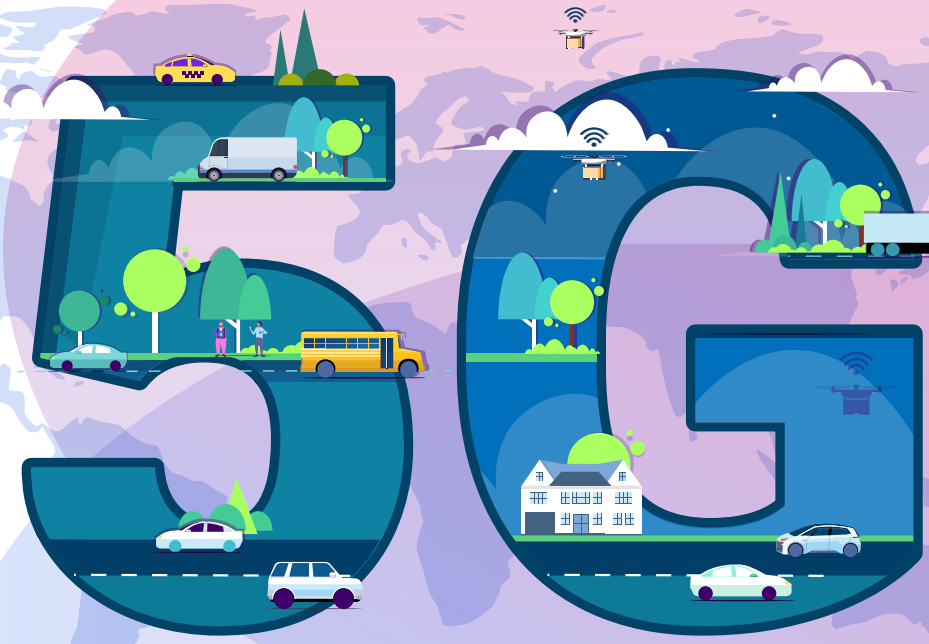
VISIONIAS
INSPIRING INNOVATION

Weekly Focus



TECHNOLOGY

CHALLENGES AND OPPORTUNITIES

Introduction

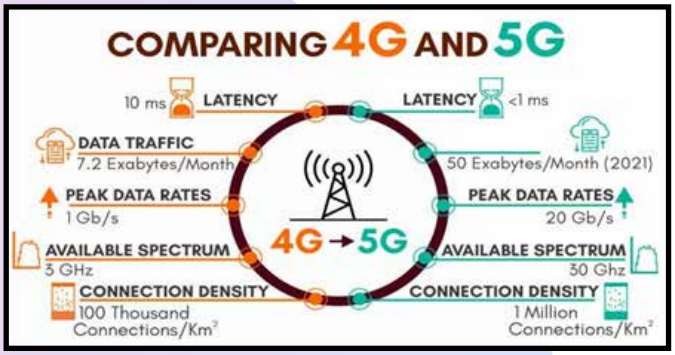
It is estimated that, 5G technology will considerably change the world around us by enabling a new kind of network that is designed to connect virtually everyone and everything together including machines, objects, and devices.

But what exactly is 5G technology and how it works? How can this technology bring about a digital revolution? If a revolution is in the offing, is India ready for this wave of transformation? Also, what are the security challenges coupled with adoption of this technology and what is the connection between the recent Huawei case and 5G? To overcome the possible challenges, what steps can we take? In this edition, we will attempt to

What is 5G Technology and how it works?

- 5G is a **next generation mobile network technology** after 4G LTE networks. It promises to provide **seamless coverage, high datarate, ultra-low latency** and as a result **highly reliable communications.**
- 5G technology is **not a single technology** but an **amalgamation of various technologies** which make the aforesaid performance possible. Following are the major technologies used in 5G:

