



Cyber Security Concerns in 5G Networks

presented by

Pradip Kumar Sharma
Email: pradip@seoultech.ac.kr



Outline

01 Introduction of 5G Networks

- What is 5G?
- Why do we need 5G?
- Key Challenges and Gap to Reach 5G

02 5G Network Architecture

- Abstract Overview of 5G Network Architecture
- Major Components in 5G Network
- 5G Service-based Architecture

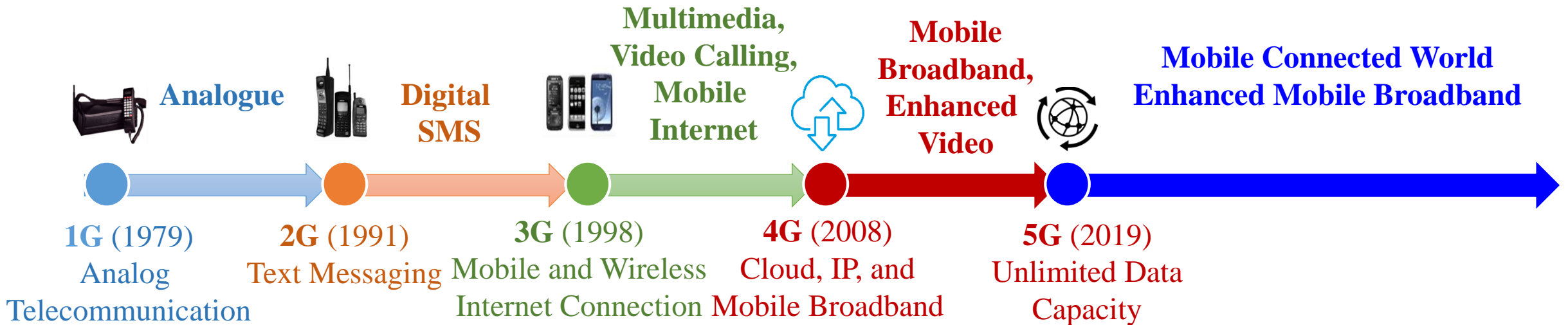
03 Cyber Security Concerns

04 Summary

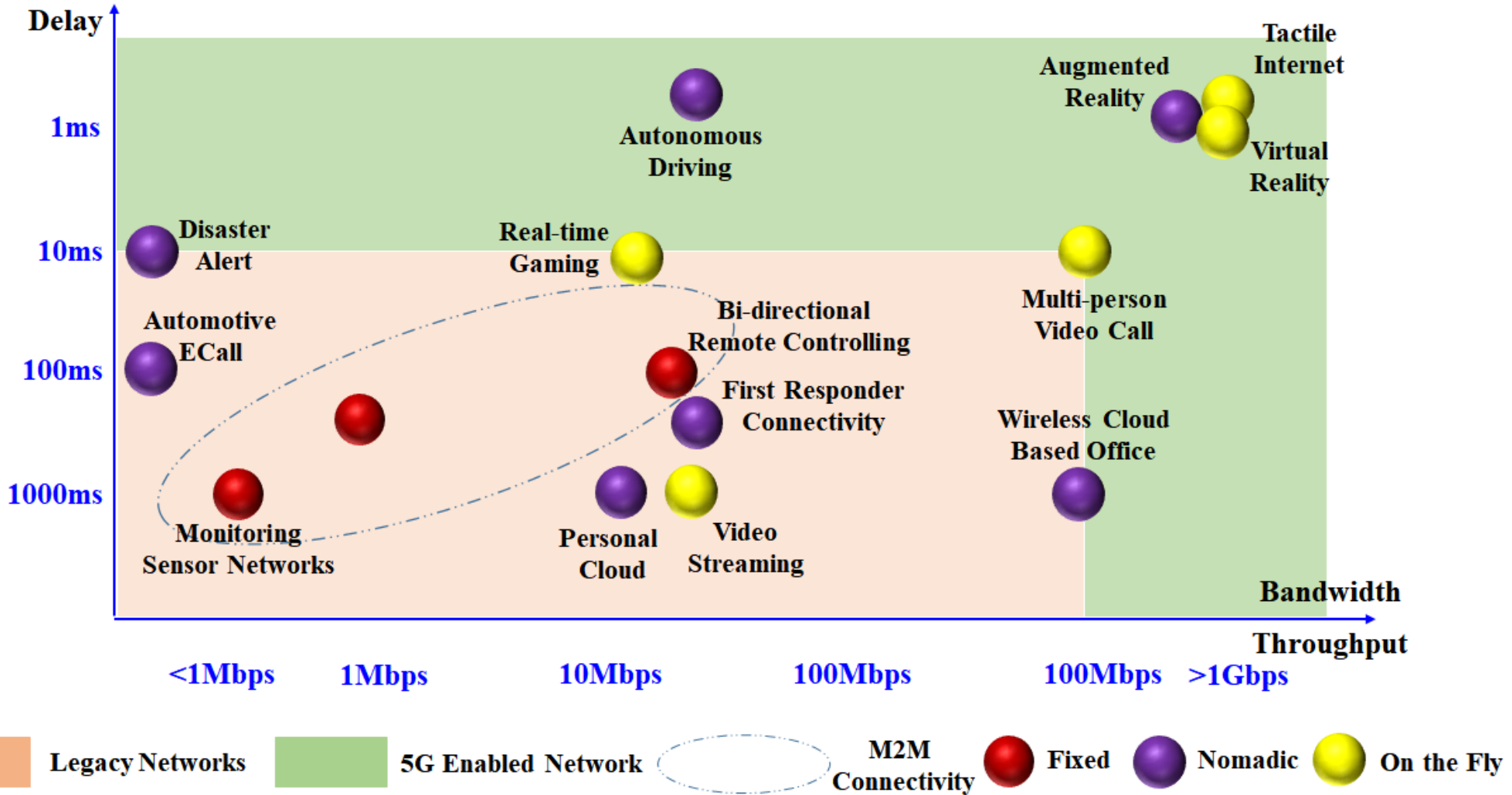
What is 5G?

