साइबर हमलों का बढ़ता आतंक

पूरे विश्व में होने वाले साइबर हमलों की बढ़ती संख्या अत्यधिक चिंताजनक है। पिछले दिनों अमेरिका की कोलोनियल पाइपलाइन पर एक रैन्समवेयर हमला किया गया था, जिसके लिए हमलावरों को 50 लाख डॉलर की फिरौती की रकम दी गई थी। देशों के महत्वपूर्ण बुनियादी ढांचों पर लगातार ऐसे हमले किए जा रहे हैं। भारत भी इससे बचा नहीं है। नोटपेत्य के हमले से विश्व की सबसे बड़ी शिपिंग कंपनी मेयर्स के कंप्यूटर नेटवर्क को संक्रमित किया जा चुका है। इसने मुंबई के जवाहलाल नेहरू बंदरगाह के संचालन को अवरूद्ध कर दिया था। 2020 में चीन के एक हैकर समूह ने भारत के ऊर्जा क्षेत्र पर हमला करके रेल्वे, बंदरगाह और बिजली विभाग को प्रभावित कर दिया था। भारत सरकार साइबर हमलों से सुरक्षा को प्राथमिकता दे रही है।

किए गए उपाय कितने कारगर -

- 2014 में सरकार ने नेशनल क्रिटिकल इंर्फोमेशन इंफ्रास्ट्रक्चर प्रोटेक्शन सेंटर की स्थापना की थी। यह एक नोडल एजेंसी है, जो सार्वजनिक और निजी क्षेत्र के बुनियादी ढांचों की कमियों को दूर करने का प्रयास करती है। महत्वपूर्ण ढांचों के सिस्टम की सुरक्षा के लिए यह समय-समय पर संचालनात्मक और तकनीकी दिशानिर्देश देती रहती है।

- कंप्यूटर एमरजेंसी रेस्पोंस टीम का गठन, मुख्यतः पावर सेक्टर की सुरक्षा के लिए किया गया है। यह थर्मल, हाइड्रो और ट्रांसमिशन क्षेत्रों को देखती है।

- भारत के विभिन्न क्षेत्रों (मुख्यतः निजी) की डेटा और कमजोरियों को साझा करने की अपनी सीमाएं हैं।

  साइबर हमला हो जाने की स्थिति में वे सुरक्षा को लेकर काम करते हैं। इस प्रकार के कदम आधे-अधूरे और निकट अवधि में काम करते हैं।

- निजी और सार्वजनिक क्षेत्र के बीच चलने वाले अविश्वास और कमजोरियों को दूर करने के लिए दोनों क्षेत्रों के बीच साझेदारी का होना बहुत जरूरी है। इसके लिए संस्थागत ढांचा तैयार किया जाए, क्षमताओं का विस्तार किया जाए, सुरक्षा मानक तैयार किए जाएं, कड़ाई के साथ ऑडिट कराया जाए और साइबर सुरक्षा संबंधी घटनाओं की रिपोटिंग का ढांचा तैयार किया जाए।

भारत ने भले ही कोई बड़ा साइबर हमला न झेला हो, लेकिन खतरा दिन-ब-दिन बढता ही जा रहा है। इसके लिए एक ऐसा एकीकृत तंत्र बनाने की बहुत जरूरत है, जो हमारे महत्वपूर्ण बुनियादी ढांचों की रक्षा कर सके।

'हिंदुस्तान टाइम्स' में प्रकाशित समीर पाटिल के लेख पर आधारित। 21 मई, 2021