- **mmWave (millimetre Wave):** 5G technology envisages to use frequencies up to 100GHz which come in the range millimetre **frequencies (30GHz to 300GHz).** In contrast, 4G technology operates in 1GHz to 6GHz band. The advantage of mmWave band is that it is **less used** and also higher frequency wave **carries much more data** than lower frequency wave.
  - **5G New Radio (NR) is the global standard** for a unified, more capable 5G wireless air interface. 5G NR uses two frequency ranges: **sub-6 GHz frequency bands** and frequency bands in the **mmWave range (24-100GHz).**
- **Massive multi-user MIMO (Multiple input multiple output):** This enables the network to have more antennas per unit (signal towers), thus ensuring larger and faster transmission of data.
- **Small Cell stations:** The mmWave technology is more susceptible to obstacles and tend to lose energy more quickly, therefore providing less coverage in comparison to their low frequency counterparts. To overcome this, small cell stations are needed to connect the base stations and users seamlessly. Small cells make use of low-power, short-range wireless transmission systems (or "base stations") that **cover small geographical areas or small proximity indoor and outdoor spaces.**
- **Beamforming:** It can be visualized as a laser beam between transmitting entity and the user. This technology makes transmission of data more directional resulting in **reduced interference and increased energy efficiency** in transmission.
- **NOMA (Non-Orthogonal Multiple Access):** This technology allows multiple signals to use the same frequency channel thus **improving load capacity** of every channel.
- **Mobile Edge Computing (MEC):** MEC brings cloud computing closer to the user physically. This has twin advantages- One, reduced distance **decreases the latency period** and second, by keeping just the required data near the user, it is also reduces the amount of data that the server has to handle, which also **speeds things up.**
  - **Edge computing** is a distributed computing paradigm that brings computation and data storage towards the edge of the network i.e. closer to the location where it is needed by using "cloudlets", It thus provide content caching, service delivery, storage and IoT management resulting in better response times and transfer rates.

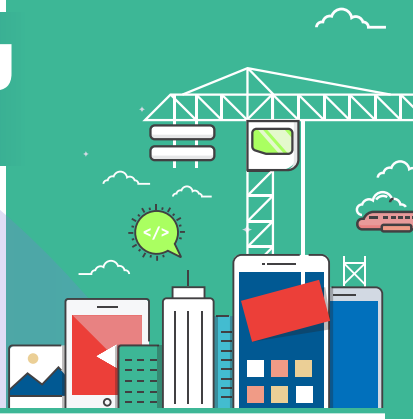


Related definitions and concepts:

- **Bandwidth** commonly measured in bits/second is the maximum rate at which information can be transferred.
- **Throughput** is the actual measure of how much information is successfully transferred.
- **Latency is** the delay between the sender and the receiver decoding the information. This is mainly a function of the signals travel time, and processing time at any nodes the information traverses.
- **Test bed** is a platform for conducting rigorous, transparent, and replicable testing of scientific theories, computational tools, and new technologies.
- **Network virtualization:** Network virtualization is the process of consolidating hardware and software resources into a software-based, virtual network.

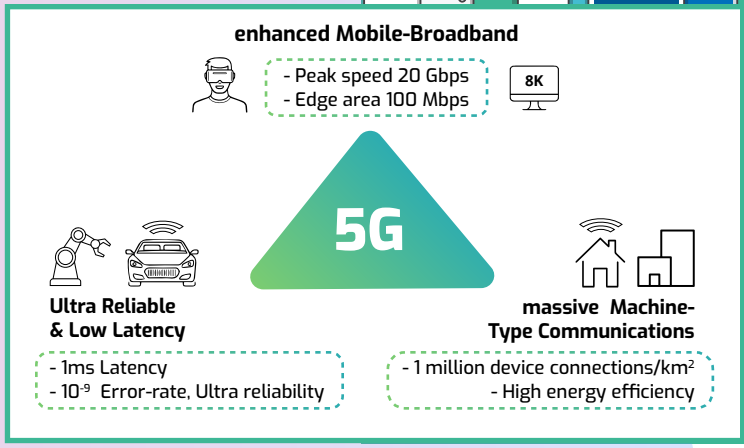
Apart from above, there are several technologies which could become part of the 5G network. The final standard for 5G technology will be set up by the **International Telecommunications Union (ITU).**

How can 5G Technology potentially bring about a digital revolution?



A recent 5G Economy study has estimated that by the year 2035, 5G technology will **generate $13.2 Trillion dollars of global economic output** by supporting a wide range of industries. It also estimated that 5G value chain (including Original Equipment Manufacturer(OEMs), operators, content creators, app developers, and consumers) could alone **support up to 22.3 million jobs globally.**

But how exactly will this revolution be materialized and who will be the major beneficiaries? All the major applications and services supported by 5G can be broadly divided in **three use cases** (A use case is a software and system engineering term that describes how a user uses a system to accomplish a particular goal):



- **High speed use cases** (a.k.a. Enhanced Mobile Broadband (eMBB)): By transmitting data faster and ensuring more uniform data rates, 5G will help speed up a range of applications such as enhanced consumer experience via **high quality streaming, faster storage and access of cloud by businesses, better communication between public institutions and citizens.**

- **Mission-critical communication use cases** (a.k.a. Ultra-Reliable and Low Latency Communications (uRLLC)): This will provide seamless communication between entities making possible real time interactions. Here, we will see new applications that require response in fractions of a second such as **Autonomous Vehicles, Augmented Reality (AR) and Virtual Reality (VR), enhanced range and interactivity of drones.**

- **Massive Internet of Things (IoT)** (a.k.a. Massive Machine-Type Connectivity (mMTC)): 5G is meant to seamlessly connect a massive number of embedded sensors in virtually everything through the ability to scale down in data rates, power, and mobility—providing extremely lean and low-cost connectivity solutions. It is easily showcased in areas like **Smart City Infrastructure and Traffic Management, Industrial Automation, Wearables and Mobile devices, Precision agriculture** etc.

