Command Cyber Operations and Support Wings

For Prelims: CCOSW, Technical Entry Scheme model, Cyber security

For Mains: Significance of the CCOSWs in the Indian Army's cybersecurity posture

Why in News?

In the recent **Army Commanders' Conference (ACC),** the Indian Army decided to operationalize the **Command Cyber Operations and Support Wings (CCOSWs)** to strengthen its cybersecurity **capabilities**, defend its networks, and counter threats in the key domain of **cyberspace.**

What is the Army Commanders' Conference (ACC)?

- The ACC is a **biannual institutional event** that serves as a platform for **high-level conceptual discussions and decision-making on important policies for the Indian Army.**
- The latest conference discussed various agenda points, updates from the Army Headquarters, progress on **transformation initiatives, and budget management.**

What are CCOSWs?

- **About:**
  - The CCOSWs are a specialized unit of the Indian Army that will assist the **formations in undertaking mandated cyber security functions.**
    - The unit will be responsible for **safeguarding the networks and enhancing the cybersecurity posture** of the Indian Army.
  - They will also facilitate better **utilization of modern communication systems and networks within the Indian Army.**
- **Importance:**
  - The migration towards **network centricity and increased reliance on modern communication systems** makes the CCOSWs important.
    - The CCOSWs will help the Indian Army counter their adversaries in the **grey zone and their cyber warfare.** And to stay ahead of its **adversaries in terms of cybersecurity.**
  - The CCOSWs will be instrumental in maintaining the **confidentiality, integrity, and availability of critical information.**
  - The CCOSWs will ensure that the Indian Army's communication networks are **secure from cyber-attacks.** And will be responsible for identifying and **mitigating cyber threats to the Indian Army's networks.**

What Were the Other Key Decisions Made in ACC?

- **Training and Technology Infusion:**
  - Nominating lead directorates and test bed formations to evolve optimal employment philosophies and facilitate better **modern communication systems and networks across the force.**
- **Force Structuring and Optimization:**
  - Quantifying progress on the ongoing transformational initiatives in the key domains of **force structuring and optimization, modernization and technology infusion, processes and functions, human resource management, and jointness and integration.**
  - Deliberating upon the efficient implementation of the **Agnipath Scheme.**
  - Transitioning from the existing (5-year) **1+3+1 years Technical Entry Scheme (TES) model to (4-year) 3 + 1 TES model** from January 2024 onwards.
    - The current five-year TES model for officer entry as B.Tech graduates has been in place since 1999.
      - Under the current model, **1 year of military training is imparted, followed by 3 years of B.Tech degree at Cadet Training Wings (CTWs) and 1 year at one of the three engineering colleges of the Army.**
    - The Upcoming new model will have **3 years of technical training at CTWs,** followed by **1 year of Basic Military Training (BMT).**
      - The new model has received AICTE **approval in March 2023.**
- **Paralympic Events:**
  - Identifying and training selected motivated soldiers for **paralympic events.**

What are India's Initiatives in Cyber Warfare?

- **Defence Cyber Agency:**
  - It is a tri-service agency that deals with cyber issues and coordinates with other agencies such as **the National Cyber Security Coordinator, National Technical Research Organisation, etc.**
    - The Agency is responsible for formulating cyber doctrine, strategy, and policy for the defense forces. It also conducts **joint training, exercises, and operations in the cyber domain.**
- **Indian Computer Emergency Response Team (CERT-In):**
  - This is the national nodal agency for responding to **cyber security incidents and providing cyber security services** to various sectors.
- **National Critical Information Infrastructure Protection Centre (NCIIPC):**
  - This is the national agency for protecting the **critical information infrastructure of the country,** such as power, banking, defense, etc.
- **Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre):**
  - This is a platform for detecting and cleaning infected devices and providing **malware analysis reports.**

Way Forward

- Develop a **comprehensive cybersecurity strategy** that integrates the **CCOSWs with other cybersecurity capabilities** across the Indian Armed Forces, to ensure seamless coordination and effective response to cyber-attacks.
- Continue to **invest in modern communication systems and networks,** while also prioritizing cybersecurity training and awareness programs for all personnel within the Indian Army to ensure they are equipped with the **necessary skills** to identify and **respond to cyber threats.**
- **Regularly review and update the cybersecurity policies** and procedures in light of emerging security scenarios, to ensure the Indian Army remains prepared to tackle cyber threats in the future.

UPSC Civil Services Examination, Previous Year Questions (PYQs)

Prelims

Q.1 In India, under cyber insurance for individuals, which of the following benefits are generally covered, in addition to payment for the loss of funds and other benefits? (2020)

1. Cost of restoration of the computer system in case of malware disrupting access to one's computer
2. Cost of a new computer if some miscreant wilfully damages it, if proved so
3. Cost of hiring a specialised consultant to minimise the loss in case of cyber extortion
4. Cost of defence in the Court of Law if any third party files a suit

Select the correct answer using the code given below:

(a) 1, 2 and 4 only
(b) 1, 3 and 4 only
(c) 2 and 3 only
(d) 1, 2, 3 and 4

Ans: (b)

Q2. In India, it is legally mandatory for which of the following to report on cyber security incidents? (2017)

1. Service providers
2. Data centres
3. Body corporate

Select the correct answer using the code given below:

(a) 1 only
(b) 1 and 2 only
(c) 3 only
(d) 1, 2 and 3

Ans: (d)

Mains

Q. What are the different elements of cyber security? Keeping in view the challenges in cyber security, examine the extent to which India has successfully developed a comprehensive National Cyber Security Strategy. **(2022)**

Source: TH