A balance between data localisation and data privacy has to be established by government of India to crack the cyber crimes. Explain (1).

Data is the 'new oil'. In the era of Industrial revolution 4.0, any country that can generate copious data is a superpower when information is processed. This very aspect has led to growth of cyber crimes in the world. India can be an attractive target given its vast resources.

Nature of Cyber crimes:-

→ Cheating, swindling, identity theft, hacking happening in online virtual world, with intention to cause harm to country or person. is called cyber crime
→ These are transnational in nature, can be performed by any entity.
→ In certain cases it can be intentional or unintentional.
example:- Leaking information of Zomato users - unintentional.
Facebook selling data to Cambridge Analytica - intentional
to help to influence elections

Thus to solve a cybercrime, one needs access to 'servers' which houses digital footprint of perpetrator. This necessitates capture and storage of data by respective countries - LOCALISATION.

Need for Localisation in India:-

1) Data is treated as 'NATIONAL ASSET'. Thus any threat to it leads to compromising national sovereignty.
2) Justice Srikrishna committee reports that top 10 most accessed websites in India are owned by US entities.
3) Thus, when any investigation routine needs to be conducted, police officials are forced to rely on arduous bilateral - Mutual Legal Assistant Treaty
4) Data localisation would enable a copy of national data on Indian soil, expediating the cybercrime investigation, ease of access.

But this very extent of localisation enabled accessibility sidelines the privacy guaranteed.

Question of privacy:-

1) Privacy is the blanket security guaranteed by social media operators.
2) Localisation can give a free hand for monitoring its citizen's data giving rise to surveillance state
3) Supreme courts notings on Puttaswamy's 'Right to Privacy' is held as leverage by social media entities to deter government from accessing legitimate data for its security reasons.

Example:- Whatsapp, Facebook rejection on sharing encryption details for dealing with mob lynching, hate propoganda.

Balancing act between Data Privacy and localisation:-

Digital India needs cyber security. With 90% of country's IT capability outside the government, CYBER PATRIOTISM is pivotal in breaking cyber monopoly of data. The following steps can be taken for a balancing act.

1) Giving proper checks, freedom, 'Right to forgot' data as enshrined in GDPR laws of European Union
2) Implementing the Data protection bill 2018.
3) Giving robust sovereign privacy policy to sign executive agreement for CLOUD Act of USA.
4) Set up independent authority to oversee Copc provision on data theft

When future wars is predicted to be a 'cyberwarfare', robust cyber security implementation shouldn't be hindered by the doubts on privacy and localisation.