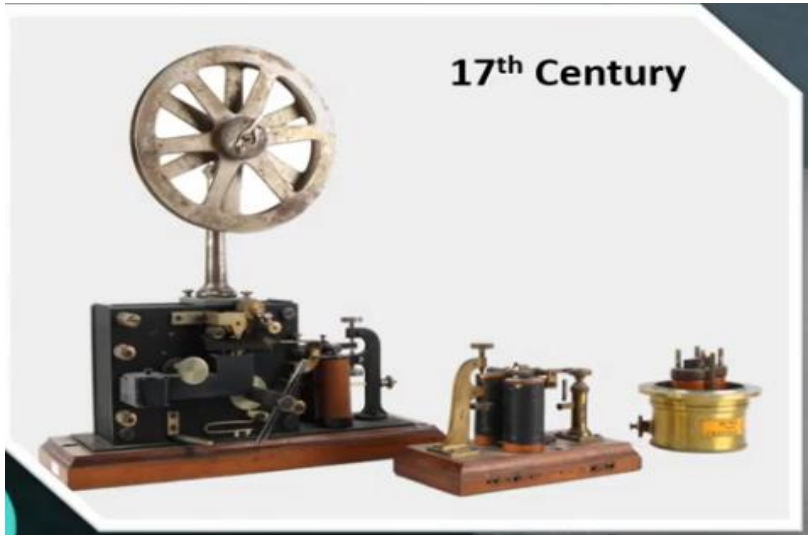
CREATING
# RISK INTELLIGENT PROFESSIONALS


GRMI | GLOBAL RISK MANAGEMENT INSTITUTE

## *Complex Security risk to 4G-5G Evolution | by Shubhangini Dwivedi (Batch 8)*

| PROGRAMME ENDORSED BY | ASSOCIATE PARTNER | STRATEGIC PARTNER | ASSOCIATE MEMBER | STRATEGIC PARTNER |
|---|---|---|---|---|
| othm qualifications | The Institute of Internal Auditors India | SHRM BETTER WORKPLACES BETTER WORLD | FICCI Federation of Indian Chambers of Commerce and Industry | HAUSPETER Consulting Internal Auditing Control |

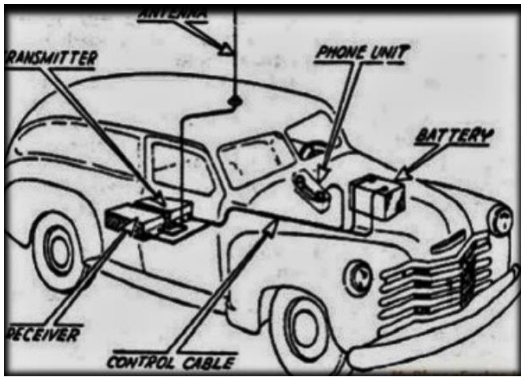




## History of Telephone and Wireless network Journey

Alexander Graham Bell invented and patented wired telephone in 1876 and even before that when telegraph was first used in 17 th century that the real journey started many years ago.

Moving from Wired telephone to wireless communication was a big revolution, this revolution was first called mobile radio telephone But when next wireless generations got created it was called Pre –cellular or 0G.

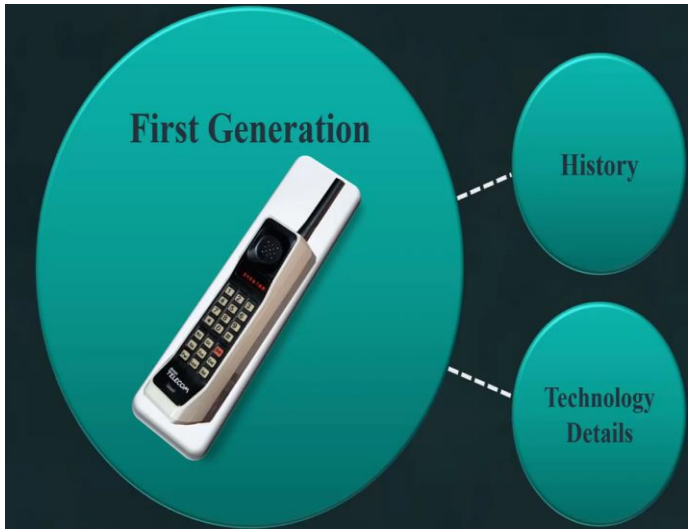




## Zero Generation Telecommunication (0G)

Technologies : used in 0G systems included :