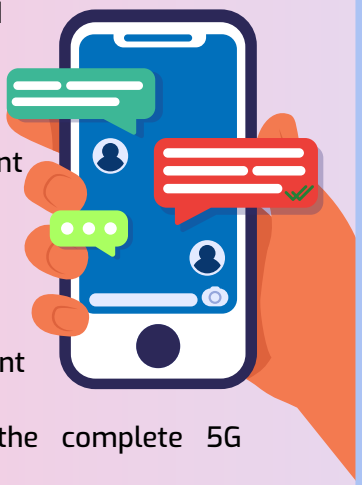
Is India ready for this wave of digital transformation?

According to some estimates, **208 million new subscribers will get connected in India by the year 2025.** Also, it is estimated that increasing 5G subscribers could create a cumulative **economic impact of $1 trillion in India by 2035**. Moreover, the technology will unleash new business opportunities and bring substantial socioeconomic benefits through increase in productivity, improvements in service delivery, optimum use of scarce resources as well as creation of new jobs.

But to realize this potential transformation, several hurdles have to be crossed, ranging from technological, financial, infrastructural and most importantly the security concerns that have arisen.

Technological Challenges:

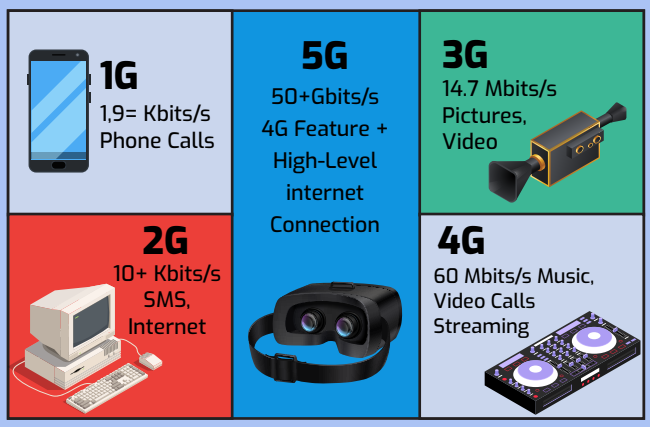
- **Availability of spectrum:** 5G needs a significant amount of **new harmonised mobile spectrum within three key frequency ranges** to deliver widespread coverage and support all use cases: sub-1 GHz, 1-6 GHz and above 6 GHz. This may be difficult due to unavailability of some bands. For example, DoT has accepted ISRO's demand to reserve 26 GHz band primarily for satellite services which will make deployment of 5G challenging.



- **Electronic Equipment Manufacturing:** Imports account for about 90% of India's telecom equipment market resulting in high import dependency on the complete 5G supply chain.
- **Testing Challenges:** 5G technology will need to take on the characterizing and testing of new systems to ensure both performance and regulatory adherence.
  - **mmWave and beamforming technologies** present the biggest testing challenges as they have to be tested simultaneously with other technologies.

Growth of Wireless Networks in India

- The **first mobile phone service** was launched in 1985 on a non- commercial basis, but it was only in 1995 that commercial service was started.
- Beginning 2007, the subscriber base rapidly increased reaching 560 million in 2009 and well over **a billion by 2017.**
- **Early deployment of mobile networks was based on 2G technology,** with **3G technology** entering service in 2010 and **4G in 2016.**
- All mobile services from 2G to 4G offered services based on increasingly advanced phones, with smart phones arriving about a decade ago.



Financial Challenges:

- **Capital Investment:** It is anticipated that industry might require an **additional investment of $60-$70 billion to seamlessly implement 5G networks.** In midst of **rising debt levels** and **market consolidation** activity, the telcos are seen to be constrained on capital expenditure.
  - The Average Revenue Per User (ARPU) for telecom service providers has drastically reduced. The industry had a cumulative debt of Rs. 7.7 trillion in 2018.
- **High Tax burden:** Close to 30% of revenue of Telcos goes to the Government in taxes and levies, which includes Import duty for equipment such as base stations, optical transport gear etc.