5G is the 5th generation of mobile networks

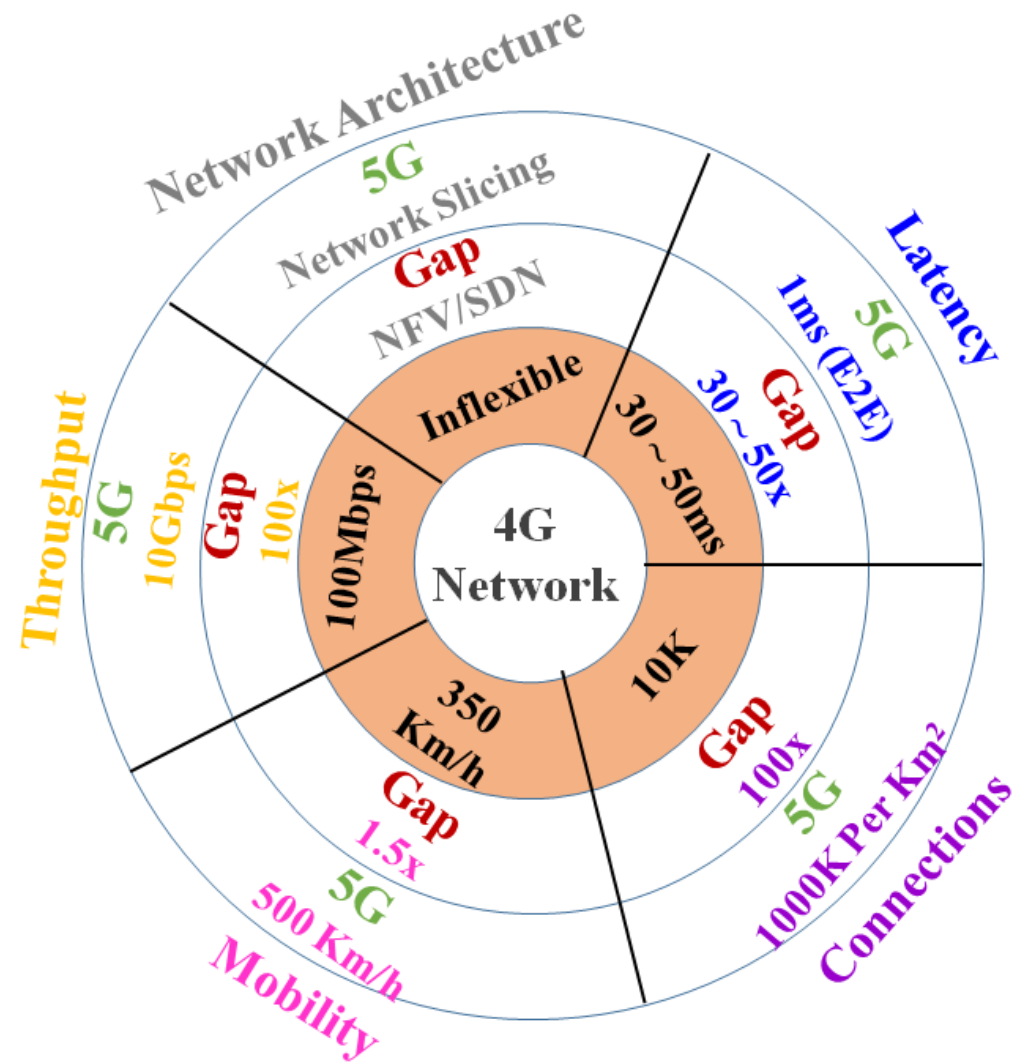
- ❑ Operation from **quite low to very high** bands: 0.4 – 100 Ghz
 - Including stand-alone operation in unlicensed bands
- ❑ **10 times** more capacity than others
- ❑ Expected speed up to **10 Gbps**
- ❑ **Hundred times** faster than the current 4G technology (theoretical)
- ❑ **Lower cost** than previous



