नई राष्ट्रीय सुरक्षा नीति की आवश्यकता

यह एडिटोरियल 21/10/2021 को 'द हिंदू' में प्रकाशित "The Outlines of A National Security Policy" लेख पर आधारित है। इसमें सामरिक क्षेत्र में साइबर प्रौद्योगिकी को शामिल किये जाने की आवश्यकता और प्रौद्योगिकी युग में भारत के लिये राष्ट्रीय सुरक्षा नीति के बदलते परिप्रेक्ष्यों के संबंध में चर्चा की गई है।

संदर्भ

साइबर को प्रायः भूमि, समुद्र, वायु और अंतरिक्ष क्षेत्र के साथ युद्ध के पाँचवें आयाम के रूप में देखा जाता है। इस बात की संभावना लगातार बढ़ रही है कि साइबर वारफेयर जल्द ही राष्ट्रों के शस्त्रागार का एक नियमित अंग बन जाएगा।

जहाँ तक भारत का प्रश्न है, इंटरनेट उपयोगकर्त्ताओं की संख्या के मामले में यह संयुक्त राज्य अमेरिका और चीन के बाद विश्व में तीसरे स्थान पर है, लेकिन फिर भी इसकी साइबर सुरक्षा संरचना अभी नवजात अवस्था में ही है।

विश्व भर में बदलता सैन्य सिद्धांत अब साइबर कमान की स्थापना करने की आवश्यकता पर बल दे रहा है, जो साइबर स्पेस में प्रतिरोधक क्षमता के निर्माण के साथ-साथ रणनीतियों में परिवर्तन को भी परिलक्षित करता है।

साइबर वारफेयर और भारत

- **परिचय:** यह किसी राज्य या संगठन की गतिविधियों को बाधित करने हेतु कंप्यूटर प्रौद्योगिकी के उपयोग की क्रिया है, जिसमें विशेष रूप से रणनीतिक या सैन्य उद्देश्यों के लिये उनकी सूचना प्रणाली पर हमला करना शामिल है।
  - साइबर वारफेयर में आमतौर पर इंटरनेट पर अवैध 'एक्सप्लोइटेशन' ('एक्सप्लोइट' एक कोड होता है, जो सॉफ्टवेयर की कमज़ोरी या सुरक्षा दोषों का लाभ उठाता है) के तरीकों का उपयोग करना, कंप्यूटर नेटवर्क और सॉफ्टवेयर में करप्शन या डिशरप्शन उत्पन्न करना, हैकिंग, कंप्यूटर फोरेंसिक और जासूसी करना शामिल होते हैं।
- **साइबर वारफेयर के पक्ष में तर्क:** उत्तरदायित्वपूर्ण उपयोग और उपयुक्त नियंत्रणों के साथ साइबर वारफेयर एक सुरक्षित और अधिक लचीला रणनीतिक विकल्प है, जो प्रतिबंध आरोपित करने और बमबारी करने के बीच का एक महत्त्वपूर्ण चरण हो सकता है।
  - **मानव-जीवन की क्षति को कम करता है:** मानव जीवन की क्षति को कम करना युद्ध की नैतिकता के मूल सिद्धांतों में से एक है।
    - साइबर युद्धों को वैश्विक हिंसा को कम करने के एक अवसर के रूप में देखा जा सकता है और यह युद्धों में मानव जीवन की हानि को कम कर सकता है।
  -
  - **भौतिक क्षेत्रीय आक्रमणों को रोकना:** डिजिटल रूप से युद्ध करना एक अनूठा अवसर प्रदान करता है, जहाँ किसी संप्रभु क्षेत्र पर भौतिक आक्रमण के बिना अन्य साधनों से राजनीति की निरंतरता बनी रहती है।
- **साइबर वारफेयर के विरुद्ध तर्क:**
  - **अंतर्राष्ट्रीय सुरक्षा के लिये खतरा:** साइबर वारफेयर के तहत सैन्य अवसंरचना, सरकारी एवं निजी संचार प्रणालियों और वित्तीय बाज़ारों पर हमला करना शामिल है, जो अंतर्राष्ट्रीय सुरक्षा के लिये एक तेज़ी से बढ़ते (लेकिन जिसे अभी कम समझा गया है) खतरे को प्रकट करता है और देशों के बीच भविष्य के संघर्षों/युद्धों में एक निर्णायक साधन बन सकता है।
  - **युद्ध संलग्नता में वृद्धि का जोखिम:** किसी देश की रक्षा नीतियों में एक प्रमुख अंग के रूप में साइबर प्रौद्योगिकी के प्रवेश के बाद देश का आकार विशेष मायने नहीं रखेगा।
    - साइबर प्रौद्योगिकी से सशक्त कोई छोटा देश भी अमेरिका, रूस, भारत या चीन जैसे बड़े देशों के बराबर शक्तिशाली होगा, क्योंकि उनके पास भारी क्षति उत्पन्न कर सकने की क्षमता होगी।
  - **संघर्षों की संख्या में वृद्धि:** साइबर वारफेयर की सामान्यता के साथ, प्रत्येक राष्ट्र को द्विपक्षीय संघर्षों के लिये अधिक तैयार रहना होगा, जो पारंपरिक युद्ध की बहुपक्षीय गतिविधियों या लामबंदी के लिये सैन्य ब्लॉकों पर निर्भरता के बजाय साइबर वारफेयर पर आधारित होंगे।
- **भारत के लिये खतरा:**
  - **अतीत के अनुभव:** भारत अतीत में कई बार साइबर हमलों का शिकार हो चुका है।