Infrastructural Challenges:

- **Backhaul Infrastructure:** India lacks a strong backhaul to transition to 5G. Nearly 75% of cell sites are connected through microwave backhaul, while under 25% sites are connected through fibre. The former has bandwidth issues as it uses traditional bands while the latter provides low latency and unlimited capacity (a prerequisite for 5G).
  - The term **backhaul** is often used in telecommunications and refers to a high capacity line transmitting a signal from a remote site or network to another site, usually a central one. The high throughput offered by 5G will result in high traffic on cellular networks which will need to be backhauled from mobile sites to an operator's core network (Central Exchange).
- **Increasing role of memory and storage infrastructure:** With 5G, the quantum of data generated from users' devices multiplies, resulting in more data that has to be stored, moved, processed and secured. This brings need for large scale enhancement in memory and storage infrastructure.

- **Right of Way (RoW) and Lack of uniform policy framework:** Delays due to complex procedures across states and non-uniformity of levies along with administrative approvals impact telecom service providers in rolling-out Optical Fibre Cables (OFC) and telecom towers necessary for 5G.

Other challenges:

- **Privacy concerns:** From the user's perspective, privacy concerns centre around location tracking, identity, and other personal data. For instance, since 5G uses more antennas with smaller coverage area, it allows for **precise location tracking** of users both inside and outside.
- **Digital Divide:** In the current context, **5G is feasible mainly for more populated areas,** where many antennas can be placed close together. This brings challenge of widening of the **digital divide,** rural areas where user density would be relatively low and regions with poor digital infrastructure would be left out.

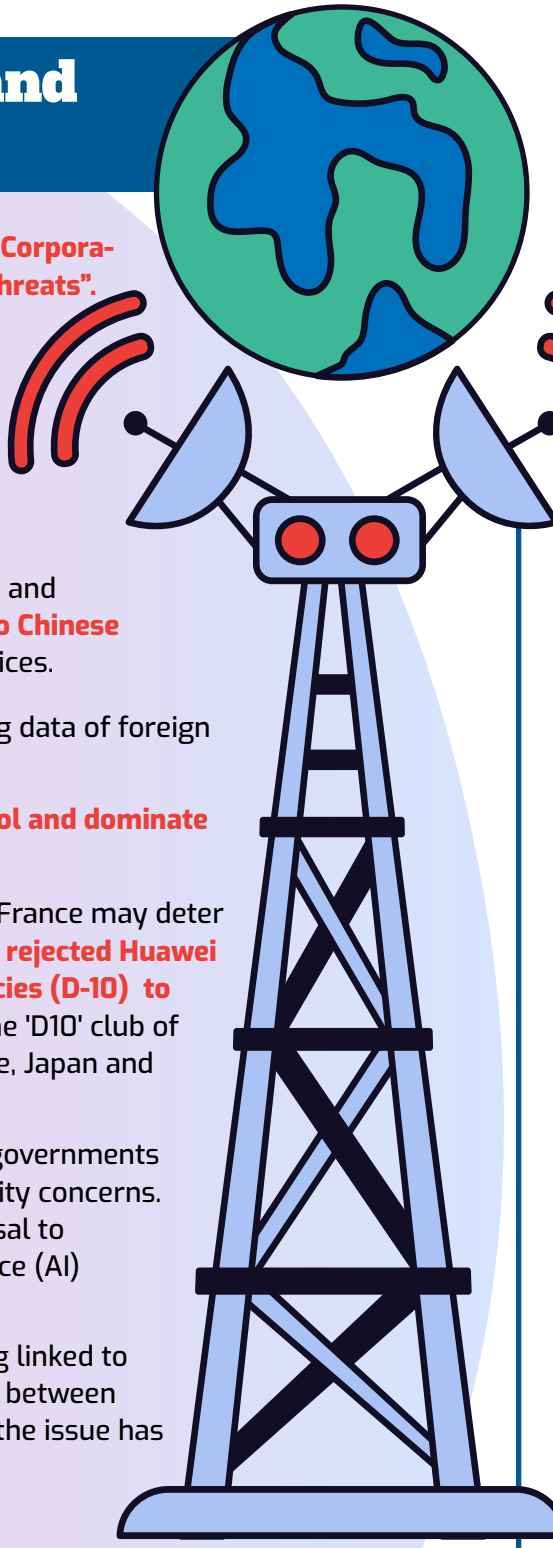
How adoption of 5G Technology could generate a cyber security challenge?

Wireless communication systems have always been prone to some security vulnerabilities. In the early 1980s, **1G networks** saw mobile phones being targeted **for illegal cloning and masquerading.** On early **2G networks, message spamming** was commonplace. With **3G and 4G networks, proliferation of smart devices** moved the threats faced by computer systems to wireless domain.