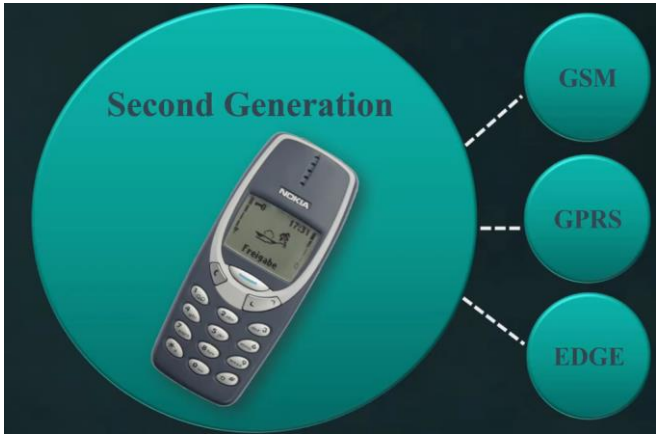
PTT (Push to Talk),
MTS (Mobile Telephone System),
IMTS (Improved Mobile Telephone Service),
AMTS (Advanced Mobile Telephone System). Since they were the predecessors of the first generation of cellular telephones, these systems are sometimes retroactively referred to as pre-cellular (or sometimes zero generation) systems.

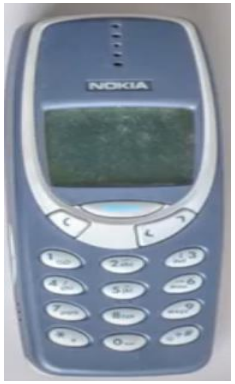
Mobile telephones systems were always usually vehicle mounted in the vehicle boot/trunk. The transceiver was mounted in the vehicle boot and usually placed to the head section, usually fixed close to the driver's seat.




# First Generation Telecommunication (1G)

First Experience of wireless telephone communication AMPS in USA Chicago 1983.
Analog Technology
Only Voice call, Call freely within a network.
Speed limit to 2.4kbps.
Data Transmission at 150 MHz.
Big Size Mobile phones
Battery Drainage issues.
Bad Voice quality.
Poor Encryption and security.
Crop Drops on mobility



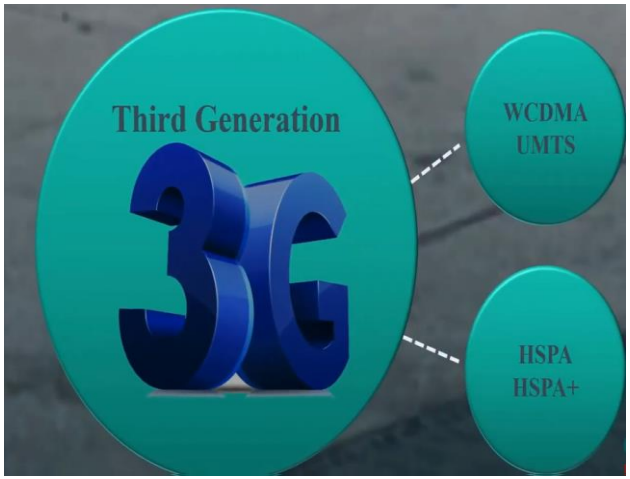




## Second Generation Telecommunication (2G)

GSM Launched In 1991 in Finland.
Digital Modulation- TDMA( Time division Multiple access)& CDMA( code division multiple access)-900 MHz.
Speed: 30-35 kbps
Voice call & SMS,Picture Msg-MMS, Simple internet browsing.
Smaller and More secureMobile Phones.
Provide better quality.

