NEXT IAS

दैनिक संपादकीय विश्लेषण

विषय

ग्रे-ज़ोन वॉरफेयर और पारंपरिक संघर्ष के लिए साइबर पूर्वसूचक

www.nextias.com

ग्रे-ज़ोन वॉरफेयर और पारंपरिक संघर्ष के लिए साइबर पूर्वसूचक

संदर्भ

- ग्रे-ज़ोन वॉरफेयर आधुनिक संघर्ष को पुनः आकार दे रहा है, जो अस्पष्टता का लाभ उठाकर और साइबर अभियानों को पारंपरिक सैन्य संलग्नता से पहले एक रणनीतिक पूर्वसूचक के रूप में प्रयोग करके किया जाता है।

ग्रे-ज़ोन युद्ध को समझना

- यह शत्रुतापूर्ण कार्रवाइयों के एक स्पेक्ट्रम को संदर्भित करता है जो जानबूझकर अस्पष्ट होते हैं, जिससे राज्य अपने रणनीतिक उद्देश्यों को सीमा पार किए बिना आगे बढ़ा सकते हैं।
  - इसमें साइबर हमले, दुष्प्रचार अभियान, आर्थिक दबाव, प्रॉक्सी और गैर-राज्य अभिनेताओं का उपयोग, तथा कानूनी एवं कूटनीतिक हेरफेर शामिल हैं।
- यह अस्पष्टता, अस्वीकरण और गैर-गतिज रणनीतियों का उपयोग करता है ताकि पारंपरिक युद्ध से जुड़े रणनीतिक प्रभाव हासिल किए जा सकें।
- समकालीन संघर्षों में राज्य अभिनेताओं के बीच लड़ाई तेजी से ग्रे-ज़ोन में लड़ी जा रही है और साइबर क्षेत्र इसमें केंद्रीय बिंदु पर खड़ा है, जो मात्र सहायक कार्य से विकसित होकर एक निर्णायक युद्धक्षेत्र बन गया है जो परिणामों को आकार देने में सक्षम है।

ग्रे-ज़ोन युद्ध में प्रथम प्रहार के रूप में साइबर अभियान

- आधुनिक संघर्ष यह दर्शाते हैं कि साइबर अभियान राज्य-से-राज्य टकराव का उद्घाटन प्रहार बन गए हैं।
  - ये अभियान महत्वपूर्ण अवसंरचना जैसे विद्युत ग्रिड, दूरसंचार, परिवहन नेटवर्क और कमांड सिस्टम को निशाना बनाते हैं ताकि प्रतिद्वंद्वी की प्रभावी प्रतिक्रिया देने की क्षमता को पंगु बनाया जा सके।
- साइबर हमले शासन, सैन्य तत्परता और जन मनोबल पर श्रृंखलाबद्ध प्रभाव डालते हैं, बिना तत्काल राजनीतिक प्रतिक्रिया को उकसाए, आधुनिक समाज की रीढ़ को बाधित करके।
- मैलवेयर, सुप्त इम्प्लांट्स और औद्योगिक नियंत्रण प्रणालियाँ सक्रियण से वर्षों पहले ही स्थापित की जा सकती हैं, जिससे रणनीतिक आश्चर्य उत्पन्न होता है।
  - 2015–16 में यूक्रेनी पावर ग्रिड पर हमले इस दृष्टिकोण का उदाहरण हैं, जो दिखाते हैं कि सुप्त साइबर उपकरण निर्णायक क्षण में आवश्यक सेवाओं को पंगु बना सकते हैं।

ग्रे-ज़ोन युद्ध में साइबर अभियानों के पीछे तर्क

- ग्रे-ज़ोन में साइबर अभियान रणनीतिक भ्रम और पक्षाघात के लिए डिज़ाइन किए जाते हैं।
  - ये विश्वास को कमजोर करते हैं, निर्णयों में देरी करते हैं और प्रतिद्वंद्वी की शासन या प्रतिक्रिया क्षमता को कम करते हैं।
- लाभ संभाव्य अस्वीकरण में निहित है, क्योंकि साइबर व्यवधान तकनीकी दोषों या दुर्घटनाओं की तरह दिख सकते हैं, जिससे आरोप-प्रत्यारोप और जवाबदेही जटिल हो जाती है।
  - परिणामस्वरूप, राज्य बिना प्रत्यक्ष आक्रामकता के पर्याप्त रणनीतिक लागत थोप सकते हैं।