5G wireless networks will **connect over 7 trillion wireless devices** serving over 7 billion people, ushering a new era of security threats, which could arise in following forms:

- **Decentralized security needs:** Pre-5G networks had fewer hardware traffic points-of-contact, which made it easier to do security checks and upkeep. 5G's dynamic software-based systems have far more traffic routing points. To be completely secure, all of these need to be monitored. Since this might prove difficult, any unsecured areas might compromise other parts of network
- **Critical infrastructure protection:** 5G will enable real-time connectivity within critical infrastructure. Thus, any possible weakness in the network security can threaten security of this infrastructure and in turn may threaten our national security. For instance, **recent cyber-attacks** on Kudankulam Nuclear Power Project as well as on ISRO showcase our cyber vulnerabilities.
- **Many IoT devices are manufactured with a lack of security:** As more devices are encouraged to connect, billions of devices with varied security means billions of possible breach points thus increasing overall vulnerability of the system.
- **Network Switching:** Another security risk is posed by **the protocol designed to allow 4G or 3G connections when a dependable 5G signal isn't available.** When a 5G device switches to 3G or 4G, it is exposed to the vulnerabilities that haven't been addressed in the previous generations' protocol.
- **More bandwidth will strain current security monitoring:** While current networks are limited in speed and capacity, this has actually helped providers monitor security in real-time. So, the benefits of an expanded 5G network might actually hurt cyber security.

Huawei Case: 5G Technology and Global Geopolitics



Recently, US formally designated **Huawei Technologies Company and ZTE Corporation,** leading companies in 5G technology research, as **"national security threats".** (Huawei Technologies is a Chinese multinational company which designs, develops, and sells telecommunications equipment and consumer electronics such as Cables (OFC) and telecom towers necessary for 5G.)

There is an apprehension that Huawei Technologies may provide an inner system to enable **surveillance and cyber-espionage for China.** This apprehension is due to following reasons:

- Both Huawei and ZTE have close ties to the Chinese Communist Party and China's military apparatus, and both companies are **broadly subject to Chinese law obligating** them to cooperate with the country's intelligence services.
- They have been **accused of spying** for Chinese Government by sharing data of foreign citizens.
- The distrust has further multiplied because of **China's policy to control and dominate** various sectors through its software and hardware systems.

As a result, many **countries have become sceptical of them.** For instance, France may deter operators from using the Chinese telecom giant's equipment. Also, **UK has rejected Huawei** as a 5G partner, and said that it is now **forging an alliance of ten democracies (D-10) to create alternative suppliers for 5G** and other technologies from China. (The 'D10' club of democratic partners, **includes G7 countries** – UK, US, Italy, Germany, France, Japan and Canada – plus **Australia, South Korea and India.)**

In response to this allegation, **Huawei has criticized** the decision of these governments as political and based on **"ideological prejudices,"** rather than actual security concerns. Also, to counter a D-10 like geopolitical exclusion, China has made a proposal to create a 'BRICS innovation base' to take forward 5G and Artificial Intelligence (AI) cooperation among the five countries.

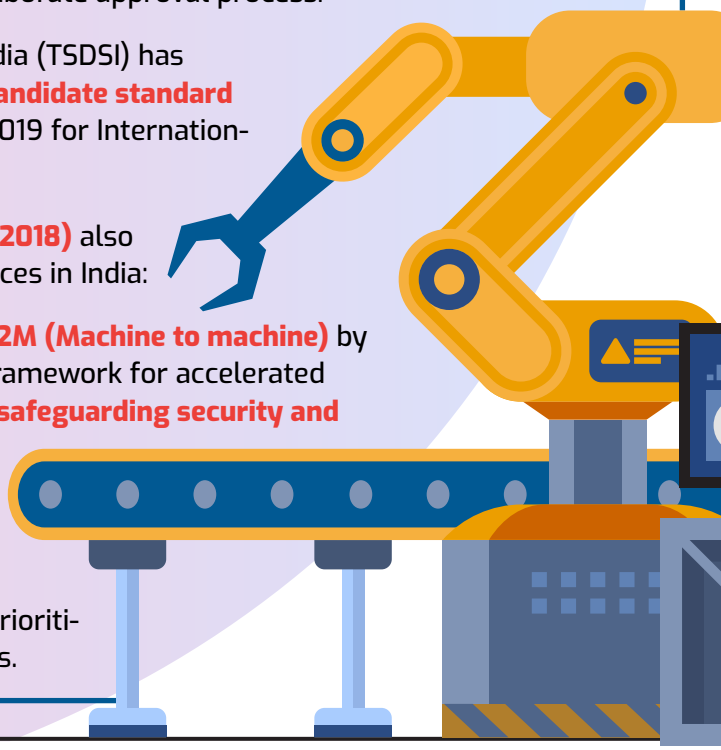
Since, there is no hard evidence against Huawei currently, the issue is being linked to the **ongoing trade war between US & China** and has thus sparked a debate between **free commerce and national security.** Taking another geoeconomics turn, the issue has the potential to set off a **technological arms race between US and China.**