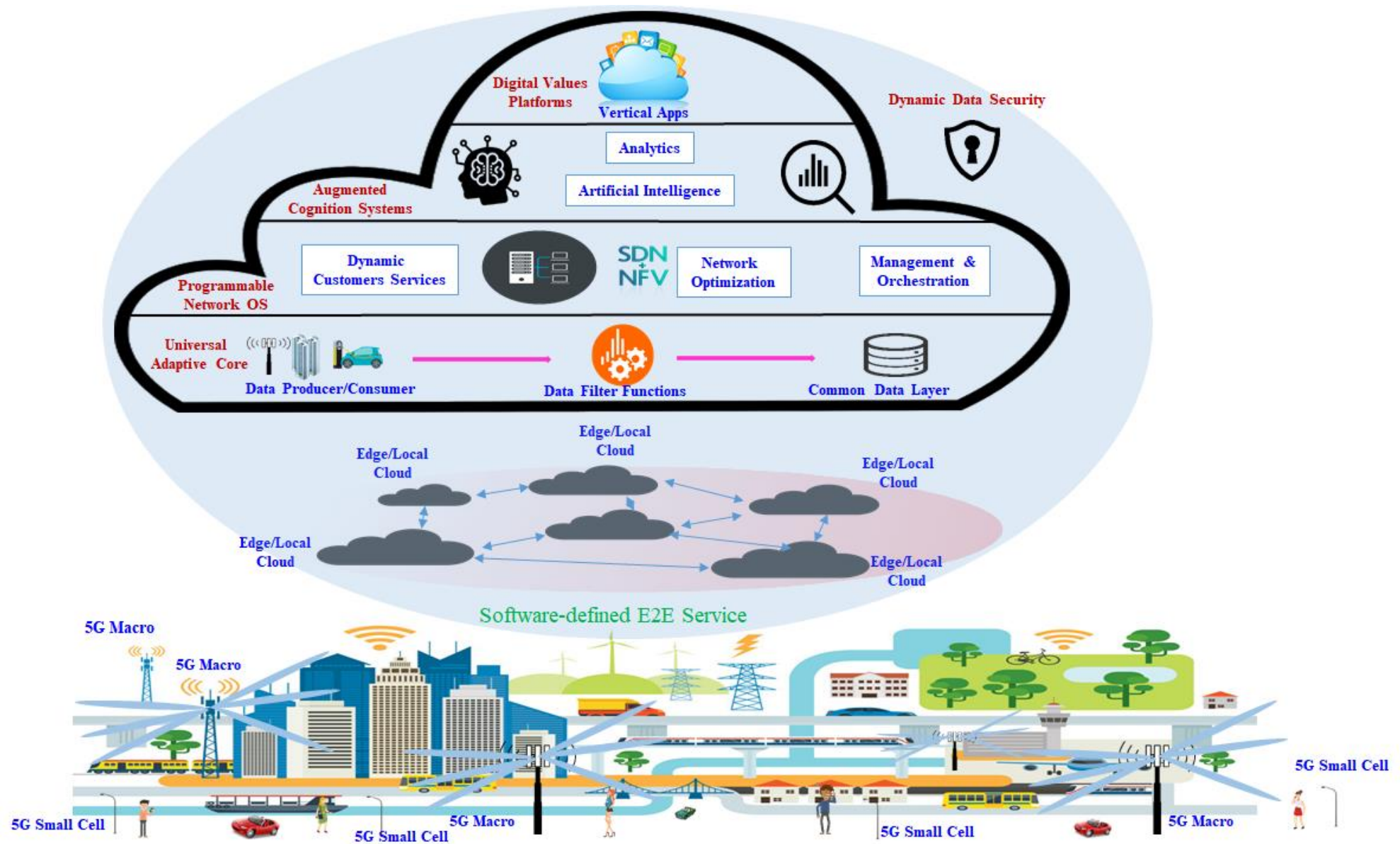
Why do we need 5G?