केस स्टडी: पूर्वसूचक के रूप में साइबर

- **वेनेज़ुएला में हालिया अभियान (2026):** अमेरिकी समन्वित कार्रवाई, जिसने वेनेज़ुएला के राष्ट्रपति को पकड़ने में सफलता पाई, ने साइबर और गतिज अभियानों के एकीकरण को प्रदर्शित किया, जैसे साइबर पूर्व-स्थिति, वायु रक्षा हेरफेर, संचार व्यवधान एवं निगरानी अवसंरचना का शोषण।
- **रूस-यूक्रेन संघर्ष:** 2022 के आक्रमण से पहले, यूक्रेन को सरकारी वेबसाइटों और अवसंरचना पर साइबर हमलों की बौछार का सामना करना पड़ा, जिसने गतिज अभियानों के लिए आधार तैयार किया।
- **चीन की दक्षिण चीन सागर रणनीति:** चीन ने साइबर जासूसी एवं दुष्प्रचार का उपयोग प्रभुत्व व्यक्त करने और प्रतिद्वंद्वी दावेदारों को कमजोर करने के लिए किया है, बिना प्रत्यक्ष टकराव के।
- **ईरान-इज़राइल छाया युद्ध:** दोनों देशों ने अवसंरचना और निजी क्षेत्रों पर साइबर हमलों में प्रतिशोधात्मक भागीदारी की है, खुले युद्ध से बचते हुए भी रणनीतिक क्षति पहुँचाई है।

भारत का अनुभव: ग्रे-ज़ोन से सीख

- **भारत – चीन:**
  - अवसंरचना और मनोवैज्ञानिक युद्ध: चीन ने LAC के साथ अपने ग्रे-ज़ोन अभियान को जारी रखा है, विवादित क्षेत्रों के पास दोहरे उपयोग वाली अवसंरचना (सड़कें, हेलीपैड, गाँव) का निर्माण करके क्षेत्रीय दावे व्यक्त करने हेतु, और नियमित गश्त के बहाने सैनिकों एवं निगरानी संसाधनों को तैनात करके।
  - गलवान घाटी संघर्ष और आगे: घटना के बाद चीन की रणनीति भारतीय विद्युत ग्रिड और दूरसंचार नेटवर्क में साइबर घुसपैठ पर केंद्रित रही है।
  - वृत्तांत हेरफेर: राज्य मीडिया और कूटनीतिक चैनलों के माध्यम से भारत को आक्रामक के रूप में प्रस्तुत करना।
  - मुंबई ब्लैकआउट (2020): चीनी राज्य-प्रायोजित अभिनेताओं को उत्तरदायी ठहराया गया, इस आउटेज ने उजागर किया कि नागरिक अवसंरचना भू-राजनीतिक संकटों के दौरान दबाव के साधन के रूप में काम कर सकती है।
- **भारत – पाकिस्तान:**
  - साइबर युद्ध वृद्धि (2025): पाकिस्तान ने सरकारी पोर्टलों, वित्तीय संस्थानों और मीडिया आउटलेट्स को निशाना बनाते हुए साइबर हमलों की श्रृंखला शुरू की। इनमें शामिल थे:
    - भारतीय बैंकिंग प्रणालियों पर वितरित सेवा-अस्वीकरण (DDoS) हमले।
    - आधिकारिक वेबसाइटों का विकृतिकरण, जिन पर भारत विरोधी प्रचार डाला गया।
    - सैन्य कर्मियों और महत्वपूर्ण अवसंरचना संचालकों को लक्षित करने वाले फ़िशिंग अभियान।
  - हालांकि, इन घटनाओं ने भारत की साइबर प्रतिरोधक क्षमता में खामियों को उजागर किया, विशेष रूप से आरोप-प्रत्यारोप, समन्वय और सिद्धांतगत स्पष्टता में।

भारत की साइबर तैयारी में संरचनात्मक खामियाँ

- खंडित संस्थागत ढाँचा: साइबर सुरक्षा की जिम्मेदारियाँ नागरिक, सैन्य और क्षेत्रीय एजेंसियों के बीच विभाजित रहती हैं।
- समन्वय की कमी: राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC), राज्य प्राधिकरणों और निजी संचालकों के बीच समन्वय असंगत है।