GPRS (2.5 G): Launched In 1993 by packet Switched Technpologies
Data Max Speed : 110 kbps
Introduced MMS: Multimedia Message service.
Supports IP to coonrect to internet

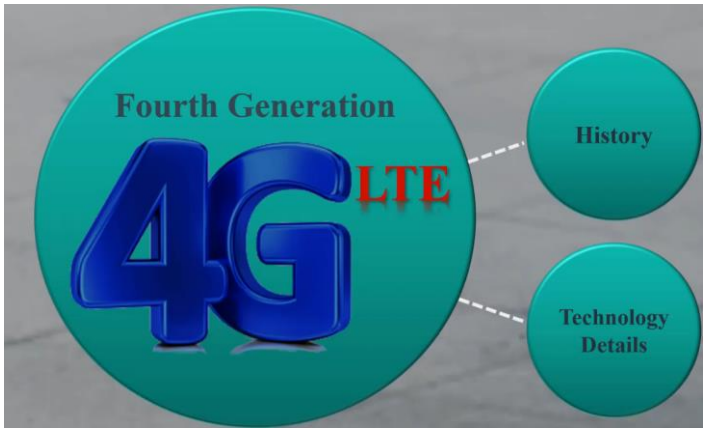
EDGE(2.75)
introduced in 2003 by at& T
Max speed 144 kbps .
8PSK encoding (symbol E).




# Third Generation Telecommunication (3G)

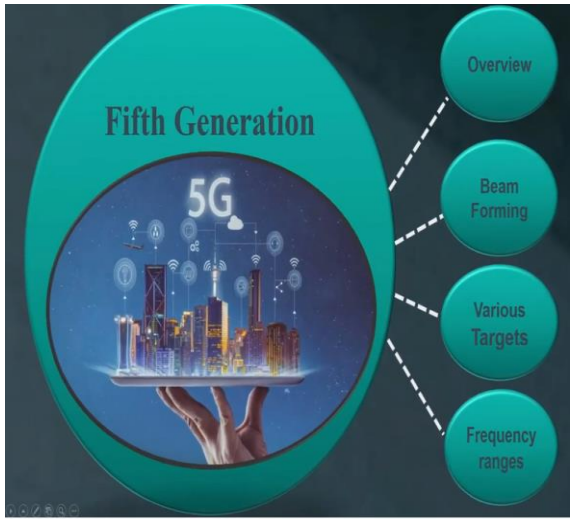
In 1998, **3G** was pre-commercially launched in Japan by NTT DoCoMo for testing;
October 2001, it was widely launched commercially on W-CDMA standard
Wcdma standard based on GSM and UMTS standard in Europe by 3GPP
Speed 384 Kbps-2Mbps
Video calling –mobile internet –streaming
Send/receive large emails and texts, provide fast web browsing, video streaming and more security amongst others. Conferencing call on the move, mobile TV, etc

HSPA3.5G & HSPA+ 3.75G
HSPA3.5G: ENHANCED WCDMA technology and symbol: H
whereas HSPA+3.75 Envolved HSPA-MIMO and symbol: H+




# Fourth Generation Telecommunication (4G)

In 2004 LTE standardization started by ITU
In 2005 LTE Specification was released
WiMax was first released commercially in June 2006 in South Korea
4G LTE(Long Term Evolution) was released commercially in December 2009 in the UK.
LTE is fully packet switched based on IP or internet protocol
For LTE download speed 100 Mbps.
LTE advanced download speed 1 Gbps
Frequency Bands: 700/800/900/1700/1800/1900/2100/2600 MHZ
High speed and low latency.
LTE supports such as IP telephone or voiceover IP,
3 D television support,
video conferencing with multiple participants,
easy and fast mobile web access,
hd mobile tv , online gamming and even cloud computing.,