        - वर्ष 2009 में 'घोस्टनेट' (GhostNet) नामक एक संदिग्ध साइबर जासूसी नेटवर्क ने अन्य लोगों के साथ-साथ भारत में तिब्बत की निर्वासित सरकार और कई भारतीय दूतावासों को निशाना बनाया था।
        - कई विशेषज्ञों का मत है कि वर्ष 2020 में मुंबई में हुआ पावर आउटेज चीन के एक राज्य प्रायोजित समूह के हमले का परिणाम था।
    - **चीन से खतरा:** भारत के लिये वास्तविक खतरा शत्रु देशों से होने वाले लक्षित साइबर हमलों में निहित है।
        - चीन जैसे देशों में परिष्कृत साइबर हमलों को अंजाम देने हेतु अपार संसाधन मौजूद हैं।
    - **साइबरस्पेस अवसंरचना की कमी:** भारत उन कुछ देशों में से एक है, जिनकी सेना के पास अभी भी एक समर्पित साइबर घटक मौजूद नहीं है।
        - एक डिफेंस साइबर एजेंसी की स्थापना की घोषणा तो की गई थी, लेकिन इस दिशा में आधे-अधूरे कदम ही उठाए गए, जो भारत में रणनीतिक योजना प्रक्रिया की अक्षमता को प्रकट करता है।

