कमांड साइबर ऑपरेशंस और सपोर्ट विंग्स

प्रिलिम्स के लिये:

कमांड साइबर ऑपरेशंस और सपोर्ट विंग्स (CCOSW), टेक्निकल एंट्री स्कीम मॉडल, साइबर सुरक्षा

मेन्स के लिये:

भारतीय सेना की साइबर सुरक्षा में CCOSWs का महत्त्व

चर्चा में क्यों?

हाल ही में **सेना कमांडरों के सम्मेलन (Army Commanders' Conference- ACC)** में भारतीय सेना ने अपनी साइबर सुरक्षा क्षमताओं को मज़बूत करने, नेटवर्क की रक्षा करने और साइबर स्पेस के प्रमुख डोमेन में खतरों का मुकाबला करने के लिये **कमांड साइबर ऑपरेशंस एंड सपोर्ट विंग्स (Command Cyber Operations and Support Wings- CCOSW)** को संचालित करने का निर्णय लिया।

सेना कमांडरों का सम्मेलन (ACC):

- **ACC** एक द्विवार्षिक संस्थागत कार्यक्रम है जो **भारतीय सेना के लिये महत्त्वपूर्ण नीतियों पर उच्च स्तरीय वैचारिक चर्चा और निर्णय लेने हेतु एक मंच के रूप में कार्य करता है।**
- हाल ही में हुए सम्मेलन में विभिन्न एजेंडा बिंदुओं, **सेना मुख्यालय द्वारा प्राप्त अद्यतन सूचनाओं, परिवर्तन पहलों की प्रगति** और **बजट प्रबंधन** पर चर्चा की गई।

कमांड साइबर ऑपरेशंस और सपोर्ट विंग्स:

- **परिचय:**
    - CCOSWs भारतीय सेना की एक विशेष इकाई है जो **अनिवार्य साइबर सुरक्षा सुनिश्चित करने में सहायता करेगी।**
        - यह इकाई **नेटवर्क सुरक्षा और भारतीय सेना की साइबर सुरक्षा बढ़ाने** में महत्त्वपूर्ण भूमिका अदा करेगी।
    - यह **भारतीय सेना में आधुनिक संचार प्रणालियों और नेटवर्क के बेहतर उपयोग की सुविधा भी प्रदान करेगी।**
- **महत्त्व:**
    - **नेटवर्क केंद्रितता की ओर पलायन** और **आधुनिक संचार प्रणालियों पर बढ़ती निर्भरता** को देखते हुए CCOSW काफी महत्त्वपूर्ण है।
        - CCOSW भारतीय सेना को **ग्रे ज़ोन** और **साइबर युद्ध में अपने विरोधियों से एक कदम आगे रहने एवं मुकाबला करने** में मदद करेगा।
    - भारतीय सेना संबंधी **गोपनीयता, अखंडता और महत्त्वपूर्ण जानकारी की उपलब्धता को बनाए** रखने में CCOSW की भूमिका महत्त्वपूर्ण है।
    - CCOSW **भारतीय सेना के संचार नेटवर्क को साइबर हमलों से सुरक्षित रखने, भारतीय सेना के नेटवर्क के लिये साइबर खतरों की पहचान करने और उन्हें कम करने में मदद करेगा।**

सम्मेलन के अन्य प्रमुख बिंदु:

- **प्रशिक्षण और प्रौद्योगिकी का समन्वय:**

  - **सभी सुरक्षा बलों में बेहतर आधुनिक संचार प्रणालियों और नेटवर्क की सुविधा प्रदान करना।**
- **बल संरचना और अनुकूलन:**
  - बल संरचना और अनुकूलन, **आधुनिकीकरण** एवं **प्रौद्योगिकी समावेशन, प्रक्रियाओं तथा कार्यों, मानव संसाधन प्रबंधन** और **एकीकरण** की सहायता से प्रमुख क्षेत्रों में जारी परिवर्तनकारी पहलों की प्रगति निर्धारित करना।
  - **अग्निपथ योजना** के कुशल कार्यान्वयन पर विचार-विमर्श।
  - जनवरी 2024 से **मौजूदा (5-वर्षीय) 1+3+1 वर्ष की तकनीकी प्रविष्टि योजना (TES) मॉडल से (4-वर्ष) 3 + 1 TES मॉडल** में संक्रमण।
    - बी.टेक स्नातकों के रूप में अधिकारी प्रवेश के लिये मौजूदा पाँच वर्षीय TES मॉडल 1999 से लागू है।
      - मौजूदा मॉडल के तहत **1 वर्ष का सैन्य प्रशिक्षण दिया जाता है, इसके बाद कैडेट ट्रेनिंग विंग्स (CTWs) में 3 वर्ष की बी.टेक डिग्री** और **सेना के तीन इंजीनियरिंग कॉलेजों में से एक में 1 वर्ष की डिग्री** दी जाती है।
    - आगामी **नए मॉडल में CTWs में 3 वर्ष का तकनीकी प्रशिक्षण** होगा, इसके बाद **1 वर्ष की बेसिक मिलिट्री ट्रेनिंग (BMT)** होगी।
      - नए मॉडल को **मार्च 2023** में **अखिल भारतीय तकनीकी शिक्षा परिषद (AICTE)** की मंज़ूरी मिल गई है।
- **पैरालंपिक आयोजन:**
  - पैरालंपिक आयोजनों के लिये चयनित प्रेरित सैनिकों की पहचान करना और उन्हें प्रशिक्षण देना।

साइबर युद्ध से निपटने हेतु भारत की पहल:

- **रक्षा साइबर एजेंसी:**
  - **यह साइबर मुद्दों से निपटने वाला एक त्रि-सेवा अभिकरण है और राष्ट्रीय साइबर सुरक्षा समन्वयक, राष्ट्रीय तकनीकी अनुसंधान संगठन जैसे** अन्य अभिकरणों के साथ समन्वय करता है।
  - यह अभिकरण रक्षा बलों के लिये साइबर सिद्धांत, रणनीति और नीति तैयार करने के लिये उत्तरदायी है। यह **साइबर क्षेत्र में संयुक्त प्रशिक्षण, अभ्यास एवं संचालन का भी आयोजन करता है।**
- **भारतीय कंप्यूटर आपातकालीन प्रतिक्रिया दल** (Indian Computer Emergency Response Team- CERT-In):
  - यह साइबर सुरक्षा संबंधी घटनाओं के मामले में तीव्रता से कारवाई करने और विभिन्न क्षेत्रों को साइबर सुरक्षा सेवाएँ प्रदान करने के लिये राष्ट्रीय नोडल एजेंसी है।
- **राष्ट्रीय महत्त्वपूर्ण सूचना अवसंरचना संरक्षण केंद्र** (National Critical Information Infrastructure Protection Centre- NCIIPC):
  - यह देश की महत्त्वपूर्ण सूचना अवसंरचना, जैसे- विद्युत, बैंकिंग, रक्षा आदि की सुरक्षा के लिये राष्ट्रीय एजेंसी है।
- **साइबर स्वच्छता केंद्र (बोटनेट क्लीनिंग एंड मालवेयर एनालिसिस सेंटर):**
  - यह संक्रमित उपकरणों का पता लगाने और वायरस को हटाने तथा **मैलवेयर विश्लेषण रिपोर्ट प्रदान करने हेतु एक मंच** है।

आगे की राह

- **एक ऐसी व्यापक साइबर सुरक्षा रणनीति विकसित करना जो भारतीय सशस्त्र बलों** में अन्य साइबर सुरक्षा क्षमताओं के साथ **CCOSW को एकीकृत करे,** ताकि साइबर हमलों हेतु सहज समन्वय एवं प्रभावी प्रतिक्रिया सुनिश्चित की जा सके।
- **भारतीय सेना के सभी कर्मियों हेतु साइबर सुरक्षा प्रशिक्षण और जागरूकता कार्यक्रमों को प्राथमिकता देते हुए आधुनिक संचार प्रणालियों एवं नेटवर्क में निवेश करना जारी** रखना ताकि यह सुनिश्चित किया जा सके कि वे साइबर खतरों की पहचान करने तथा उनका सामना करने के लिये आवश्यक कौशल से युक्त हों।
- उभरते सुरक्षा परिदृश्यों के आलोक में **साइबर सुरक्षा नीतियों और प्रक्रियाओं की नियमित समीक्षा एवं अद्यतन करना, ताकि यह सुनिश्चित किया जा सके** कि भारतीय सेना भविष्य में साइबर खतरों से निपटने हेतु तैयार रहे।

UPSC सिविल सेवा परीक्षा, विगत वर्ष के प्रश्न:

???????????:

प्रश्न. भारत में किसी व्यक्ति के लिये साइबर बीमा कराने पर निधि की हानि की भरपाई एवं अन्य लाभों के अतिरिक्त सामान्यतः निम्नलिखित में से कौन-कौन से लाभ दिये जाते हैं? (2020)

दृष्टि The Vision

1. यदि कोई मैलवेयर कंप्यूटर तक पहुँच बाधित कर देता है, तो कंप्यूटर प्रणाली को पुनः प्रचालित करने में लगने वाली लागत।
2. यदि यह प्रमाणित हो जाता है कि किसी शरारती तत्त्व द्वारा जान-बूझकर कंप्यूटर को नुकसान पहुँचाया गया है तो नए कंप्यूटर की लागत।
3. यदि साइबर बलात्-ग्रहण होता है तो इस हानि को न्यूनतम करने के लिये विशेषज्ञ परामर्शदाता की सेवाएँ लेने पर लगने वाली लागत।
4. यदि कोई तीसरा पक्ष मुकदमा दायर करता है तो न्यायालय में बचाव करने में लगने वाली लागत।

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1, 2 और 4
(b) केवल 1, 3 और 4
(c) केवल 2 और 3
(d) 1, 2, 3 और 4

उत्तर: (b)

प्रश्न. भारत में साइबर सुरक्षा घटनाओं पर रिपोर्ट करना निम्नलिखित में से किसके/किनके लिये विधितः अधिदेशात्मक है? (2017)

1. सेवा प्रदाता (सर्विस प्रोवाइडर)
2. डेटा सेंटर
3. कॉर्पोरेट निकाय (बॉडी कॉर्पोरेट)

नीचे दिये गए कूट का प्रयोग कर सही उत्तर चुनिये:

(a) केवल 1
(b) केवल 1 और 2
(c) केवल 3
(d) 1, 2 और 3

उत्तर: (d)

?????

प्रश्न. साइबर सुरक्षा के विभिन्न तत्त्व क्या हैं? साइबर सुरक्षा की चुनौतियों को ध्यान में रखते हुए समीक्षा कीजिये कि भारत ने किस हद तक एक व्यापक राष्ट्रीय साइबर सुरक्षा रणनीति सफलतापूर्वक विकसित की है। **(2022)**

स्रोत: द हिंदू

PDF Refernece URL: https://www.drishtiias.com/hindi/printpdf/command-cyber-operations-and-support-wings