India's Position in the debate

- The **Confederation of All India Traders (CAIT)** has asked to **ban Chinese companies Huawei and ZTE** from participating in 5G network roll-out in the country. It also urged that technology and equipment of both companies should be banned from use in 5G network rollout by any company.
- Apart from CAIT, other industry bodies such as the Telecom Equipment Manufacturers Association of India (TEMA) have also urged the Centre to use products made in India to provide telecom connectivity, especially to **border and sensitive areas in the country.**
- In the context of strained India-China ties, government has been **citing security and strategy related issues** and thus indicating towards exclusion of these firms from the 5G roll-out in India.

Steps already taken by Government to kick-start 5G

- A **5G High Level Forum** was set up by the Government in 2017 to **articulate the Vision for 5G in India** and to recommend policy initiatives and action plans to realize this vision.
  - It aims to achieve a globally-competitive product development and manufacturing ecosystem targeting 50% of India's market and 10% of global market over 5-7 years.
  - The forum has kept aside a corpus of Rs. 500 crore for R&D in 5G technology.
- **Cellular Operators Association of India (COAI)** has formed the **5G India Forum (5GIF)** that is expected to serve as a national initiative where all stakeholders, private and public, small and large, can meet and discuss the challenges of making 5G a reality in India, in conjunction with leaders of the rest of the world.
- To improve **testing capabilities:**
  - The Government has launched a program titled **'Building an End-to-End 5G Test Bed'.** The programme envisages close collaboration between the universities and startups and create an ecosystem that closely resembles a real-world 5G deployment.
  - The Department of Telecommunications (DoT) has simplified the testing method by making the **spectrum available for demonstration purposes.**
  - The **testing of 5G wireless products** can now be done only through a **self-declaration,** stakeholders can get the spectrum, and need not go through an elaborate approval process.
- Telecommunications Standards Development Society, India (TSDSI) has successfully introduced an **indigenously developed 5G candidate standard** at the International Telecommunications Union (ITU) in 2019 for International Mobile Telecommunication (IMT)-2020 ratification.
- The **National Digital Communication Policy-2018 (NDCP-2018)** also lays out the following objectives with respect to 5G services in India:
  - **Enabling Hi-speed internet, Internet of Things and M2M (Machine to machine)** by rollout of several 5G technologies. Also, developing framework for accelerated deployment of M2M services needs to be done while **safeguarding security and interception** for M2M devices.
  - **Enhancing the backhaul** capacity to support the development of next generation networks.
  - **Reviewing industry practices** with respect to traffic prioritization to provide 5G enabled applications and services.



Way Forward

5G technology has the potential for ushering a major socio-economic transformation in India by enabling a rapid expansion of the role of information technology across manufacturing, educational, healthcare, agricultural, financial and social sectors. But from the aforementioned discussion it is clear that it is not without challenges. To embrace that potential and overcome these challenges following steps could be taken:

Technology and Infrastructure provisions:

- **Core Technology and Manufacturing:** Building India's capacity in core technology development (Design and IP) and manufacturing for 5G and more broadly for all Information Technologies needs a deep and long- term effort.
- **Technology Demonstration and Major Trials:** 5G trials will be an important learning opportunity for our Telecom Service Providers (TSP), academia and industry. To enable this, major global **Original Equipment Manufacturers could be invited to conduct major 5G trials in India** in collaboration with local partners.
- **Securing data center and cloud components** becomes critical as mobile network components are virtualized and potentially deployed on virtualized software infrastructure. To cover these unique software related risks, network providers will need to collaborate with cyber security firms to **develop solutions for encryption, network monitoring, and more.**
- **Globally Harmonized Spectrum(GHS):** A GHS would enable economies of scale and facilitate cross-border coordination and roaming for end users which is a critical factor for the initial deployment of 5G.
  - Spectrum Harmonisation is a global effort under the auspices of the ITU to encourage governments and regulators to allocate RF spectrum consistently across borders, thereby enabling global roaming, interoperability and global markets for telecom equipment.
- **Backhaul infrastructure can be strengthened by adopting higher capacity density:** For 5G, the mobile networks would **need to be densified using small cells.** The compact size and low power (consumed and radiated) make small cells suitable for street level, lamp pole and indoor deployment.