आगे की राह

- **राष्ट्रीय सुरक्षा नीति में परिवर्तन लाना:**
    - **उद्देश्यों को स्पष्ट करना:** 21वीं सदी में राष्ट्रीय सुरक्षा नीति को यह परिभाषित करने की आवश्यकता है कि किन संपत्तियों की रक्षा की जानी है, और उन विरोधियों की पहचान करनी होगी जो लोगों में भ्रांति को बढ़ावा देने हेतु असामान्य उपायों के माध्यम से लक्षित राष्ट्र के लोगों को भयभीत करने की कोशिश करते हैं।
    - **प्राथमिकताएँ निर्धारित करना:** राष्ट्रीय सुरक्षा प्राथमिकताओं को हाइड्रोजन फ्यूल सेल, समुद्री जल के विलवणीकरण, परमाणु प्रौद्योगिकी के लिये थोरियम के उपयोग, एंटी-कंप्यूटर वायरस और नई प्रतिरक्षी दवाओं जैसे नवाचार और प्रौद्योगिकी के विभिन्न मोर्चों के सहयोग और समर्थन के लिये नए विभागों की आवश्यकता होगी।
        - नई प्राथमिकता पर इस फोकस के लिये, विशेष रूप से विश्लेषणात्मक विषयों के अनुप्रयोग हेतु, विज्ञान और गणित की अनिवार्य शिक्षा की आवश्यकता होगी।
        - इसके साथ ही, प्रत्येक नागरिक को इस रिमोट नियंत्रित नई सैन्य तकनीक से अवगत कराने और इसके लिये तैयार रहने के लिये सजग करने की आवश्यकता होगी।
    - **रणनीति में परिवर्तन:** इस नई राष्ट्रीय सुरक्षा नीति के लिये आवश्यक रणनीति में यह क्षमता होनी चाहिये कि वह विभिन्न आयामों में शत्रुओं का अनुमान कर सके और शत्रुओं का प्रतिरोध कर सकने वाली रणनीति विकसित कर एक प्रदर्शनकारी लेकिन सीमित पूर्व-हमले की क्षमता रखे।
        - चीन की साइबर क्षमता भारत के लिये नया खतरा है जिसके लिये उसे एक नई रणनीति तैयार करनी होगी।
    - **नया एजेंडा:** नई रणनीति के लिये एजेंडे को महत्त्वपूर्ण एवं उभरती हुई प्रौद्योगिकियों, कनेक्टिविटी एवं अवसंरचना, साइबर सुरक्षा और समुद्री सुरक्षा पर ध्यान केंद्रित करना होगा।
- **नीति-निर्माताओं की भूमिका:** सरकार को साइबर सुरक्षा के लिये एक अलग बजट प्रदान करना चाहिये।
    - राज्य-प्रायोजित हैकरों का मुकाबला करने के लिये साइबर योद्धाओं का एक केंद्रीय निकाय बनाना होगा।
        - कॅरियर के अवसर प्रदान कर सॉफ्टवेयर विकास में भारत के टैलेंट बेस का लाभ उठाया जाना चाहिये।
    - केंद्रीय वित्तपोषण के माध्यम से राज्यों में साइबर सुरक्षा क्षमता कार्यक्रम को सहयोग देना चाहिये।
- **रक्षा, प्रतिरोध और दोहन (Defence, Deterrence and Exploitation):** साइबर खतरों का मुकाबला करने के लिये किसी भी राष्ट्रीय रणनीति के ये तीन मुख्य घटक होंगे।
    - महत्त्वपूर्ण साइबर अवसंरचना का बचाव किया जाना चाहिये और अलग-अलग मंत्रालयों एवं निजी कंपनियों द्वारा उल्लंघनों की ईमानदार रिपोर्टिंग के लिये आवश्यक प्रक्रियाएँ स्थापित की जानी चाहिये।
    - साइबरस्पेस में प्रतिरोध (Deterrence) एक बेहद जटिल मुद्दा है। परमाणु प्रतिरोध इसलिये सफल है, क्योंकि शत्रुओं की क्षमता प्रकट या स्पष्ट होती है, लेकिन साइबर वारफेयर के मामले में ऐसी स्पष्टता मौजूद नहीं होती।
    - राष्ट्रीय सुरक्षा उद्देश्यों की प्राप्ति के लिये साइबरस्पेस का दोहन किया जाना आवश्यक है। इसकी तैयारी भारतीय सेना द्वारा खुफिया जानकारी जुटाने, लक्ष्यों का मूल्यांकन करने और साइबर हमलों के लिये विशिष्ट उपकरण तैयार करने से शुरू करनी होगी।

निष्कर्ष

- जब साइबर प्रौद्योगिकी किसी राष्ट्र की रक्षा नीतियों का एक महत्त्वपूर्ण अंग बन जाएगी, तब भूमि क्षेत्र या सकल घरेलू उत्पाद के आकार जैसे घटक अप्रासंगिक हो जाएंगे। इसलिये, भारत की साइबर सुरक्षा स्थिति में सुधार के लिये स्पष्ट और अधिक पारदर्शी रणनीति काफी महत्त्वपूर्ण है।
- साइबर रक्षा और वारफेयर पर एक स्पष्ट सार्वजनिक रुख नागरिकों के भरोसे को बढ़ाती है, सहयोगियों के बीच भरोसे के निर्माण में मदद करती है और संभावित विरोधियों को इरादे का स्पष्ट संकेत देती है; इस प्रकार एक अधिक स्थिर और सुरक्षित साइबर पारितंत्र को सक्षम करती है।

अभ्यास प्रश्न: ''साइबर को प्रायः भूमि, समुद्र, वायु और अंतरिक्ष क्षेत्र के साथ युद्ध के पाँचवें आयाम के रूप में देखा जाता है। हालाँकि, साइबर वारफेयर के सामान्य होने के साथ प्रत्येक राष्ट्र को द्विपक्षीय संघर्षों के लिये अधिक तैयार रहना होगा।'' टिप्पणी कीजिये।

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/the-need-for-a-new-national-security-policy