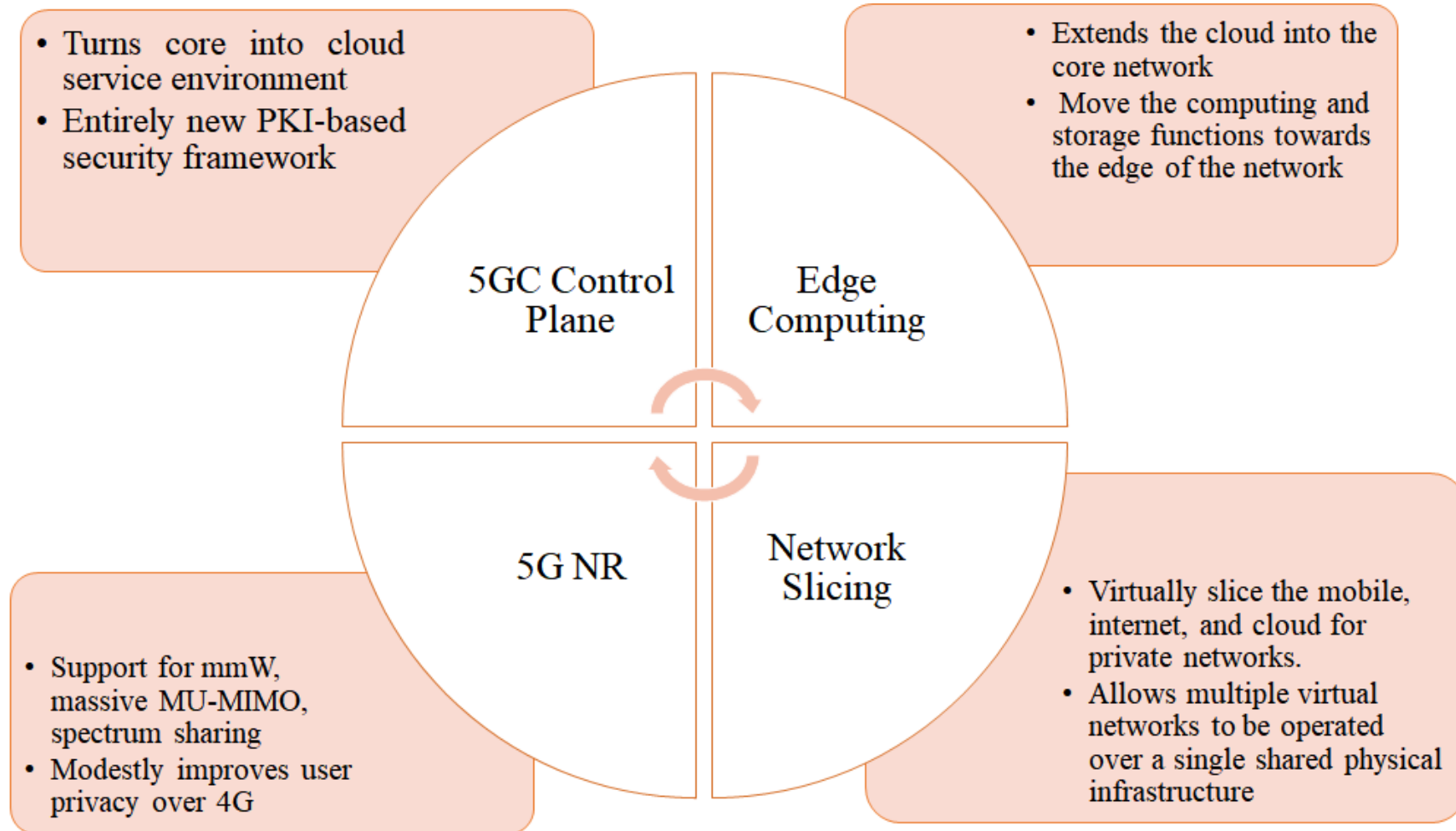
Key Challenges and Gaps to Reach 5G



Abstract Overview of 5G Network Architecture



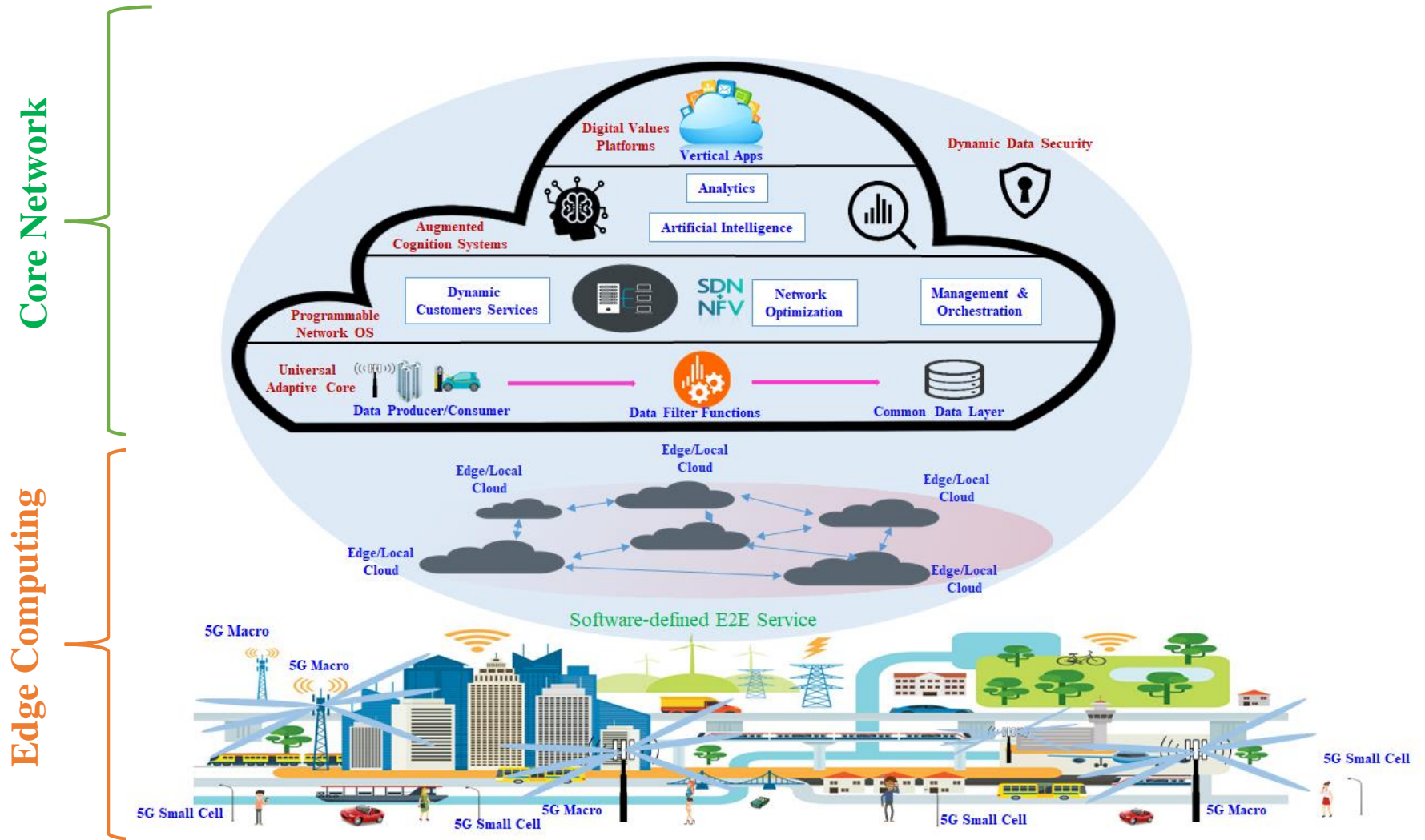
Major Components in 5G Network



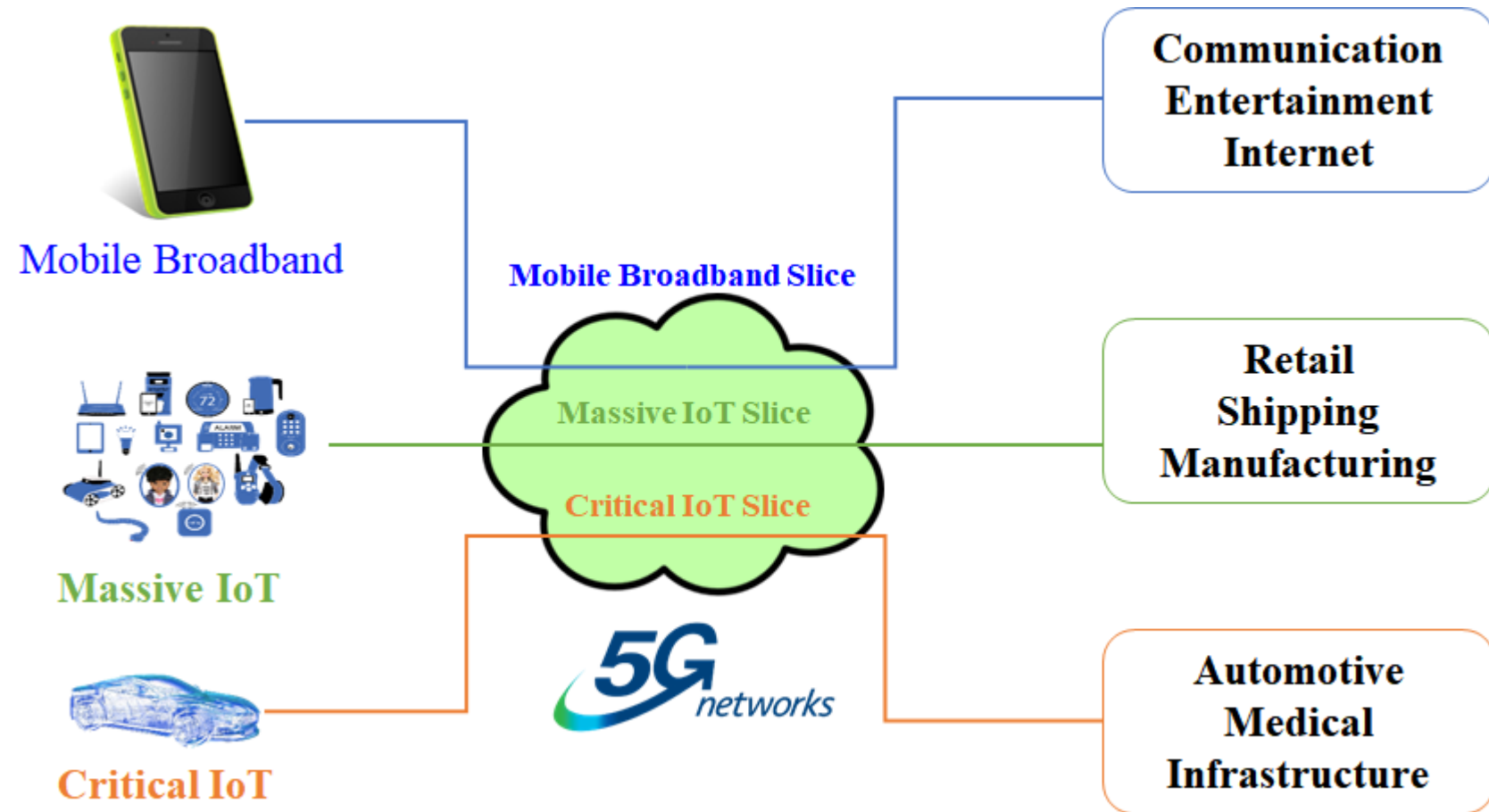
Major Components in 5G Network – Edge Computing

Edge Computing

- ❑ Brings the **data** closer to the end-user,
 - Move the **computing and storage** functions towards the edge of the network.
- ❑ **Reduces latency** and the **data volume** handled by the core network
- ❑ Enhance the performance benefits.



