साइबर सुरक्षा से संबंधित चुनौतियाँ

(प्रारंभिक परीक्षा : राष्ट्रीय और अंतर्राष्ट्रीय महत्त्व की सामयिक घटनाएँ)
(मुख्य परीक्षा, प्रश्नपत्र 3 : संचार नेटवर्क के माध्यम से आंतरिक सुरक्षा को चुनौती, साइबर सुरक्षा की बुनियादी बातें)

संदर्भ

- पेगासस स्पाइवेयर के दुरुपयोग के बाद वैश्विक स्तर पर साइबर हथियारों की भूमिका को लेकर एक फिर से बहस शुरू हो गई है।
- पूर्व में कभी-कभार या छिटपुट साइबर हमले की घटनाएँ, अब एक खतरनाक हद तक बढ़ गई हैं, जो साइबर हथियार युग के उद्भव का संकेत देती हैं।

साइबर हथियारों का विकास-क्रम

- इस तरह के शुरुआती उदाहरण 1990 के दशक में मिलते हैं। याह्या अब्द-अल-लतीफ अय्याश, जो हमास का मुख्य बम निर्माता था, उसकी हत्या इज़राइल की खुफिया एजेंसी ने विस्फोटकों से युक्त फोन के प्रयोग द्वारा की थी।
- अतीत के हमलों के लिये कई महीनों का प्रयास और बड़ी संख्या में लोगों एवं संसाधनों का प्रयोग किया जाता था, लेकिन साइबर युग में बहुत कम प्रयास और संसाधनों के साथ यह संभव है।
- द्वितीय विश्व युद्ध के दौरान वेमोर्क पावर स्टेशन (नॉर्वे) का विनाश किया गया, जिसके लिये महीनों की योजना बनाई गई और मित्र देशों के व्यापक संसाधनों का प्रयोग किया गया।
- वर्तमान समय में ऐसे लक्ष्य एक अंश के साथ प्राप्त किये जा सकते है।
- वर्ष 2019 में, नॉरस्क हाइड्रो, जो एल्यूमीनियम व ऊर्जा उत्पादन संयंत्र है, एक साइबर हमले का शिकार हो गया, जिसे दूर से और गुमनाम रूप से कम से कम समय में पूरा किया गया था।
- वर्तमान में निजता संबंधी धारणाएँ लगभग समाप्त हो गई हैं और इंटरनेट, फायदा उठाने की कोशिश करने वालों के हाथों में एक शक्तिशाली हथियार बन गया है।

साइबर युद्ध

- भूमि, समुद्र, वायु, अंतरिक्ष के अतिरिक्त, साइबर को अक्सर युद्ध के पाँचवें आयाम के रूप में देखा जाता है।
- हालाँकि, यह समझने की ज़रूरत है कि साइबर, सैन्य और राष्ट्रीय सुरक्षा के क्षेत्र के साथ-साथ रोज़मर्रा की जिंदगी के एक डोमेन में भी मौजूद है।
- युद्ध अब केवल युद्धक्षेत्र में ही नहीं लड़े जाते, बल्कि अब यह बंद कमरों अथवा सीधे किसी के 'ड्राइंग रूम' के अंदर से भी लड़े जा रहे हैं, क्योंकि 'साइबर हथियारों' के कारण यह बहुत आसान हो गया है।

नया हथियार

- साइबर जगत में सिर्फ इज़राइल ही अग्रणी नहीं है, बल्कि आज चीन, रूस, कोरिया और अमेरिका भी साइबर डोमेन में हावी हैं।
- परंपरागत परमाणु उपकरणों के विपरीत, साइबर हथियारों को शुरुआत से ही विशेष हथियारों के रूप में महत्त्व दिया गया है।
- वर्ष 2010 में 'स्टक्सनेट वर्म' को मुक्त करने में संयुक्त रूप से यू.एस.-इज़रायल प्रयास ने नटांज में ईरानी परमाणु सुविधा में कई सौ सेंट्रीफ्यूज को निष्क्रिय करने में मदद की थी।

वर्तमान विवाद

- वर्तमान विवाद से पहले **पेगासस स्पाइवेयर** के प्रयोग की कई घटनाएँ पहले भी हो चुकी हैं। वर्ष 2019 में, व्हाट्सएप ने एन.एस.ओ. पर आरोप लगाया था कि उसके कई उपयोगकर्ता के विरुद्ध पेगासस स्पाइवेयर का प्रयोग किया गया है।
- इज़राइली कंपनी का दावा है कि स्पाइवेयर केवल सरकारों और आधिकारिक एजेंसियों को ही बेचा जाता है। हालाँकि इसके बारे में पुष्टि होना अभी शेष है।
- इज़राइल, अपने हिस्से में पेगासस को एक 'साइबर हथियार' के रूप में चिह्नित करता है तथा दावा करता है कि इसका 'निर्यात नियंत्रित' है।

