साइबर सुरक्षा दिशानिर्देश" प्रकाशित किए हैं, जिसमें स्मार्ट सिटी के अवसरंचना और अनुप्रयोगों के लिए आर्टिफिशियल इंटेलिजेंस (एआई) और मशीन लर्निंग (एमएल) के सुरक्षित उपयोग के उपाय शामिल हैं।
   viii. सर्ट-इन ने नवंबर 2024 में डीपफेक खतरों और डीपफेक से सुरक्षित रहने के लिए जिन उपायों का पालन करने की आवश्यकता है, उन पर एक परामर्शी निदेश जारी किया है।
   ix. सर्ट-इन ने अगस्त 2023 में मास्टरकार्ड के सहयोग से एक श्वेतपत्र प्रकाशित किया है, जिसमें एप्लिकेशन प्रोग्रामिंग इंटरफ़ेस (एपीआई) पर बढ़ते हमलों और इन हमलों को कम करने में एआई के उपयोग पर प्रकाश डाला है।
   x. सर्ट-इन ने मई 2023 में आर्टिफिशियल इंटेलिजेंस (एआई) आधारित अनुप्रयोगों से उत्पन्न होने वाले प्रतिकूल खतरों को कम करने के लिए किए जाने वाले सुरक्षा उपायों पर एक परामर्शी निदेश जारी किया है।

******