- नागरिक-सैन्य डिसकनेक्ट: अधिकांश महत्वपूर्ण अवसंरचना जैसे विद्युत ग्रिड, बंदरगाह, दूरसंचार नागरिकों द्वारा संचालित होती है, लेकिन सीधे राष्ट्रीय सुरक्षा से जुड़ी होती है।
- संयुक्त अभ्यासों का अभाव: एकीकृत साइबर-सैन्य अभ्यासों की अनुपस्थिति भारत को संयुक्त साइबर-गतिज परिदृश्यों के लिए अप्रस्तुत छोड़ती है।
- आपूर्ति-श्रृंखला कमजोरियाँ: भारत की विदेशी हार्डवेयर और सॉफ़्टवेयर पर निर्भरता, जो अक्सर प्रतिद्वंद्वी क्षेत्रों से आती है, छिपे हुए जोखिम प्रस्तुत करती है।
- मानव संसाधन की कमी: ऐसे विशेषज्ञों की कमी है जो सूचना प्रौद्योगिकी (IT) और परिचालन प्रौद्योगिकी प्रणालियों को जोड़ सकें।
- अस्पष्ट प्रतिरोधक मुद्रा: भारत में साइबर प्रतिशोध पर स्पष्ट नीतियाँ नहीं हैं। बिना स्पष्ट संकेतों या अनुपातिक प्रतिक्रिया तंत्र के, प्रतिद्वंद्वी साइबर दबाव को कम-जोखिम विकल्प मान सकते हैं।

भारत की साइबर तैयारी में प्रयास और पहल

- **साइबर सुरक्षा के लिए संस्थागत ढाँचा :**
  - **राष्ट्रीय महत्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र (NCIIPC):** इसे 2014 में राष्ट्रीय तकनीकी अनुसंधान संगठन (NTRO) के अंतर्गत एक शीर्ष निकाय के रूप में स्थापित किया गया था, जो भारत की महत्वपूर्ण सूचना अवसंरचना (CII) की सुरक्षा के लिए उत्तरदायी है।
  - **भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया टीम (CERT-In):** यह साइबर सुरक्षा घटनाओं का जवाब देने के लिए राष्ट्रीय नोडल एजेंसी के रूप में कार्य करती है।
    - CERT-In द्वारा जारी नए निर्देश संगठनों को छह घंटे के अंदर साइबर सुरक्षा घटनाओं की रिपोर्ट करने, 180 दिनों तक लॉग बनाए रखने और भारतीय टाइम सर्वरों के साथ समन्वय करने का आदेश देते हैं ताकि घटना प्रतिक्रिया की दक्षता में सुधार हो सके।
- **नीति और रणनीतिक ढाँचे :**
  - **राष्ट्रीय साइबर सुरक्षा नीति (NCSP) 2013:** यह भारत की साइबरस्पेस को सुरक्षित करने की दृष्टि को रेखांकित करने वाला आधारभूत नीति दस्तावेज बना हुआ है।
  - **नई राष्ट्रीय साइबर सुरक्षा रणनीति (NCS):** वर्तमान में मसौदा चरण में है, जिसका उद्देश्य आधुनिक ग्रे-ज़ोन और हाइब्रिड खतरों को अद्यतन एवं संबोधित करना है।
  - **राष्ट्रीय साइबर सुरक्षा समन्वय केंद्र (NCCC):** यह वास्तविक समय निगरानी और समन्वय केंद्र के रूप में कार्य करता है।
  - **राष्ट्रीय साइबर अपराध रिपोर्टिंग पोर्टल:** यह नागरिकों को साइबर अपराधों की रिपोर्ट करने के लिए एक केंद्रीकृत तंत्र प्रदान करता है, विशेष रूप से वित्तीय धोखाधड़ी, पहचान की चोरी और बाल शोषण से संबंधित मामलों में।
- **क्षमता निर्माण और मानव संसाधन विकास:**
  - **साइबर सुरक्षित भारत पहल:** इसका उद्देश्य राज्य और जिला स्तर पर सरकारी अधिकारियों के बीच साइबर स्वच्छता एवं जागरूकता को बढ़ावा देना है।

- **सूचना सुरक्षा शिक्षा और जागरूकता (ISEA) कार्यक्रम:** इसका उद्देश्य शैक्षणिक संस्थानों में प्रशिक्षण कार्यक्रमों के माध्यम से साइबर सुरक्षा में कुशल जनशक्ति तैयार करना है।
- **रक्षा साइबर अनुसंधान:** कृत्रिम बुद्धिमत्ता और रोबोटिक्स केंद्र (CAIR), DRDO के अंतर्गत, साइबर सुरक्षा, क्रिप्टोग्राफी और सुरक्षित नेटवर्क संचार प्रौद्योगिकियों में अनुसंधान एवं विकास का नेतृत्व करता है।