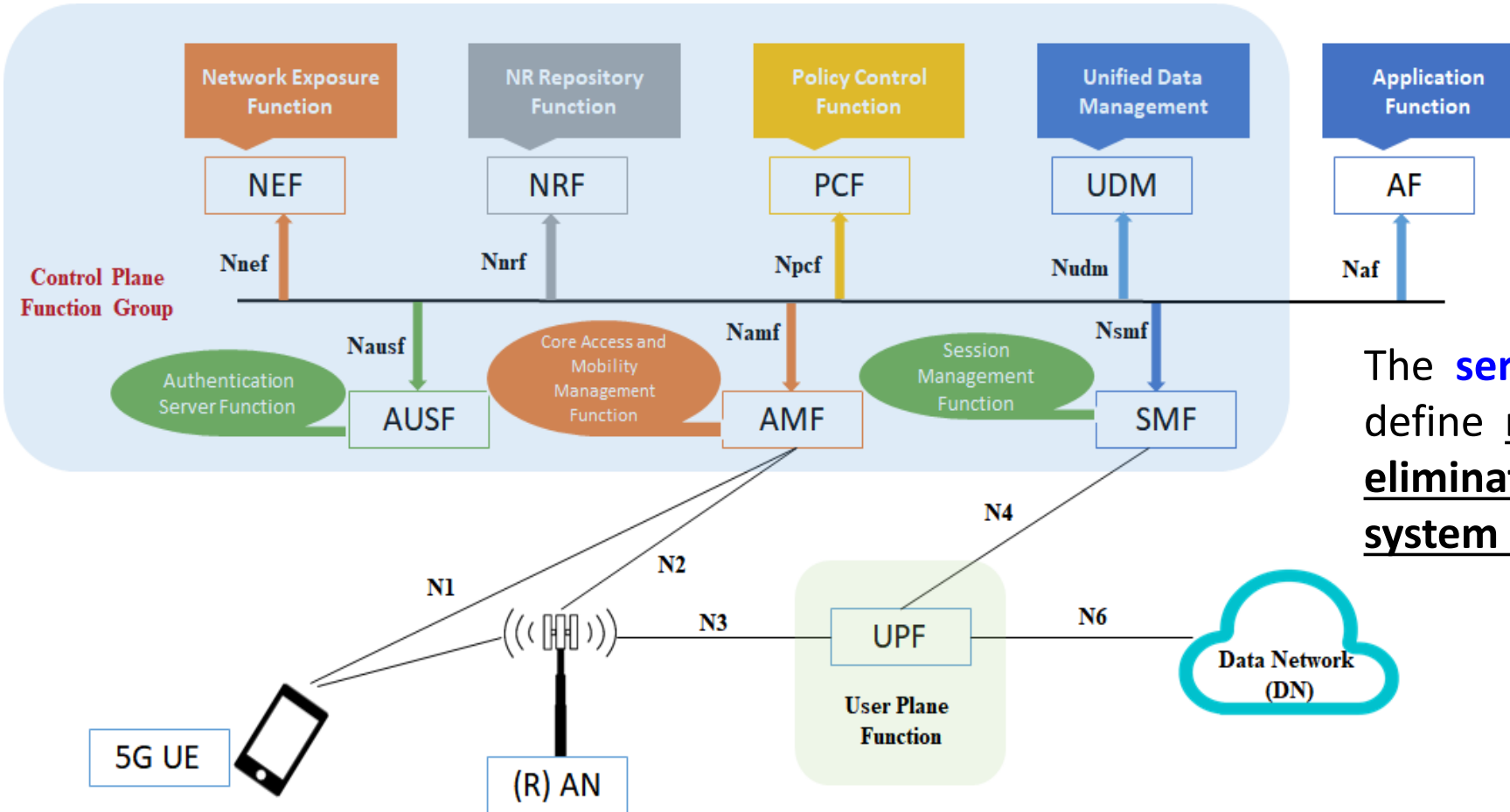
Major Components in 5G Network – Network Slicing



Network Slicing

- ❑ Network slicing spans multiple layers of the network.
- ❑ It enables service providers to build end-to-end virtual networks tailored to application requirements.

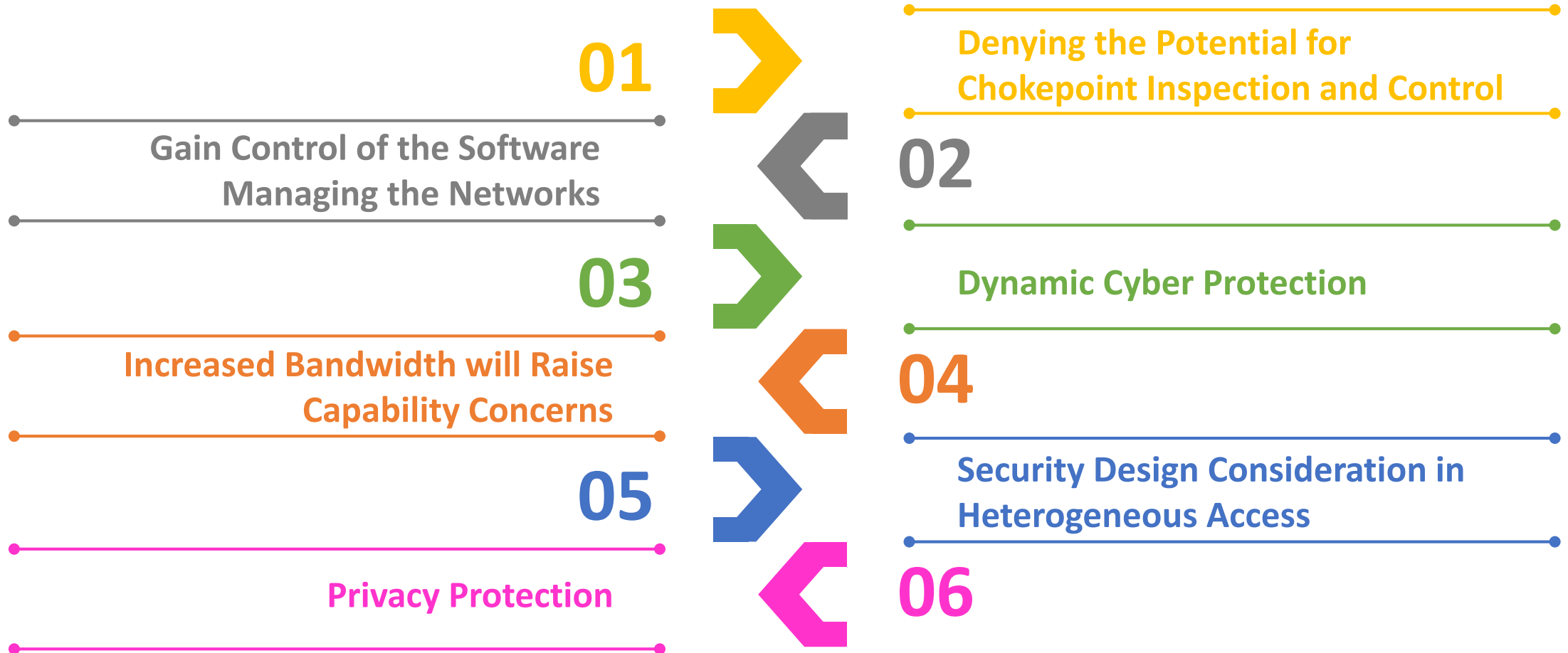
5G Service-based Architecture



The **service-based architecture** helps to define modular components, effectively eliminating large data pipes, and reducing system complexity.

