- **Lack of adequate infrastructure and trained staff:** There are currently around 30,000 cyber security vacancies in India but demand far outstrips supply of people with required skills.
- **Sophisticated nature of attacks**: Though phishing is a generally well-known attack, hackers and malicious actors are becoming smarter due to technological evolution, and their attacks are becoming more and more sophisticated as shown by the Wannacry and Petya ransomware.
- **Lack of coordination**: In India, critical infrastructure is owned by both public sector and private sector, both operating with their own norms and protocols for protecting their infrastructure from cyber-attacks. The armed forces too have their own agencies for it. Private sector, despite being a major stakeholder in cyberspace, has not been involved proactively for consultation and development of cybersecurity architecture in India.

To tackle these, the government has taken steps such as formation of National Cyber Coordination Centre (NCCC), Indian Computer Emergency Response Team (CERT-In), National Cyber Security Policy 2013 etc. Recently, Indian Cyber Crime Coordination Centre (I4C) was set up to deal with all types of cybercrimes in a comprehensive and coordinated manner. In addition, India needs to undertake the following **steps** to address the aforementioned challenges:

- **Ensure coordination:** National Cybersecurity Coordinator (NCC) may be **strengthened** to bring about much-needed **synergy among various institutions** and work out a coordinated approach to cyber security.
- **Cyber-attack deterrence:** India needs to make a proper assessment of an offensive cyber doctrine adopted by many countries where they are acquiring offensive capabilities by building bits of software called 'cyberweapons' to do enormous damage to the adversary's networks.
- **Investment in cybersecurity by businesses:** Investment in IT security has to be increased with adoption of a cybersecurity plan, purchase of cyber-insurance as well as appointment of a data security officer.
- **Amendment of IT Act 2008:** The regulations need to keep pace with the changing cyber scenario to ensure that penalties serve as deterrence for crimes. For example, in the Indian IT Act, financial fraud is still a bailable offence.
- **Become part of international conventions and adopting international standards:** India should consider signing of the Budapest Convention on cybercrime to garner global support. Also, adhering to international standards must be made applicable for all government websites, applications before hosting and publishing.
- **Establishing cybersecurity framework at state level:** For example, establishment of state CERT to work in conjunction with CERT-In.

The government of India plans to launch a National Cyber Security Strategy, which would deal with all issues related to cyber security including standardization, testing, auditing and capacity development.

13. Identify the various issues related to Indo-Bangladesh border and challenges faced in managing this border. What measures has the government taken in this regard?

(250 words) 15

Approach:

- Giving a brief introduction, identify issues related to the Indo-Bangladesh Border.
- Then discuss challenges that are being faced in managing the border.
- Then bring out the measures that have been taken by the government in this regard.
- Conclude accordingly.

Answer:

India shares the longest land border with Bangladesh, stretching over 4097 km, which runs through a diverse topography.

The **issues related to the Indo-Bangladesh border include:**

- **Illegal immigration:** Since 1971 War, illegal immigrants have been pouring into India. They act as a security risk and a social economic threat to the natives.