साइबर सुरक्षा सिद्धांत

drishtiias.com/hindi/current-affairs-news-analysis-editorials/news-editorials/10-03-2021/print

इस Editorial में The Hindu, The Indian Express, Business Line आदि में प्रकाशित लेखों का विश्लेषण किया गया है। इस लेख में भारत के लिये एक मज़बूत साइबर सुरक्षा नीति की आवश्यकता व इससे संबंधित विभिन्न पहलुओं पर चर्चा की गई है। आवश्यकतानुसार, यथास्थान टीम दृष्टि के इनपुट भी शामिल किये गए हैं।

संदर्भ:

वर्तमान में विश्व भर में साइबर कमानों (Cyber Commands)की स्थापना और उन्हें बढ़ावा देने के समर्थन के साथ सैन्य सिद्धांतों में परिवर्तन बड़े रणनीतिक बदलाव को दर्शाता है, जिसमें साइबर क्षेत्र में अवरोधक का निर्माण शामिल है।

इसके अतिरिक्त साइबर सुरक्षा के प्रभाव का दायरा सैन्य क्षेत्र तक ही सीमित नहीं है बल्कि यह देश के शासन, अर्थव्यवस्था और कल्याण सभी पहलुओं को शामिल करता है।

इंटरनेट उपभोक्ताओं की सर्वाधिक संख्या के मामले में विश्व में अमेरिका और चीन के बाद भारत का तीसरा स्थान है, परंतु अभी भी भारत का साइबर सुरक्षा तंत्र अपने शुरुआती स्तर पर ही है।

इसे न्यूयॉर्क टाइम्स में प्रकाशित एक रिपोर्ट के आधार पर समझा जा सकता है, जिसमें इस संभावना को रेखांकित किया गया है कि वर्ष 2020 में मुंबई में पावर आउटेज की घटना एक चीनी राज्य-प्रायोजित समूह के हमले का परिणाम हो सकती है।

ऐसे में सैन्य, शासन और आर्थिक क्षेत्र में साइबर क्षमता की महत्त्वपूर्ण भूमिका को देखते हुए भारत में शीघ्र ही एक व्यापक साइबर सुरक्षा सिद्धांत को अपनाए जाने की आवश्यकता है।

नोट:

भारत पूर्व में भी कई बार साइबर हमलों का शिकार हो चुका है।

- वर्ष 2009 में एक संदिग्ध साइबर जासूसी नेटवर्क जिसे 'घोस्टनेट' नाम दिया गया था, को अन्य लोगों/संस्थानों के अलावा भारत में निर्वासित तिब्बत की सरकार और कई भारतीय दूतावासों को निशाना बनाते हुए पाया गया था।

- इस खोज से प्राप्त जानकारियों पर आगे जाँच करते हु, शोधकर्त्ताओं ने पाया कि जिसे उन्होंने एक शैडो नेटवर्क माना था, वह एक विशाल साइबर जासूसी ऑपरेशन था जिसके तहत बड़े पैमाने पर भारत में स्थित रणनीतिक महत्त्व की कई संस्थाओं को निशाना बनाया गया।
- इस घटना के बाद कई हमले हुए जिन्होंने भारत को निशाना बनाया, जिसमें स्टक्सनेट (Stuxnet) भी शामिल था, इसने ईरान में परमाणु रिएक्टरों को बंद कर दिया था।
- सकफ्लाई (Suckfly) नामक एक साइबर हमले में न केवल सरकारी बल्कि निजी संस्थाओं को भी निशाना बनाया गया, इसमें नेशनल स्टॉक एक्सचेंज को तकनीकी सहायता प्रदान करने वाली एक कंपनी भी शामिल थी।
- डीट्रैक (Dtrack) नामक एक साइबर हमले में वर्ष 2019 में पहले भारतीय बैंकों को और बाद में कुडनकुलम परमाणु ऊर्जा संयंत्र (तमिलनाडु) को निशाना बनाया गया।

भारत के साइबर सुरक्षा ढाँचे से जुड़ी चुनौतियाँ:

