महत्त्वपूर्ण बुनियादी ढाँचों की सुरक्षा

यह एडिटोरियल दिनांक 20/05/2021 को 'द हिंदुस्तान टाइम्स' में प्रकाशित लेख “Cyber attacks on critical infrastructure: Is India ready?” पर आधारित है। इसमें साइबर हमले के प्रति भारत के महत्त्वपूर्ण बुनियादी ढाँचों की सुरक्षा पर चर्चा की गई है।

हाल ही में साइबर हमले के ज़रिये संयुक्त राज्य अमेरिका की सबसे बड़ी पाइपलाइनों में से एक, कोलोनियल पाइपलाइन (Colonial Pipeline) को निष्क्रिय कर दिया गया। ज्ञातव्य है कि यह पाइपलाइन देश के पूर्वी तट पर खपत होने वाली ईंधन के लगभग 45% भाग की आपूर्ति करता है। इस हमले से जहाँ ईंधन की आपूर्ति बाधित हुई वहीं देश के कुछ हिस्सों में गैस की कीमतों में उछाल भी आया।

यह एक रैंसमवेयर हमला था, जहाँ हैकर्स आमतौर पर सिस्टम को ब्लॉक करने या लक्षित कंपनी या पीड़ित के गोपनीय डेटा को प्रकाशित करने की धमकी देते हैं, जब तक कि फिरौती (Ransom) का भुगतान नहीं किया जाता है।

कोलोनियल पाइपलाइन पर हमला हाल के वर्षों में ऐसे महत्त्वपूर्ण बुनियादी ढाँचे पर साइबर हमलों का एक उदाहरण है, जिन्हें हर समय परिचालन की आवश्यकता होती है जैसे कि यातायात प्रणाली, बैंक, बिजली ग्रिड, तेल पाइपलाइन एवं परमाणु रिएक्टर।

महत्त्वपूर्ण बुनियादी ढाँचे पर साइबर हमलों की बढ़ती संख्या को देखते हुए भारत जैसे देशों के लिये एक मज़बूत साइबर सुरक्षा संरचना विकसित करना आवश्यक हो गया है।

महत्त्वपूर्ण बुनियादी ढाँचा क्या है?

- महत्त्वपूर्ण बुनियादी ढाँचा नेटवर्क और परिसंपत्तियों का एक ऐसा तंत्र है, जिसे किसी राष्ट्र की सुरक्षा, उसकी अर्थव्यवस्था तथा जनता के स्वास्थ्य या सुरक्षा को सुनिश्चित करने के लिये निरंतर संचालित किये जाने की आवश्यकता है।

साइबर सुरक्षा फ्रेमवर्क की आवश्यकता

- **महत्त्वपूर्ण बुनियादी ढाँचों पर बढ़ते हमले:** हाल के वर्षों में महत्त्वपूर्ण बुनियादी ढाँचे और व्यवसायों को निशाना बनाने वाले साइबर हमलों में वृद्धि हुई है।
    - इनमें वर्ष 2017 में WannaCry और NotPetya रैंसमवेयर हमले, यूक्रेन के पॉवर ग्रिड पर वर्ष 2015 का हमला और ईरानी परमाणु रिएक्टर पर वर्ष 2010 का Stuxnet हमला शामिल हैं।
    - वर्ष 2020 में चीन से संबंधित एक हैकर समूह RedEcho ने भारत के बिजली से जुड़े क्षेत्रों, बंदरगाहों एवं रेलवे के आधारभूत संरचनाओं के कुछ हिस्सों को निशाना बनाया।
- **साइबर युद्ध:** भू-राजनीतिक लाभ प्राप्त करने के लिये एक देश द्वारा दूसरे देशों पर साइबर हमले किये जा रहे हैं। इसके अलावा ऐसे हमलों की ज़िम्मेदारी से बचने के लिये, कई राज्य प्रॉक्सी के रूप में हैकिंग सिंडिकेट का उपयोग करते हैं।
    - इन सभी कारणों को देखते हुए साइबर हमले से महत्त्वपूर्ण बुनियादी ढाँचों को सुरक्षित रखने की ज़िम्मेदारी भारत की प्राथमिकता सूची में आ गई है।

संबंधित चुनौतियाँ

- **सूचना साझा ना करना:** महत्त्वपूर्ण बुनियादी ढाँचे की सुरक्षा में एक बड़ी चुनौती निजी (और सार्वजनिक) क्षेत्र की कंपनियों द्वारा अपने सिस्टम की भेद्यता के बारे में जानकारी साझा करने में अनिच्छा जाहिर करना है।
    - क्योंकि उनका मानना है कि अपनी कमज़ोरियों एवं अपनी मालिकाना जानकारी का खुलासा कर वे अपने व्यवसायिक प्रतिद्वंद्वियों के साथ प्रतिस्पर्द्धा में पिछड़ सकते हैं।
    - इस कारण भारतीय नियामकों ने चेतावनी दी है कि साइबर हमलों के लिये केवल प्रतिक्रियाशील उपायों द्वारा भारत के खिलाफ विरोधी देशों द्वारा साइबर युद्ध की संभावना की अनदेखी की जा रही है।

