प्रश्न संख्या (Question No.) 25/10/20

U.P.S.C.

इस भाग में कुछ न लिखें (Don't write anything in this part)

Ques considering the post-pandemic realities there is a need to re-think about the approach on cyber security. Elaborate.

Ans cyber security is protecting cyberspace including critical information infrastructure from attack, damage, misuse etc

Beg According to EY's latest Global information security survey (GISS) - 2018-19 - Indian edition - ~~India~~ one of the highest number of cyber threats have been detected in India and country ranks second in terms of target attacks.

The number of attacks has surged during the pandemic period. several thousands malicious domains and websites are reported to have been registered in a very short period of time; apart from creation of a number of fraudulent UPI IDs and web portals.

~~Cyber security~~:

NEED FOR CYBER SECURITY FRAMEWORK:

① National security imperatives:

The change in military doctrines favouring the need to raise cyber commands reflects a shift in strategies, which include building deterrance in cyberspace

For eg: It need emphasized in Kargil Review committee 1999

(2) Increasing importance of digital economy
The digital economy today comprises 14-15% of India's total economy; is targeted to reach 20% by 2024.

(3) Added complexity: with more inclusion of artificial intelligence (AI), machine learning (ML), data analytics, cloud computing and Internet of things (IOT) cyberspace will become a complex domain, giving rise to issues of techno legal nature.

(4) Securing Data: There are issues related to data sovereignity, data localization internet governance etc.

RECOMMENDATIONS:-

(1) Bringing cyber-security in Education
educational institutions must incorporate courses on cybersecurity.

(2) Promoting indigenization: There is need to create suitable hardware on a unique pattern that can serve localized needs.

(3) Strengthening of existing cyber security framework: National cybersecurity projects such as National cyber

coordination centre (NCCC), National Critical information infrastructure protection centre (NCIIPC) and computer emergency response team (CERT) need to be strengthened manifold and reviewed.

(4) Creating Awareness: With countries resorting to digital warfare and hackers targeting business organisation and government processes, India has to create awareness that not a single person or institution is immune to it.

Way forward: Given the future of technology under Industrial revolution 4.0, India requires a strong cybersecurity framework based on the 4D principles i.e Deter, Detect, Destroy and Document so that it can subvert all attempts towards any cyber challenges.

—x—x—x—