पेगासस स्पाइवेयर

- पेगासस स्पाइवेयर भेजे या प्राप्त किये गए संदेशों की प्रतिलिपि बना सकता है, फोटो व कॉल रिकॉर्ड, फोन के कैमरे के माध्यम से गुप्त रूप से फिल्म, या बातचीत रिकॉर्ड करने के लिये माइक्रोफ़ोन को सक्रिय कर सकता है।
- साथ ही, यह संभावित रूप से इंगित कर सकता है कि आप कहाँ हैं और किससे मिले हैं।
- यह एक बार फोन में इंस्टॉल हो जाने के पश्चात् कमोबेश किसी भी जानकारी को इकट्ठा कर सकता है या किसी भी फाइल को भेज सकता है।
- पेगासस के निर्माता, एन.एस.ओ. समूह द्वारा स्पाइवेयर का पता लगाना की प्रक्रिया को बेहद जटिल बनाते हैं।
- यह 'ज़ीरो क्लिक' द्वारा फोन में इंस्टाल किया जाता है, अर्थात फोन उपयोगकर्ता द्वारा किसी भी गतिविधि की आवश्यकता नहीं होती है।
- इसका प्रयोग ऑपरेटिंग सिस्टम में पाई जाने वाली कुछ 'ज़ीरो डे' कमज़ोरियों का फायदा उठाने के लिये किया जाता है, जिसके बारे में निर्माता खुद अनभिज्ञ होता है।
- अनिवार्यतः पेगासस वायरस 'रूट प्रिविलेज', जो इंटरनेट एड्रेस, सर्वर और ट्रांजिट डेटा पर एक अज्ञात नेटवर्क, के माध्यम से अपने नियंत्रकों के साथ संचार को सक्षम बनाता है।

हालिया साइबर हमले

- एस्टोनिया के महत्त्वपूर्ण बुनियादी ढाँचे पर वर्ष 2007 में **साइबर हमला** हुआ था। इसके बाद कुछ वर्ष उपरांत ईरान की परमाणु सुविधा पर 'स्टक्सनेट वर्म' हमला हुआ था।
- वर्ष 2012 में, सऊदी अरब की तेल कंपनी अरामको पर 'शमून वायरस' का हमला हुआ था।
- यूक्रेन के स्टेट पावर ग्रिड पर वर्ष 2016 में साइबर हमले हुआ था।
- वर्ष 2017 के 'रैनसमवेयर अटैक' ने 64 देशों में विभिन्न उपकरणों को प्रभावित किया था।
- उसी वर्ष यूनाइटेड किंगडम की राष्ट्रीय स्वास्थ्य सेवा पर एक 'वानाक्राई' हमला हुआ था।
- आयरलैंड की स्वास्थ्य देखभाल प्रणाली तथा संयुक्त राज्य अमेरिका में इस वर्ष 'सोलरविंड्स' द्वारा पाइपलाइन आदि पर साइबर हमले किये गए थे।

गंभीर खतरा

- साइबर हथियार न केवल संघर्ष के दौरान बल्कि शांतिकाल में भी पसंद का हथियार बनने के साथ-साथ एक महत्त्वपूर्ण बिंदु पर पहुँच चुके हैं।
- साइबर हथियार, नागरिक या सैन्य प्रणालियों और संरचनाओं को विकृत करने की क्षमता रखते हैं।
- सबसे महत्त्वपूर्ण यह है कि ये लोकतांत्रिक प्रक्रियाओं में हस्तक्षेप करते हैं, जैसे घरेलू स्तर पर विभाजन को बढ़ाते हैं, उन ताकतों को मुक्त करते हैं, जिन पर स्थापित संस्थानों या यहाँ तक कि सरकारों का बहुत कम नियंत्रण होता है।

बचाव की आवश्यकता

- हमें साइबर खतरों के एक नए युग के लिये तैयार रहना चाहिये तथा उससे बचाव के उपाय करने चाहिये।
- नए अत्याधुनिक साइबर हथियारों को नियोजित करना आवश्यक है।
- जैसे-जैसे अधिक से अधिक उपकरण नेटवर्क से जुड़े होते हैं, साइबर खतरा लघु व मध्यम अवधि, दोनों में ही और तेज़ होता है।
- चिंता की बात यह है कि भागीदारी के बिना रोज़मर्रा के प्रयोग वाले उपकरणों को संक्रमित या उनमें घुसपैठ किया जा सकता है।
- इसमें दुरुपयोग की संभावनाएँ बहुत अधिक हैं, तथा किसी व्यक्ति, प्रतिष्ठान या राष्ट्र के लिये इसके बहुत गंभीर परिणाम हो सकते हैं।

विश्लेषण की आवश्यकता

- पेगासस जैसे परिष्कृत स्पाइवेयर द्वारा उत्पन्न किये गए गंभीर खतरों का सामना करना बेहद कठिन है।
- 'ज़ीरो डे' की कमज़ोरियों से निपटने के लिये केवल इंटरनेट से अलग विशेष फायरवॉल या फोन बनाने की तुलना में 'विचार और आत्मनिरीक्षण' की आवश्यकता होगी।
- ज़रूरत न केवल साइबर प्रौद्योगिकियों की गहरी समझ की है, बल्कि उन लोगों की मानसिकता को भी पहचानने की है, जो पेगासस जैसे स्पाइवेयर का प्रयोग करते हैं।

भावी राह

- पेगासस जैसे साइबर हथियारों के आगमन के साथ, एक मित्र के रूप में मानी जाने वाली प्रौद्योगिकी इस संदर्भ में निराश कर सकती है।
- आर्टिफिशियल इंटेलिजेंस (AI) को अक्सर कई मौजूदा समस्याओं और बीमारियों के 'रामबाण' के रूप में देखा जाता है, लेकिन प्रौद्योगिकी में सभी विकास एक 'दोधारी तलवार' के समान होते हैं।

- ए.आई. बदले में सभी सूचनाओं को युद्ध में बदल सकती है। कम से कम ए.आई. उपकरणों के विकास के वर्तमान चरण में कोई समाधान ढूढना या रोकना लगभग असंभव है।

निष्कर्ष

नए साइबर जासूसी उपकरणों तक आसान पहुँच मौजूदा अराजकता को बढ़ाएगी। लगातार बढ़ते साइबर हथियारों के युग में सुरक्षा एक महत्त्वपूर्ण मुद्दा बन सकता है।

Cyber Security