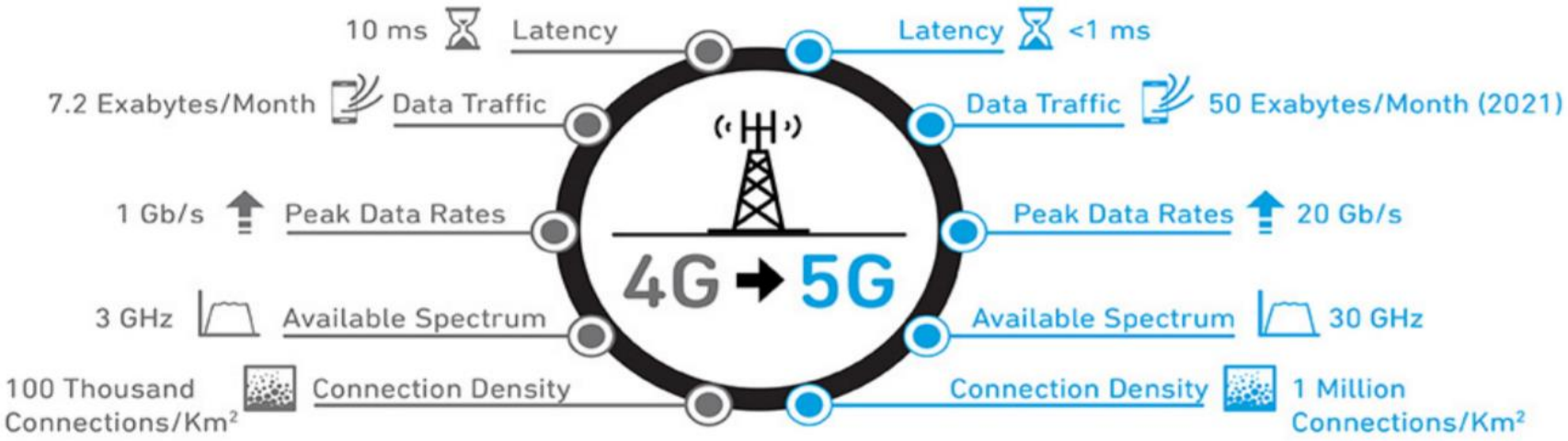



# Fifth Generation Telecommunication (5G)

what is 5G?

5G is the successor to 4G mobile network technology.
5G provides faster data rates, higher connection density, much lower latency etc Its the ability to connect to thousands of devices at once and blazing fast speeds that can move computing and processing power away from devices and into the network.
5G latency rate is at just 1 millisecond.
5G reaching 10 gigabits per second – up to 100 times faster than 4G .
5G networks to send and receive information quickly will help develop new services and devices, particularly connected cars and vehicle-to-vehicle information , remote surgical operations etc
it’s not just faster download speeds: 5G will be a game changer for many industries including hardware products and IoT solutions. Multiple users might transfer huge data within seconds.

## Comparing 4G and 5G



# Why do we need 5G?


Ultra HD movies can be downloaded in seconds.

5G will enable an interconnection of 20.8 billion devices from door locks to cars to refrigerators.

Machine to Machine Communi-cation will be enabled.

Backbone in buiding up Smart Cities with an IoT infrastructure.

5G will promote ulta low latency which means that a spectator in a cricket stadium can watch a live stream of an alternate camera angle of the action that matches what is going in the pitch ahead with no perceivable delay.

## Security Risk Of 5G

5G opens up more opportunities in areas such as healthcare, manufacturing and transport, the reality is that it is becoming an increasingly attractive target for cyber criminals, its increases the available threat surface.
5G cybersecurity needs some significant improvements to avoid growing risks of hacking. Some of the security worries result from the network itself, while others involve the devices connecting to 5G. But both aspects put consumers, governments, and businesses at risk.