Cyber Security Concerns

Cyber Security Concernes in 5G Network will be:

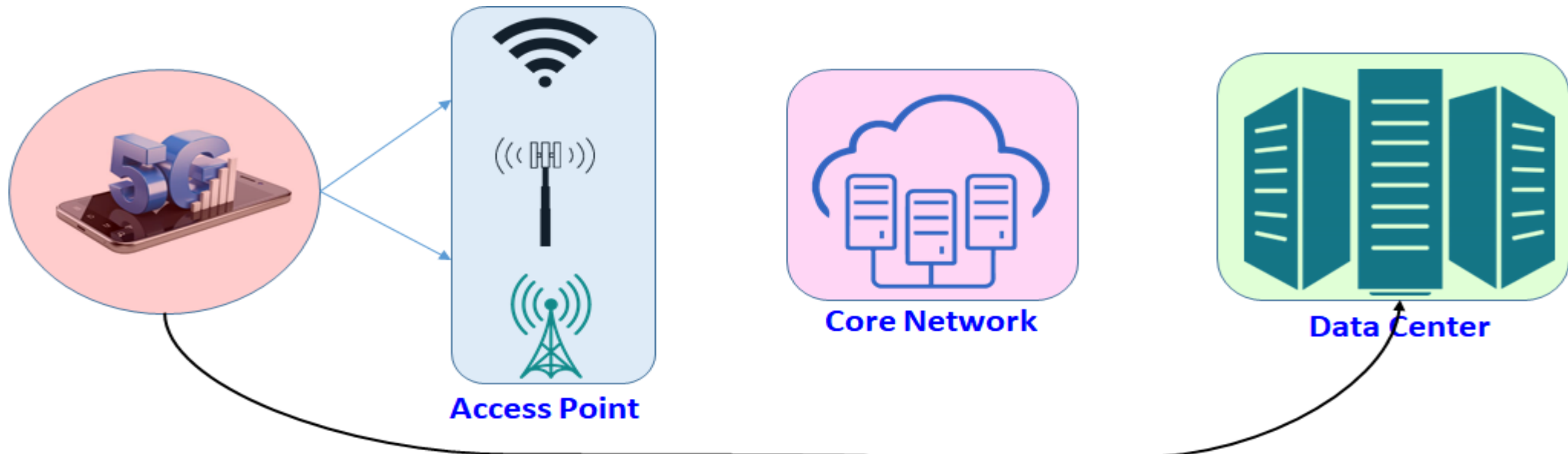


01



Denying the Potential for Chokepoint Inspection and Control

- ❑ Legacy networks have hub-and-spoke designs
 - Everything come to hardware choke points where cyber hygiene could be practiced.
- ❑ In 5G software defined network,
 - Activity is pushed outward to a web of digital routers throughout the network

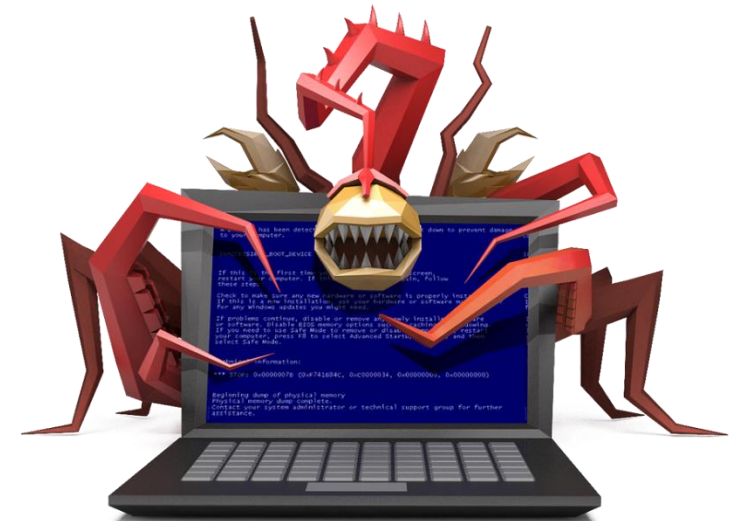


02



Gain Control of the Software Managing the Networks

- ❑ It is possible to lock down the software vulnerabilities within the network
- ❑ But, the network is also being managed by software
- ❑ An attacker that gains control of the software managing the networks can also control the network.

