Unreliable Telecom Business - Huawei Issue

What is the issue?

India continues to buy Huawei’s core network equipment, though many developing nations banned the product manufacturer.

What are the concerns with Huawei?

- Network switches, gateways, routers, and bridges, the kit that controls how and where data is sent - is what Huawei really does.
- These core infrastructure devices touch everything traversing the internet and are critical to it functioning properly.
- Although it sells laptops and phones too, Huawei's equipment is especially prominent in the parts of the network closer to the data centers, and it's this equipment which is raising concerns.
- The reason behind such concerns is due to Huawei’s origin, the company was by Ren Zhengfei, formerly an engineer in the People's Liberation Army.
- His connections to the military and to the Communist Party, alongside those of senior Huawei executives, have been cited as a security concern for foreign customers.
- Three nations in the Five Eyes intelligence alliance, the US, Australia, and New Zealand, have effectively prohibited the installation of Huawei equipment as part of the next generation of telecommunications equipment.
- Huawei has been accused by US intelligence of being funded by Chinese state security, and UK's National Cyber Security Centre said the company posed a threat to national security.
- Elsewhere, nations including India and Germany have expressed their concerns about including Huawei equipment as they upgrade telecommunications infrastructure for 5G.
- Huawei has also moved fast on developing efficient technology platforms which is hurting rival players.
- In the geopolitical sphere, there is a tussle between the US and China for dominance and the emergence of Huawei as a global major could be tilting this battle in favor of the Asian country in the area of communications technology.

What is account of lame actions of the government?

- Indian operators continue to buy from the Chinese vendor, despite the fact that the Department of Telecommunications has in the past raised concerns over possible bugs in the equipment sold by the Chinese company, but has not taken any action in the absence of any conclusive evidence.
- Indian Security agencies have also raised fears over the possible presence of embedded spyware or malicious software ('malware') that could allegedly be used by the Chinese intelligence to snoop into conversations and data flowing through the Indian network or even shut down communications in Delhi and Mumbai sitting in Beijing.
- Union government has not taken a view on the issue even though the security agencies have been flagging concerns for over a decade.
- Back in 2010 when similar concerns were raised against the Chinese company, the then Cabinet Committee on Security approved the setting up of a 'Telecom Testing and Security Certification Centre' (TTSC) and made it mandatory for operators to test all imported equipment.
- As part of the "safe to connect" telecom project in mid-2010, the DoT was given the task to set up the center at a cost of Rs. 50 crore for security certification of all equipment being imported by telecom service providers (TSPs) from October 1, 2013.
- This deadline has since been extended multiple times and until April 1, 2019, operators were not required to do the mandatory certification.
- Meanwhile, Huawei has made deep inroads into the Indian telecom network, not just the private operators but also state-owned Bharat Sanchar Nigam Ltd.

What measures are needed?

- It is high time the government settles, once and for all, whether the security-related allegations relating to the use of Chinese telecom equipment are true or if this is a well-coordinated campaign by rivals of China and Huawei.
- India should take a decision based on facts.
- If the security threat is real indeed, let the Centre take the nation into confidence and restrain Huawei from future contracts.
- At the same time, the policymakers should also act on its stated vision to help local players become an alternative source of high-tech equipment in order to reduce our reliance on imported gear.

Source: Business Line

Quick Fact

Five Eyes Alliance

- The Five Eyes, often abbreviated as FVEY, is an Anglophone intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States.
- The alliance was established in 1941, In spite of continued controversy over its methods, the Five Eyes relationship remains one of the most comprehensive known espionage alliances in history.
- These countries are parties to the multilateral UKUSA Agreement, a treaty for joint cooperation in signals intelligence.
- Since processed intelligence is gathered from multiple sources, the intelligence shared is not restricted to signals intelligence (SIGINT) and often involves defense intelligence as well as human intelligence (HUMINT) and geospatial intelligence (GEOINT).