**Decentralized security .** Pre-5G networks had less 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 the network.

**More bandwidth will strain current security monitoring .** While existing networks are limited in speed and capacity, this has helped providers monitor security in real-time. So, the benefits of an expanded 5G network might hurt cybersecurity. The added speed and volume will challenge security teams to create new methods for stopping threats.
5G is potentially so susceptible for cyberattacks because of its possibilities and flexibility. Everything is managed by software and so that in itself has a security risk.  Bllions of devices will be connected to 5G networks

## Cybersecurity vulnerabilities can take form in a wide variety of attacks.

**Mobile Malware Attacks Targeting User Equipment:** The Future User Equipmentthe will be exposed to more sophisticated attacks originated from mobile malware and target both the UE and the 5G cellular network. The open operating systems will allow end-users to install applications on their devices. Consequently, mobile malware, which will be included in applications will be downloaded and installed on end-user's mobile device exposing them to many threats. Mobile malware can be designed to enable attackers to exploit the stored personal data on the device or to launch attacksagainst other entities.

**Mobile Botnets Attack**: In 5G communication environment, mobile botnets are expected to be increasingly used by attackers, since future mobile devices will be ideal remote controlled machines due to their specific features . In particular, 5G mobile devices will support different connectivity options and increased uplink bandwidth, and will tend to be always turned on and connected to the Internet. Thus, future attackers will be enabled to deploy mobile botnets for 5G communication networks in many efficient ways .

# Increased usage & IoT-related 5G risks

**If the implementation and use of 5G lead to a greater number of connections and a larger amount of data being transferred, it follows that the attack surface area will increase alongside it. Greater use simply brings more opportunities for hackers to find a way in.The increased usage that will come along with 5G will only serve to sharpen this.**

**5G speeds and capacities associated will make IoT devices far more practical for a range of new tasks and will also increase the attack surface area, by introducing a host of new endpoints. This is worrying many because Iot devices have poor security, especially those that come from cheaper and less-reputable manufacturers.**

# Radio jamming & related attacks

Radio jamming is a significant worry **because attackers can block access to network service in an area**. Spoofing is another key threat because **adversaries can use it to impersonate other parties**. Sniffing is also a concern because **it allows attackers to view the contents of data transmissions, which can violate privacy and lead to other attacks.**. The most worrying areas involve the Primary Synchronization Signal (PSS) and the Physical Broadcast Channel (PBCH) because these are susceptible to attacks that are efficient and have a low level of complexity..

When the PBCH is jammed, end users can't access the information they need to make connections to the base station. This lack of information stops new devices from accessing base stations, therefore preventing them from being able to make calls or send messages.

# How You Should Prepare for 5G?

**Install an anti-virus solution on all your devices.** Antiviruses will help prevent your devices from becoming infected.

**Use a VPN** to stop strangers from accessing your data without permission and spying on your online activity.

**Practice strong password security.** Always use passwords when available and make them incredibly strong. Long strings of random characters are considered the best passwords possible. Make sure you include uppercase, lowercase, symbols, and number as well.

**Update the default backend passwords on all your IoT devices.** Follow your device's instructions on updating the "admin/password" style credentials of your gadgets. To find this information, consult with your manufacturer's tech manuals or contact them directly.

**Keep all your IoT devices updated with security patches.** This includes your mobile phone, computers, all smart home devices, and even your car's infotainment system. Remember, any device that connects to the internet, Bluetooth, or other data radio should have all the latest updates (apps, firmware, OS, etc.)

# REFERENCES


https://mse238blog.stanford.edu/2017/07/ssound/1g-2g-5g-the-evolution-of-the-gs/
https://www.avnet.com/wps/portal/abacus/resources/article/the-evolution-of-cellular-networks/
https://www.linkedin.com/pulse/mobile-wireless-communication-technology-journey-0g-mutabaz
https://www.kaspersky.com/resource-center/threats/5g-pros-and-cons
http://net-informations.com/q/diff/generations.html
https://www.5gradar.com/features/5g-security-5g-networks-contain-security-flaws-from-day-one
https://www.comparitech.com/blog/information-security/5g-security-risks/
https://www.helpnetsecurity.com/2019/12/02/5g-iot-security/

**Campus Address** :

88, Sector 44,
Gurgaon – 122002

**CONTACT US**

www.grm.institute

Email :
admissions@grm.institute

Thank you!