- **एकीकृत प्रतिक्रिया का अभाव: राष्ट्रीय स्तर पर साइबर सुरक्षा खतरों का मुकाबला करने और उन्हें कम करने के लिये एक एकीकृत प्रतिक्रिया को लागू करने में प्रभावी समन्वय, उत्तरदायित्वों का अधिव्यापन और स्पष्ट संस्थागत सीमाओं व जवाबदेही की कमी जैसी चुनौतियों का सामना करना पड़ सकता है।**
- **आवश्यक क्षमता का अभाव:** भारत में हार्डवेयर के साथ-साथ सॉफ्टवेयर साइबर सुरक्षा उपकरणों व तकनीकों के मामले में स्वदेशी क्षमता (आत्मनिर्भरता) का अभाव है।
    - यह भारत के साइबर क्षेत्र को शत्रु राष्ट्रों और अन्य अराजक समूहों द्वारा प्रेरित साइबर हमलों के लिये असुरक्षित बनाता है।
    - भारत में यूरोपीय संघ के '<u>सामान्य डेटा संरक्षण विनियमन</u>' (GDPR) या अमेरिका के 'क्लेरीफाइंग लॉफुल ओवरसीज़ यूज़ ऑफ डेटा (CLOUD) एक्ट' की तरह एक सक्रिय साइबर सुरक्षा ढाँचा नहीं है।
- **एक प्रभावी साइबर डिटरेंस रणनीति का अभाव:** इसके अतिरिक्त एक विश्वसनीय साइबर रणनीति के अभाव का अर्थ है कि राज्य प्रायोजित और गैर-राजकीय अराजक तत्त्वों को कई उद्देश्यों के लिये कम पैमाने पर साइबर हमलों का संचालन (जैसे-जासूसी, साइबर अपराध और महत्त्वपूर्ण सूचना अवसंरचनाओं के संचालन को बाधित करना आदि) करने के लिये प्रोत्साहन मिलता रहता है।

साइबर सुरक्षा संस्थान:

- पिछले दो दशकों में भारत ने साइबर सुरक्षा की अनुकूलता पर ध्यान केंद्रित करते हुए संस्थागत मशीनरी तैयार करने का एक महत्त्वपूर्ण प्रयास किया है, साथ ही इस पहल का विस्तार कई सरकारी संस्थाओं तक है।
- प्रधानमंत्री कार्यालय के अंतर्गत ही कई साइबर पोर्टफोलियो शामिल हैं। राष्ट्रीय सुरक्षा परिषद भी इनमें से एक है, इसकी अध्यक्षता आमतौर पर राष्ट्रीय सुरक्षा सलाहकार (NSA) द्वारा की जाती है, और यह भारत की साइबर नीति पारिस्थितिकी तंत्र को आकार देने में महत्त्वपूर्ण भूमिका निभाती है।
- NSA द्वारा राष्ट्रीय सूचना बोर्ड की अध्यक्षता भी की जाती है, जो साइबर सुरक्षा नीति पर अंतर-मंत्रालयी समन्वय के लिये सर्वोच्च निकाय के रूप में कार्य करता है।

- राष्ट्रीय तकनीकी अनुसंधान संगठन के अंतर्गत जनवरी 2014 में स्थापित राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र को महत्त्वपूर्ण सूचना बुनियादी ढाँचे के संरक्षण का कार्य सौंपा गया है।
- वर्ष 2015 में भारतीय प्रधानमंत्री द्वारा राष्ट्रीय साइबर सुरक्षा समन्वयक कार्यालय की स्थापना की गई, जो प्रधानमंत्री को रणनीतिक साइबर सुरक्षा मुद्दों पर सलाह देता है।
- केंद्रीय इलेक्ट्रॉनिक्स और सूचना प्रौद्योगिकी मंत्रालय (MEITY) के अंतर्गत स्थापित कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-In) गैर-प्राथमिकता वाले बुनियादी ढाँचे से जुड़े विभिन्न साइबर सुरक्षा खतरों से निपटने के लिये कार्य करती है।
- केंद्रीय रक्षा मंत्रालय द्वारा 'डिफेंस साइबर एजेंसी' (Defence Cyber Agency- DCA) की स्थापना के लिये डिफेंस इंफॉर्मेशन एश्योरेंस एंड रिसर्च एजेंसी को अपग्रेड किया गया है। DCA संयुक्त सशस्त्र अभियानों का समन्वय और नियंत्रण करने के लिये भारतीय सशस्त्र बलों की एक त्रि-सेवा कमान है, साथ ही यह भारत की साइबर नीति के निर्धारण में भी सहायक होगी।
- इसके अतिरिक्त केंद्रीय गृह मंत्रालय की निगरानी में कई समन्वय केंद्रों का संचालन किया जाता है जो साइबर अपराध, जासूसी और आतंकवाद के खात्मे के लिये कानून प्रवर्तन प्रयासों पर ध्यान केंद्रित करते हैं। जबकि केंद्रीय विदेश मंत्रालय भारत की साइबर कूटनीति को दोनों रूपों में (द्विपक्षीय रूप से अन्य देशों के साथ, और संयुक्त राष्ट्र जैसे अंतर्राष्ट्रीय मंचों पर) समन्वित करता है।