- **कानूनी और विनियामक ढाँचा:**
  - **सूचना प्रौद्योगिकी अधिनियम, 2000 (संशोधन 2008):** यह साइबर अपराधों को संबोधित करने के लिए कानूनी आधार प्रदान करता है, जिसमें हैकिंग, डेटा चोरी और पहचान धोखाधड़ी जैसे अपराधों को परिभाषित किया गया है।
    - 2008 के संशोधन ने इसके दायरे का विस्तार किया ताकि संगठनों और मध्यस्थों के लिए साइबर सुरक्षा जिम्मेदारियाँ शामिल की जा सकें।
  - **डेटा संरक्षण और डिजिटल इंडिया अधिनियम (मसौदा चरण):** इसका उद्देश्य आईटी अधिनियम को प्रतिस्थापित करना है, जिसमें डेटा शासन, साइबर दायित्व और महत्वपूर्ण अवसंरचना संरक्षण पर अधिक मजबूत प्रावधान शामिल होंगे, जो वैश्विक मानकों के अनुरूप होंगे।
- **सार्वजनिक–निजी सहयोग :**
  - NCIIPC, निजी उपयोगिताओं और साइबर सुरक्षा कंपनियों के बीच कमजोरियों के आकलन के लिए साझेदारी।
  - दूरसंचार ऑपरेटरों और वित्तीय संस्थानों के साथ संयुक्त अभ्यास, खतरे की प्रतिक्रिया के लिए।
- **अंतरराष्ट्रीय सहयोग :**
  - अमेरिका, जापान, ऑस्ट्रेलिया, फ्रांस और इज़राइल जैसे देशों के साथ साइबर खतरे साझा करने एवं क्षमता निर्माण पर द्विपक्षीय समझौते।
  - आपूर्ति श्रृंखला सुरक्षा और महत्वपूर्ण अवसंरचना संरक्षण पर केंद्रित चतुष्कोणीय सुरक्षा संवाद (QUAD) साइबर पहलों में भागीदारी।
  - बुडापेस्ट कन्वेंशन ऑन साइबरक्राइम (पर्यवेक्षक स्थिति) और संयुक्त राष्ट्र ओपन-एंडेड वर्किंग ग्रुप (OEWG) ऑन साइबर सुरक्षा जैसे वैश्विक ढाँचों में सदस्यता।

आगे की राह: एक सुसंगत साइबर रणनीति की ओर

- **सैन्य सिद्धांत में साइबर रक्षा का एकीकरण:** साइबर अभियानों को भारत की राष्ट्रीय रक्षा योजना का मुख्य तत्व बनना चाहिए, न कि एक परिधीय तकनीकी मुद्दा।
- **संयुक्त साइबर अभ्यास:** नियमित रेड-टीमिंग और एकीकृत नागरिक-सैन्य अभ्यास यथार्थवादी तैयारी के लिए आवश्यक हैं।
- **आपूर्ति-श्रृंखला सुरक्षा:** भारत को घरेलू विनिर्माण, कठोर ऑडिट और महत्वपूर्ण अवसंरचना घटकों की सुरक्षित सोर्सिंग को प्राथमिकता देनी चाहिए।
- **क्षमता संकेत :** रणनीतिक संचार महत्वपूर्ण है—निवारण उतना ही विश्वसनीयता पर निर्भर करता है जितना वास्तविक क्षमता पर।
- **मानव विशेषज्ञता का निर्माण:** साइबर-तकनीकी शिक्षा और परिचालन प्रशिक्षण में निवेश औद्योगिक प्रणालियों की रक्षा में महत्वपूर्ण कौशल अंतराल को समाप्त करेगा।

- **उभरते फोकस क्षेत्र :** भारत की विकसित होती रणनीति यह समझ दर्शाती है कि साइबर खतरे हाइब्रिड युद्ध और ग्रे-ज़ोन दबाव के साथ विलय हो रहे हैं। वर्तमान फोकस क्षेत्रों में शामिल हैं:
  - निवारण के लिए आक्रामक साइबर क्षमताओं का विकास।
  - विद्युत ग्रिड और दूरसंचार नेटवर्क की साइबर-भौतिक सुरक्षा को बढ़ाना।
  - एकीकृत रणनीतिक नियंत्रण के लिए राष्ट्रीय साइबर कमांड की स्थापना।
  - सुरक्षित हार्डवेयर और क्रिप्टोग्राफी के लिए स्वदेशी प्रौद्योगिकी को बढ़ावा देना।
  - पूर्वानुमानित खतरे का पता लगाने के लिए एआई और बिग डेटा एनालिटिक्स का एकीकरण।

Source: ORF

दैनिक मुख्य परीक्षा अभ्यास प्रश्न

प्रश्न: ग्रे-ज़ोन युद्ध, विशेष रूप से साइबर अभियानों के माध्यम से, किस प्रकार अंतरराष्ट्रीय संबंधों में प्रतिरोध और संप्रभुता की पारंपरिक अवधारणाओं को चुनौती देता है? पाकिस्तान और चीन के साथ भारत की संलग्नताओं के संदर्भ में मूल्यांकन कीजिए।