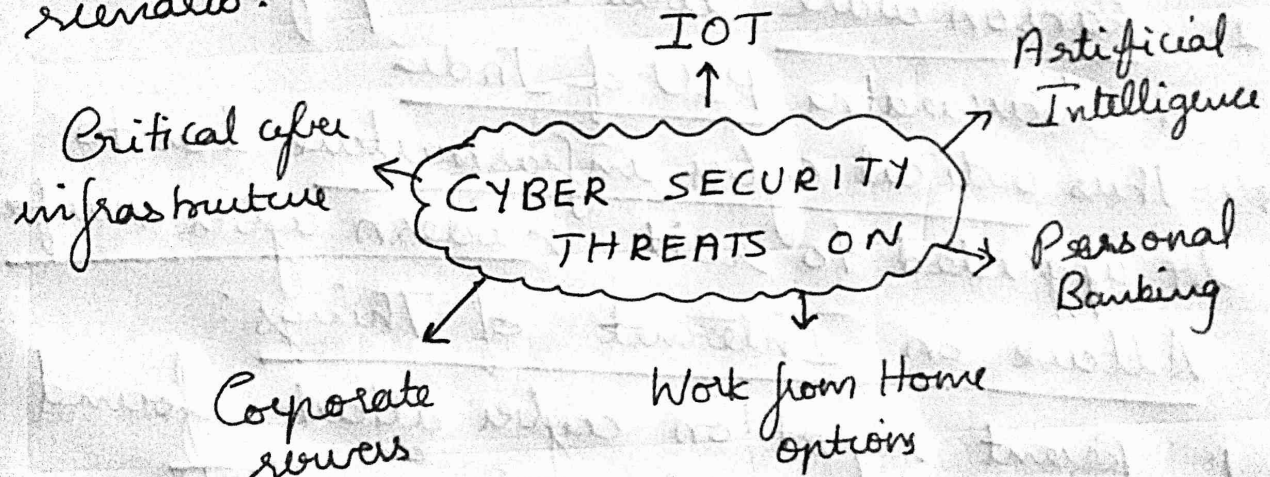
1. Considering the post pandemic realities there is a need to re-think about the approach on cyber security. Elaborate.

The post pandemic situation has created many threat not only to the society/economy but also in the cyber space. Recent attacks on IOT, personal banking and internet servers by malware and hackers define the new terms to be adopted in post-scenario.



Recent malware attacks:

1. Work from home options reported more attack in post pandemic
2. Present scenario requires new credibility in cyber infrastructure.
3. Cyber securities are to be designed to suit the present Information Technology options

2. Phishing in personal banking sector:

1. Pandemic increase usage of digital transactions
2. Thus banking internet in Andhra Pradesh recently crashed at customer side due to phishing activities.
3. New virus cyber activities are emerging which requires new outlook.

3. Attacks on Cyber infrastructure:

1. In the post-pandemic, requirement of money increased for all illegal hackers.
2. Ransom ware was recently found in a Navaratna PSU of India
3. Thus critical cyber infrastructure has to be upgraded to suit modern cyber warfare

4. Attack on Internet of Things:

1. Recent report on cyber attack found Trojan virus infiltration on IOT.
2. Infiltration at highest level created unusual activities in IOT appliances.
3. Government and Kaspersky formed a Kub lab to prevent attack on IOT in India

As desperate time require desperate measure, the cyber infrastructure and critical data has to be secured through advanced cyber walls.