आगे की राह:

राष्ट्रीय साइबर सुरक्षा नीति 2013 ने स्पष्ट किया कि भारत को एक राष्ट्रीय साइबर सुरक्षा रणनीति की आवश्यकता है, हालाँकि इसे अभी तक जारी नहीं किया गया है। अतः साइबरस्पेस के महत्त्व को देखते हुए नई रणनीति में सभी प्रमुख मुद्दों को शामिल किया जाना चाहिये, जिनमें से कुछ निम्नलिखित हैं:

- **साइबर संघर्षों पर सिद्धांत: वर्तमान में स्पष्ट रूप से एक ऐसे साइबर सुरक्षा सिद्धांत को निर्धारित करने की आवश्यकता है जो साइबर चुनौतियों से निपटने हेतु आक्रामक साइबर हमलों के संचालन या साइबर हमलों के खिलाफ जवाबी कार्रवाई की नीति के माध्यम से इससे जुड़े सभी पहलुओं को कवर करता है।**
- **वैश्विक बेंचमार्क स्थापित करना:** भारत को राष्ट्रीय साइबर सुरक्षा रणनीति को साइबरस्पेस में अंतर्राष्ट्रीय कानूनों के लागू होने की प्रक्रिया पर अपने मत को स्पष्ट करने के एक महत्त्वपूर्ण अवसर के रूप में देखना चाहिये।
    - यह भारत के सामरिक हितों और क्षमताओं को बढ़ाने के लिये वैश्विक प्रशासन की बहस को भी दिशा देने में सहायता कर सकता है।
- **बहु-हितधारक दृष्टिकोण:** राज्य समर्थित अराजक तत्त्वों और उनके सहयोगियों तथा ऑनलाइन अपराधियों से होने वाले खतरों का पता लगाने एवं उनका मुकाबला करने के लिये सरकार व निजी क्षेत्र के साथ सरकार के भीतर एवं राष्ट्रीय व राज्य स्तरों पर बेहतर समन्वय की आवश्यकता है।
- **सीमाओं का निर्धारण:** राष्ट्रीय साइबर सुरक्षा रणनीति में न केवल गैर-बाध्यकारी मानदंडों पर अपनी स्थिति को स्पष्ट करना चाहिये बल्कि साइबर हमलों के संभावित लक्ष्यों- जैसे स्वास्थ्य देखभाल प्रणाली, विद्युत ग्रिड, जल आपूर्ति और वित्तीय प्रणालियों के संबंध में कानूनी दायित्व को निर्धारित किया जाना चाहिये।

- **स्वदेशीकरण को बढ़ावा देना:** साइबर सुरक्षा और डिजिटल संचार की सुरक्षा सुनिश्चित करने के लिये सॉफ्टवेयर के विकास हेतु अवसरोंको बढ़ाने की आवश्यकता है।
    - भारत सरकार अपने मेक इन इंडिया कार्यक्रम में साइबरसिटी अवसंरचना को शामिल करने पर विचार कर सकती है।
    - साथ ही वर्तमान में स्थानीय आवश्यकताओं की पूर्ति के लिये एक अद्वितीय भारतीय पैटर्न पर उपयुक्त हार्डवेयर विकसित किये जाने की आवश्यकता है।

निष्कर्ष:

साइबर सुरक्षा और साइबर युद्ध पर एक स्पष्ट सार्वजनिक नीति नागरिकों के आत्मविश्वास को बढ़ाने में महत्त्वपूर्ण भूमिका निभाएगी, साथ ही यह सहयोगी देशों के प्रति विश्वास को मज़बूत करने और संभावित विरोधियों को एक कड़ा तथा स्पष्ट संदेश देने में सहायक होगी जो एक अधिक स्थिर और सुरक्षित साइबर पारिस्थितिकी तंत्र स्थापित करने के लिये मज़बूत आधार प्रदान करेगा।

अभ्यास प्रश्न: भारत में एक मज़बूत साइबर सुरक्षा तंत्र की स्थापना तथा इस पर एक प्रभावी सार्वजनिक नीति के विकास के लिये सैद्धांतिक स्पष्टता और संस्थागत सामंजस्य आवश्यक है। चर्चा कीजिये।