- **क्षमताओं का आकलन:** भारत में हार्डवेयर के साथ-साथ सॉफ्टवेयर साइबर सुरक्षा उपकरणों में स्वदेशीकरण का अभाव है। यह भारत के साइबर स्पेस को विरोधी देशों द्वारा प्रेरित या निजी साइबर हमलों के प्रति संवेदनशील बनाता है।
- **एक विश्वसनीय साइबर हमला प्रतिरोधी रणनीति का अभाव:** इसके अलावा एक विश्वसनीय साइबर हमला प्रतिरोधी रणनीति की अनुपस्थिति का अर्थ है कि निजी और विरोधी देशों द्वारा विभिन्न उद्देश्यों, जैसे- जासूसी, साइबर अपराध और यहाँ तक कि महत्त्वपूर्ण बुनियादी ढाँचा को क्षति पहुँचाने के लिये उचित प्रतिरोधी व्यवस्था का अभाव।

आगे की राह

- **साइबर संघर्ष से जुड़ा सिद्धांत:** साइबर संघर्ष से जुड़े एक ऐसे सिद्धांत की आवश्यकता है, जो साइबर संघर्ष के प्रति अपने दृष्टिकोण को समग्र रूप से स्पष्ट करे। इसमें आक्रामक साइबर संचालन करने एवं साइबर हमलों से जुड़े विषय, उसके खिलाफ प्रतिवाद की सीमाओं का स्पष्ट उल्लेख होना चाहिये।
- **वैश्विक बेंचमार्क स्थापित करना:** अंतर्राष्ट्रीय कानून को साइबर स्पेस पर लागू करने के लिये राष्ट्रीय साइबर सुरक्षा रणनीति को भारत द्वारा एक महत्त्वपूर्ण अवसर के रूप में देखना चाहिये।
    - यह वैश्विक चर्चा को भारत के रणनीतिक हितों और क्षमताओं की तरफ मोड़ सकता है।
- **रेडलाइन निर्दिष्ट करना:** राष्ट्रीय साइबर सुरक्षा रणनीति में न केवल गैर-बाध्यकारी मानदंडों पर स्थिति स्पष्ट होनी चाहिये बल्कि, साइबर हमलावरों के निशाने पर रहने वाले क्षेत्र जैसे- स्वास्थ्य देखभाल प्रणाली, बिजली ग्रिड, जल-आपूर्ति और वित्तीय प्रणाली के संबंध में 'रेड लाइन' पर कानूनी दायित्व भी शामिल होना चाहिये।
- **स्वदेशीकरण को बढ़ावा देना:** साइबर सुरक्षा और डिजिटल संचार की सुरक्षा के लिये सॉफ्टवेयर विकसित करने हेतु अवसर सृजित करने की आवश्यकता है।
    - भारत सरकार अपने मेक इन इंडिया कार्यक्रम में साइबर सुरक्षा संरचना को शामिल करने पर विचार कर सकती है।
    - साथ ही, भारतीय पैटर्न पर एक अद्वितीय तथा उपयुक्त हार्डवेयर बनाने की आवश्यकता है, जो स्थानीय आवश्यकताओं को पूरा कर सके।
- **सार्वजनिक-निजी भागीदारी:** सार्वजनिक एवं निजी क्षेत्र के आपसी अविश्वास और भेद्यता को देखते हुए, महत्त्वपूर्ण बुनियादी ढाँचों की सुरक्षा के लिये किसी भी समाधान में सार्वजनिक-निजी भागीदारी के माध्यम से ज़िम्मेदारियाँ साझा करना शामिल है।
    - इसके लिये एक संस्थागत ढाँचे का निर्माण, क्षमता का विस्तार, सुरक्षा मानकों और लेखाकर्म/ऑडिटिंग को सख्त बनाने तथा साइबर सुरक्षा घटनाओं की रिपोर्टिंग से संबंधित ढाँचे को विकसित करने पर ध्यान केंद्रित करना चाहिये।

निष्कर्ष

औद्योगिक क्रांति 4.0 के तहत प्रौद्योगिकी के भविष्य को देखते हुए महत्त्वपूर्ण बुनियादी ढाँचे को साइबर हमले से बचाने हेतु एकीकृत एवं व्यापक तंत्र दृष्टिकोण ही सफल होगा।

अभ्यास प्रश्न: महत्त्वपूर्ण बुनियादी ढाँचों को साइबर हमलों से सुरक्षित रखना भारत के लिये एक प्रमुख मुद्दा बन गया है। चर्चा कीजिये।

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/critical-infrastructure-protection