Privacy provisions:

- **Creating a strong data protection policy and law** to provide a legal framework which supports adoption of 5G technology.
- Encapsulating a **privacy-by-design approach** that is service-oriented and privacy-preserving. It calls for privacy to be taken into account throughout the whole engineering process.
- **Data prioritization:** Mobile operators need to adopt a hybrid cloud-based approach where sensitive data is stored locally and less sensitive data stored in the cloud.
- **Using anonymity based techniques:** Messages should also be encrypted before it is sent to a location-based service provider. Also, obfuscation techniques – where the quality of location information is reduced – can also be used to protect location privacy.
- **Creating better authentication methodology:** As IoT gains momentum, more people will be able to remotely operate or "talk" to networked devices. There is a need, therefore, for a more stringent authentication method, e.g. biometrics, to prevent unauthorised access.

Security provisions:

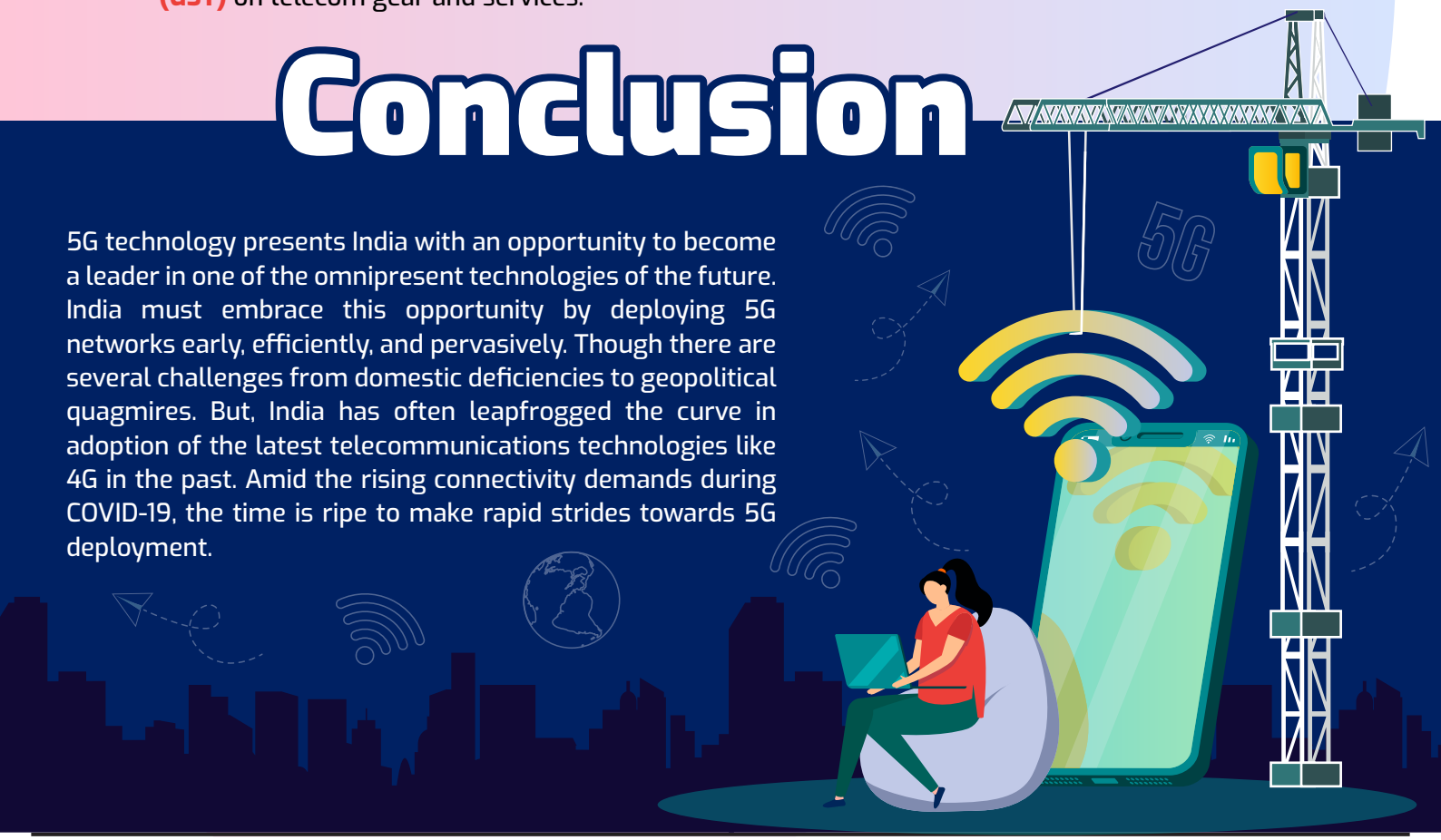
- **Providing End-to-end security solutions:** 5G Security must address multiple end-to-end operations such as IoT and devices, security operations, and network slicing security.
  - Network slicing is the ability of the network to automatically configure and run multiple logical networks as virtually independent business operations on a common physical infrastructure.
- **Centralized reporting to build trust:** This could be done by integrating 5G security systems with centralized reporting (integration) thus improving overall accountability of the system.
- **National Cyber Security Strategy (NCSS) of India: Government is planning to rollout NCSS** by upgrading **National Cyber Security Policy, 2013.** The policy could incorporate the cybersecurity issues faced by 5G technology, providing it a legal framework from security perspective.
- **Increasing consumer education on IoT cyber security:** User need to be taught various security protocols to ensure safe usage. For example, the importance of securing all internet devices with software updates, understanding the labelling standards for the IoT devices etc.

