Be Mains Ready

प्रश्न.संभावित साइबर हमलों के विरुद्ध भारत की तैयारी का मूल्यांकन कीजिये। इस संकट को रोकने के लिये किये जा सकने वाले कुछ संरक्षोपाय सुझाइये। (250 शब्द)

24 Nov 2021 | सामान्य अध्ययन पेपर 3 | आंतरिक सुरक्षा

दृष्टिकोण / व्याख्या / उत्तर

हल करने का दृष्टिकोण:

- साइबर सुरक्षा की अवधारणा का वर्णन कीजिये।
- साइबर हमलों से निपटने के लिये मौजूदा उपायों की चर्चा कीजिये।
- संबद्ध चुनौतियों का उल्लेख कीजिये।
- साइबर खतरों के संकट को प्रभावी रूप से नियंत्रित करने के लिये उपाय सुझाइये।

साइबर सुरक्षा या सूचना प्रौद्योगिकी सुरक्षा कंप्यूटरों, नेटवर्कों, प्रोग्रामों और डेटा को अनाधिकृत पैठ या हमले से सुरक्षित करने की तकनीक है। प्रौद्योगिकी के विकास ने युद्ध तथा संघर्षों की प्रकृति को परिवर्तित कर दिया है। राजनीतिक उद्देश्यों की प्राप्ति के लिये किसी प्रतिद्वंद्वी के विरुद्ध साइबर हमलों का संचालन सूचना क्षेत्र के एजेंटों के माध्यम से गुप्त तरीके से किया जाता है।

देश की बुनियादी सुविधाएँ, जैसे बिजली ग्रिड तथा वित्तीय और यातायात नेटवर्क तेज़ी से इंटरनेट से जुड़ रहे हैं, साथ ही अधिकांश आधिकारिक डेटा को ऑनलाइन भंडारित किया जा रहा है। डिजिटल अवसंरचना को सुरक्षित करने के लिये सरकार द्वारा कई पहलें की गई हैं, जैसे:

- जब भी साइबर सुरक्षा संबंधी दुर्घटनाएँ होती हैं, उस पर प्रतिक्रिया देने के लिये इंडियन कंप्यूटर इमरजेंसी रेस्पॉन्स टीम (CERT-In) को राष्ट्रीय नोडल एजेंसी के रूप में स्थापित किया गया है।
- भारत सरकार ने राष्ट्रीय साइबर सुरक्षा व्यवस्था की आवश्यकताओं की पूर्ति के लिये सूचना प्रौद्योगिकी (संशोधन) अधिनियम, 2008 लागू किया है।
- वर्ष 2013 में एक राष्ट्रीय साइबर सुरक्षा नीति लाई गई। इसकी शुरआत साइबर सुरक्षा के क्षेत्र में विद्यमान सभी पहलों को एकीकृत करने और साइबर अपराधों के बदलते स्वरूप से निपटने के लिये की गई थी।
- राष्ट्रीय साइबर समन्वय केंद्र (एन.सी.सी.सी.) राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना सुरक्षा केंद्र (एन.सी.आई.आई.पी.सी.) और CERT-In के तहत क्षेत्र विशेष के लिये कंप्यूटर आपातकालीन प्रतिक्रिया दलों (सी.ई.आर.टी.) जैसी पहलों को राष्ट्रीय साइबर सुरक्षा नीति के तहत क्रियान्वित किया गया है।
- भारत सरकार ने साइबर हमलों और साइबर आतंकवाद से निपटने के लिये एक राष्ट्रीय संकट प्रबंधन योजना निर्मित की है। साइबर हमलों के बदलते परिदृश्य से निपटने के लिये इस योजना को वार्षिक रूप से पुनर्मूल्यांकित एवं अद्यतन किया जाता है।
- सरकारी एवं निजी कंपनियों के द्वारा सुरक्षा ऑडिटिंग के संचालन हेतु सुरक्षा अंकेक्षकों (सिक्योरिटी ऑडिटर्स) को नियुक्त किया गया है।

साइबर सुरक्षा एक जटिल मुद्दा है, जो विभिन्न क्षेत्रों को प्रभावित करता है। इससे निपटने के लिये बहुआयामी, बहुस्तरीय पहलों और अनुक्रियाओं की आवश्यकता है। यह सरकार के लिये एक चुनौती साबित हुई है, क्योंकि

- अलग-अलग क्षेत्रों को कमराबंद मंत्रालयों और विभागों द्वारा प्रशासित किया जाता है।
- खतरों की अस्पष्ट एवं विविध प्रकृति तथा किसी मूर्त दोषी की अनुपस्थिति में पर्याप्त अनुक्रिया में अक्षमता नीति-निर्माण को एक कठिन कार्य बना देती है।
- निजी कंपनियाँ एवं बैंक साइबर खतरों के विषय में सरकारी संगठनों को नियमित रूप से सूचित नहीं करते हैं।
- आम लोगों के बीच साइबर सुरक्षा को लेकर जागरूकता का अभाव रहता है, इसलिये वे हैकरों के जाल में फँस जाते हैं।
- लगातार होने वाले साइबर हमलों से ग्राहकों का डिजिटल प्लेटफॉर्म पर विश्वास कम होता है और भारत के एक नकदरहित अर्थव्यवस्था बनने के सपने में बाधा उत्पन्न होती है।
- ऑनलाइन रेडिकलाइज़ेशन (कट्टरता) के मामलों में वृद्धि चिंता का एक अन्य विषय है। पारंपरिक युद्धों के विपरीत, अतिवादियों और आतंकवादियों के लिये साइबरस्पेस की कोई भौतिक सीमा नहीं होती है।

साइबर हमलों से निपटने के लिये निम्नलिखित उपाय किये जा सकते हैं:

- परिचालनात्मक स्तर पर एक साइबर समन्वय केंद्र स्थापित किया जाना चाहिये। यह केंद्र एक क्लियरिंग-हाउस की तरह कार्य करेगा, वास्तविक समय (रियल टाइम) में आने वाली सूचना का मूल्यांकन करेगा और आवश्यकतानुसार संबंधित एजेंसियों को ज़िम्मेदारी सौंपेगा।
- सरकार को महत्त्वपूर्ण अवसरंचना क्षेत्रों से संबंधित साइबर सुरक्षा के क्षेत्र में सर्वोत्तम प्रथाओं को लागू करने के लिये एक विशेष मुहिम प्रारंभ करनी चाहिये और इसके लिये आवश्यक बजटीय सहायता प्रदान करनी चाहिये।
- सरकार को संभावित साइबर हमलों के खिलाफ महत्त्वपूर्ण क्षेत्रों की तैयारी के आकलन के लिये एक तंत्र स्थापित करना चाहिये, उदाहरण के लिये- सुरक्षा सूचकांक, जो किसी क्षेत्र विशेष की तैयारी का मूल्यांकन करता है और उसके आधार पर अंक प्रदान करता है।
- सूचना एवं संचार प्रौद्योगिकी (आई.सी.टी.) अवसंरचना से संबंधित खतरों के बारे में जागरूकता पैदा की जानी चाहिये और साइबर सुरक्षा सुनिश्चित करने के लिये आवश्यक कानूनी प्रावधानों का विकास, निरंतर अद्यतन और प्रभावी रूप से विरयान्वयन किया जाना चाहिये।
- साइबर सुरक्षा को राष्ट्रीय सुरक्षा का एक अभिन्न अंग माना जाना चाहिये। साइबर सुरक्षा, साइबर आतंकवाद, साइबर युद्ध आदि के मुद्दों पर आवश्यक रूप से ध्यान दिया जाना चाहिये।