दुष्प्रचार और साइबर सुरक्षा को खतरा

(मुख्य परीक्षा, सामान्य अध्ययन प्रश्नपत्र- 3 व 4 : सूचना प्रौद्योगिकी, कंप्यूटर, संचार नेटवर्क के माध्यम से आंतरिक सुरक्षा को चुनौती, आंतरिक सुरक्षा चुनौतियों में मीडिया और सामाजिक नेटवर्किंग साइटों की भूमिका, साइबर सुरक्षा की बुनियादी बातें, भावनात्मक समझ)

संदर्भ

साइबर सुरक्षा कंप्यूटर प्रणाली, नेटवर्क और डिजिटल जीवन को व्यवधान से बचाने, रक्षा और बचाव करने पर केंद्रित है। वर्तमान में दुष्प्रचार और गलत सूचना का प्रसार एक बड़ी समस्या है।

दुष्प्रचार

- गोपनीयता व सत्यनिष्ठा से समझौता करने और आई.टी. प्रणाली का लाभ उठाने के लिये कुछ लोग साइबर हमले का सहारा लेते हैं। इसी तरह दुष्प्रचार संज्ञानात्मक अस्तित्व को प्रभावित करता है।
- राज्य समर्थित, किसी विशेष विचारधारा से संबंधित, हिंसक चरमपंथी और आर्थिक रूप से प्रेरित उद्यमों ने सामाजिक कलह, ध्रुवीकरण के साथ-साथ कुछ हद तक चुनाव परिणामों को प्रभावित करने के लिये सूचना पारिस्थितिकी तंत्र में हेरफेर के माध्यम से दुष्प्रचार करते हैं।

साइबर सुरक्षा और दुष्प्रचार

- साइबर हमले और दुष्प्रचार की रणनीति, युक्ति और तरीकों में बहुत समानता है। साइबर हमला कंप्यूटर अवसंरचना को लक्षित करता है, जबकि दुष्प्रचार व्यक्ति के संज्ञानात्मक पूर्वाग्रहों और तार्किक भ्रम का लाभ उठाता है।
- मॉलवेयर, वायरस, ट्रोजन, बॉटनेट और सोशल इंजीनियरिंग का उपयोग करते हुए साइबर सुरक्षा हमलों को अंजाम दिया जाता है। दुष्प्रचार में हेरफेर व जोड़-तोड़, गलत धारणा, गलत जानकारी, डीप फेक और चीप फेक का उपयोग होता है।

- उद्योग जगत इन हमलों से अलग-अलग और स्वतंत्र तरीकों से निपटते हैं एवं विभिन्न उपायों को लागू करते हैं। साथ ही, इन हमलों से बचाव व सुरक्षा के लिये अलग-अलग टीमें कार्य करती हैं।

संज्ञानात्मक हैकिंग

- संज्ञानात्मक हैकिंग गलत जानकारी, दुष्प्रचार और कम्प्यूटर आधारित प्रोपेगेंडा से उत्पन्न एक खतरा है। यह हमला मनोवैज्ञानिक कमजोरियों का अनुचित लाभ उठाता है, पूर्वाग्रहों को मज़बूत करता है और अंततः तार्किक और आलोचनात्मक सोच को कम करके संज्ञानात्मक असंगति को जन्म देता है।
- संज्ञानात्मक हैकिंग दुष्प्रचार का प्रयोग करके लक्षित दर्शकों के विचारों व कार्यों में परिवर्तन का प्रयास करता है तथा समाज की एकजुटता व सद्भावना को बाधित करता है। इसका लक्ष्य लोगों की वास्तविक समझ व बोध का अनुभव करने के तरीके में बदलाव और असंतुलन पैदा करना है।

प्रभाव

- अमेरिका में कैपिटल हिल दंगा संज्ञानात्मक हैकिंग के प्रभावों का एक प्रमुख उदाहरण है। संज्ञानात्मक हैकिंग का प्रभाव व निहितार्थ महत्त्वपूर्ण बुनियादी ढाँचे पर साइबर हमले की तुलना में अधिक विनाशकारी हैं और दुष्प्रचार से हुई क्षति को सुधारना अत्यंत चुनौतीपूर्ण है।
- इतिहास में बहुत से ऐसे उदाहरण हैं, जब क्रांतिकारियों ने सरकारों को उखाड़ फेंकने और समाज को बदलने के लिये संज्ञानात्मक हैकिंग तकनीकों का उपयोग किया है। इस प्रकार सीमित साधनों का प्रयोग करके मुख्य लक्ष्यों को प्राप्त करने के लिये यह एक महत्त्वपूर्ण रणनीति है।
- अमेरिकी राष्ट्रपति चुनाव को फर्जी व झूठा बताना तथा कई यूरोपीय देशों में कोरोनावायरस महामारी के प्रसार के लिये 5G टावरों को उत्तरदाई ठहराते हुए उसको जलाना भी 'कांस्पीरेसी थ्योरी' का ही एक उदाहरण है। इसके लिये भी दुष्प्रचार और संज्ञानात्मक हैकिंग काफी हद तक उत्तरदाई है।
- कोविड-19 से संबंधित दुष्प्रचार ने लोगों को मास्क पहनने, खतरनाक वैकल्पिक इलाजों का उपयोग करने और टीकाकरण से रोका है, जिससे वायरस को रोकना अधिक चुनौतीपूर्ण हो गया है।