Policy provisions:

- **Spectrum Policy:** 5G spectrum can be allocated in multiple phases based on readiness of the various bands appropriately divided between wireless access, backhaul access and WiFI access.
- **Participation in International Standards:** Telecom networks need standards to ensure interoperability and to avoid market fragmentation. Getting active in **global standards development eco-system** will open up a new realm of opportunities for India.
- **Implementation and Oversight:** A **5G Implementation Oversight Committee** can be created with participation from Government, Academia, Industry and R&D Labs to supervise 5G program implementation.
- **Education and Awareness Promotion Program** like attracting global 5G conference events to India, setting up national 5G events and creating a comprehensive skills development program.
- **The Department of Telecommunication (DoT) has sought a reduction in the goods and services tax (GST)** on telecom gear and services.

Conclusion

5G technology presents India with an opportunity to become a leader in one of the omnipresent technologies of the future. India must embrace this opportunity by deploying 5G networks early, efficiently, and pervasively. Though there are several challenges from domestic deficiencies to geopolitical quagmires. But, India has often leapfrogged the curve in adoption of the latest telecommunications technologies like 4G in the past. Amid the rising connectivity demands during COVID-19, the time is ripe to make rapid strides towards 5G deployment.



TOPIC AT A GLANCE

5G Technology

- 5G is a **next generation mobile network technology** after 4G LTE networks.
- 5G technology is **not a single technology** but an amalgamation of various technologies.
- Major technologies used in 5G:
  - **mmWave (millimetre Wave):** 5G technology envisages to use frequencies up to 100GHz.
  - **Massive multi-user MIMO** (Multiple input multiple output) enabled network.
  - **Small cell stations** to connect the base stations and users seamlessly.
  - **NOMA (Non-Orthogonal Multiple Access)** allows multiple signals to use the same frequency channel.
  - **Mobile Edge Computing (MEC)** brings cloud computing closer to the user physically.

Potential use of 5G Technology

- **Enhanced Mobile Broadband:** High quality streaming, faster storage and access of cloud by businesses and better communication between public institutions and citizens.
- **Mission-critical communication:** Autonomous Vehicles, Augmented Reality (AR) and Virtual Reality (VR) and enhanced range and interactivity of drones.
- **Massive Internet of Things (IoT):** Smart City Infrastructure and Traffic Management, Industrial Automation, Wearables and Mobile devices and Precision agriculture.

Challenges in achieving this potential

Technological	Financial	Infrastructural
• Lack of spectrum availability. • Domestic electronic equipment manufacturing. • Testing challenges.	• Unavailability of high capital cost. • High tax burden on Telcos.	• Backhaul Infrastructure. • Memory and storage infrastructure. • Lack of uniform policy framework.

Cybersecurity challenges

- Requirement of decentralized security.
- Real time critical information protection.
- IoT devices lack requisite security.
- Issue related to Network Switching.
- Secure cloud computing.
- More bandwidth will strain current security.

Way Forward

Technology and infrastructure provisions	Privacy provisions	Security provisions	Policy provisions
• Building core technology and manufacturing capacity. • Technology demonstration and major trials. • Securing data center and cloud components. • Creating a Globally Harmonized Spectrum. • Building Backhaul, memory and storage infrastructure.	• Creating a strong data protection policy and law. • Local storage of sensitive data. • Using anonymity-based techniques. • Using Temporary Mobile Subscriber Identity (TMSI). • Creating better authentication methodology.	• Providing end-to-end security solutions. • Adopting centralized reporting to build trust. • Implementation of National Cyber Security strategy. • Increasing consumer education on cybersecurity and IoT.	• Adopting a clear spectrum policy. • Participation in developments of International Standards. • Creation of an implementation Oversight Committee. • Tax reduction for the Telecom Sector.