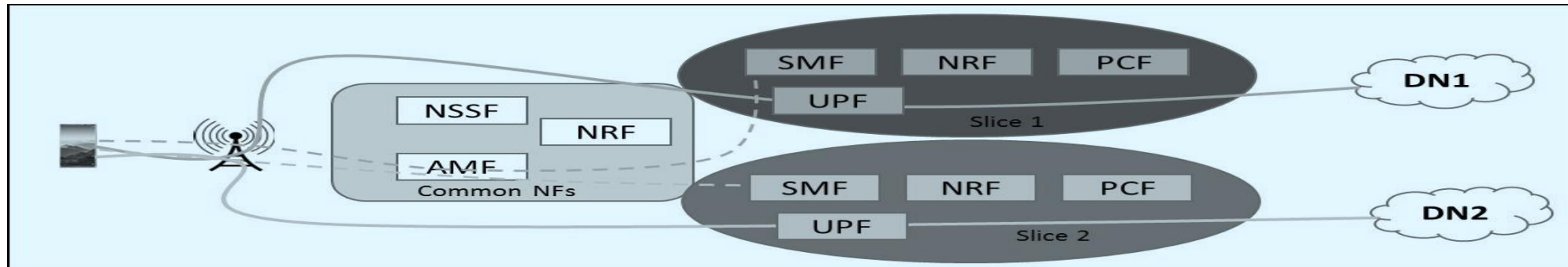


03



Dynamic Cyber Protection

- ❑ The dramatic expansion of bandwidth that makes 5G possible creates additional avenues of attack.
- ❑ 5G's Dynamic Spectrum Sharing capability in which multiple streams of information share the bandwidth in so-called "slices"
 - Each slice with its own varying degree of cyber risk.
- ❑ When software allows the functions of the network to shift dynamically
 - Cyber protection must also be dynamic rather than relying on a uniform lowest common denominator solution





Increased Bandwidth will Raise Capability Concerns

- ❑ Many security solutions involve monitoring traffic in real time to identify potential threats based on activity and sniffed data.
 - These systems are largely able to keep up because of bandwidth limitations.
 - The Internet bandwidth or capacity of a network can only handle so much traffic at once.
 - This is bad in terms of user performance but good in terms of managing security and traffic.

- ❑ With 5G, which offers incredibly higher speeds and capacity, all of that goes out the window
 - Security solutions must be upgraded to deal with these new capabilities
 - A majority of legacy solutions may no longer work
 - Because of the increased capacity, speeds, and overall latency boost that 5G offers.
 - To achieve the higher capabilities, hardware will need to be upgraded to become more powerful



05

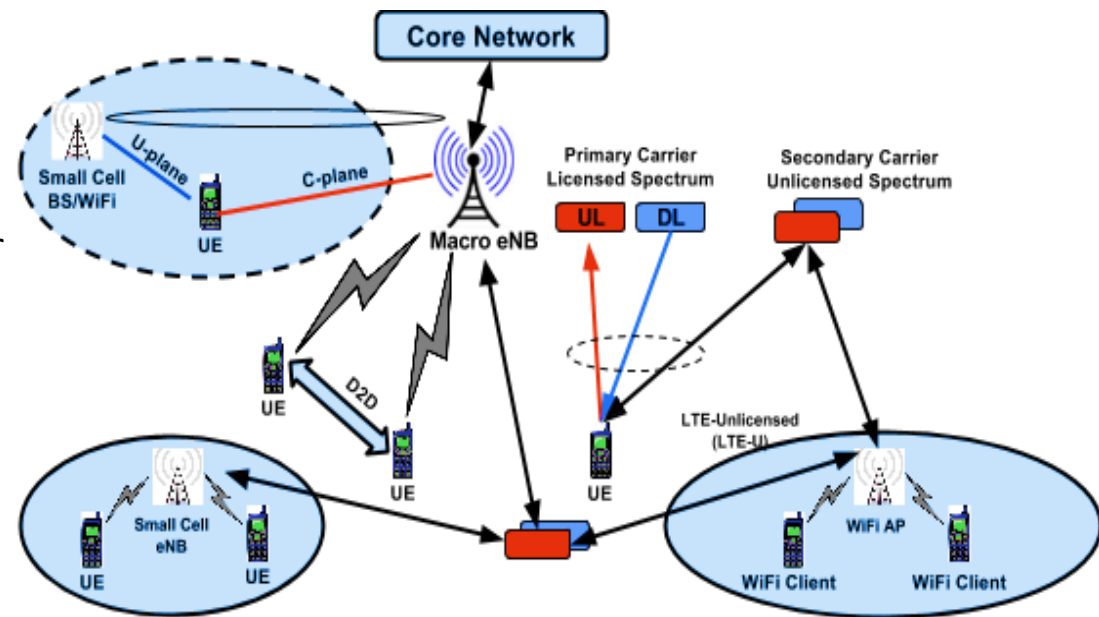


Security Design Consideration in Heterogeneous Access

- ❑ The heterogeneous nature comes not only from the use of different access technologies (WiFi and LTE),
 - But also from multi-network environment, which might imply that the access network architecture from different networks are different.

- ❑ IoT devices have many choices in the way they access networks.
 - For instance, they may connect to networks directly, or via a gateway, or in the D2D or Relay fashion.

- ❑ Comparing to mobile handset, security management of IoT device in 5G may be efficient and lightweight.





- ❑ As primary method for network accessing, mobile networks carries data and signaling that contains many personal privacy information
 - For instance, identity, position, and private content.

- ❑ In order to offer differentiated quality of service, networks may need to sense what type of service a user is using.
 - The service type sensing may involve user privacy.

- ❑ As open network platforms, 5G networks raise serious concerns on privacy leakage. In these cases, privacy leakage can cause serious consequences.



Summary

- ❑ Advanced 5G and wireless networks introduces a slew of cybersecurity concerns and problems,
 - Particularly as it relates to current security solutions.
- ❑ Cyber security requirements are often seen as obstacles or burden in the system design
 - But ignoring them in the beginning is not cost-efficient in the long run.
 - Adding features afterwards is less effective and often more costly than including proper mechanisms from the beginning.
- ❑ Organizations must recognize and be held responsible for a new cyber duty of care.
- ❑ Government must establish a new cyber regulatory paradigm to reflect the new realities.