गलत जानकारी का प्रसार

- 'डिस्ट्रिब्यूटेड डिनायल-ऑफ़-सर्विस' (DDoS) अच्छी तरह से समन्वित एक साइबर सुरक्षा हमला है, जो वैध अनुरोधों को पूरा करने से रोकता है। इसी प्रकार अच्छी तरह से समन्वित दुष्प्रचार अभियान प्रसारण इकाईयों और सामाजिक प्रणाली को अत्यधिक गलत जानकारी से भर देता है, जिससे वास्तविक सच्चाई ख़त्म हो जाती है।
- विज्ञापन केंद्रित व्यवसाय और अर्थव्यवस्था दुर्भावनापूर्ण व्यक्तियों को 'विवेकयुक्त दुष्प्रचार अभियान' के लिये प्रोत्साहित करती है, जो सत्य को दबाने के लिये सूचना चैनलों को अत्यधिक तीव्रता और बड़े पैमाने पर गलत जानकारी से भर देते हैं।

- दुष्प्रचार का उपयोग 'सोशल इंजीनियरिंग' खतरों के लिये बड़े पैमाने पर किया जाता है। दुष्प्रचार अभियान भावनाओं से खेलते हैं और साइबर अपराधियों को अन्य व्यवहार्य तरीके प्रदान करते हैं।
- एक रिपोर्ट के अनुसार 48% साइबर सुरक्षा पेशेवर दुष्प्रचार को खतरा मानते हैं, जबकि शेष 49% का कहना है कि यह खतरा बहुत बड़ा है। सर्वेक्षण में शामिल साइबर सुरक्षा पेशेवरों में से 91% ने इंटरनेट पर कड़े कदम उठाने का आह्वान किया है।
- डीप फेक ने दुष्प्रचार अभियानों में खतरे का एक नया स्तर जोड़ दिया हैं। उच्चस्तरीय डीप फेक का प्रयोग करके चलाये जाने वाले दुष्प्रचार अभियान लोकतंत्र में लोगों के बीच विभाजन को और बढ़ा सकते हैं, जिससे अराजकता एवं हिंसा का स्तर बढ़ जाता है तथा संपत्ति व जीवन को नुकसान पहुँचता है।

आग की राह

- साइबर सुरक्षा विशेषज्ञों ने वायरस, मॉलवेयर और हैकर्स द्वारा उत्पन्न खतरों को सफलतापूर्वक समझकर उनको प्रबंधित किया है और उद्योग जगत ने सर्वोत्तम सुरक्षा प्रथाओं में भारी निवेश किया।
- इसने साइबर सुरक्षा को लचीला बनाने के लिये कठोर सुरक्षा ढाँचे, दिशानिर्देश और मानकों के साथ-साथ सर्वोत्तम प्रथाओं, जैसे- 'डिफेन्स-इन-डेप्थ', 'थ्रेट मॉडलिंग', 'सुरक्षित विकास जीवनचक्र' और 'रेड-टीम-ब्लू-टीम' को विकसित किया है।
- साइबर सुरक्षा के दशकों के अनुभव से बचाव, सुरक्षा और प्रतिक्रिया करने तथा प्रभावी व व्यावहारिक समाधान खोजने में सहायता मिल सकती हैं। साथ ही 'दुष्प्रचार रक्षा प्रणाली' का भी विकास किया जा सकता है।
- दुष्प्रचार को एक प्रकार का साइबर सुरक्षा खतरा मानकर संज्ञानात्मक हैकिंग के लिये प्रभावी प्रतिकार और उपाय खोजा जा सकता हैं।
- साथ ही दुष्प्रचार के प्रति की जाने वाली प्रतिक्रिया को एकीकृत और समन्वित किये जाने की आवश्यकता है, जिसमें सुसंगत वर्गीकरण, परिभाषाएँ, नीति, मानदंड और प्रतिक्रिया का विकास शामिल है।
- इससे संबंधित पहचान, सामग्री, संदर्भ, कार्य और व्यवहार को साझा करने के लिये एक मंच की भी आवश्यकता है। सूचना का आदान-प्रदान वृहद पैमाने पर और तेज़ी से प्रतिक्रिया करने में मदद करेगा।
- साइबर सुरक्षा का एक महत्त्वपूर्ण घटक शिक्षा है। तकनीक पर आधारित उद्योग, नागरिक समाज और सरकार को इस संबंध में जागरूकता फ़ैलाने के लिये समन्वय की आवश्यकता है।
- साथ ही मीडिया साक्षरता के प्रसार और उसमें वृद्धि की आवश्यकता है। गौरतलब है कि दुष्प्रचार के खतरे के साथ बोलने के अधिकार को संतुलित करना नीति-निर्माताओं और नियामकों के लिये एक चुनौती है।
- सूचना क्षेत्र में स्थिरता और सुरक्षा के लिये 1,000 से अधिक संस्थाओं ने 'पेरिस कॉल फॉर ट्रस्ट एंड सिक्योरिटी इन साइबरस्पेस' पर हस्ताक्षर किये हैं। इसी तरह, 52 देशों और अंतर्राष्ट्रीय निकायों ने आतंकवादी और हिंसक चरमपंथी सामग्री हटाने के लिये 'क्राइस्टचर्च कॉल टू एक्शन' पर हस्ताक्षर किये हैं।