

Beyond the Hype: 5G and What You Need to Know

Lauren Cooper

Cybersecurity Engineer

lacooper@cert.org

Software Engineering Institute
Carnegie Mellon University
Pittsburgh, PA 15213

Copyright 2020 Carnegie Mellon University.

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center.

The view, opinions, and/or findings contained in this material are those of the author(s) and should not be construed as an official Government position, policy, or decision, unless designated by other documentation.

References herein to any specific commercial product, process, or service by trade name, trade mark, manufacturer, or otherwise, does not necessarily constitute or imply its endorsement, recommendation, or favoring by Carnegie Mellon University or its Software Engineering Institute.

NO WARRANTY. THIS CARNEGIE MELLON UNIVERSITY AND SOFTWARE ENGINEERING INSTITUTE MATERIAL IS FURNISHED ON AN "AS-IS" BASIS. CARNEGIE MELLON UNIVERSITY MAKES NO WARRANTIES OF ANY KIND, EITHER EXPRESSED OR IMPLIED, AS TO ANY MATTER INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR PURPOSE OR MERCHANTABILITY, EXCLUSIVITY, OR RESULTS OBTAINED FROM USE OF THE MATERIAL. CARNEGIE MELLON UNIVERSITY DOES NOT MAKE ANY WARRANTY OF ANY KIND WITH RESPECT TO FREEDOM FROM PATENT, TRADEMARK, OR COPYRIGHT INFRINGEMENT.

[DISTRIBUTION STATEMENT A] This material has been approved for public release and unlimited distribution. Please see Copyright notice for non-US Government use and distribution.

This material may be reproduced in its entirety, without modification, and freely distributed in written or electronic form without requesting formal permission. Permission is required for any other use. Requests for permission should be directed to the Software Engineering Institute at permission@sei.cmu.edu.

Carnegie Mellon® and CERT® are registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

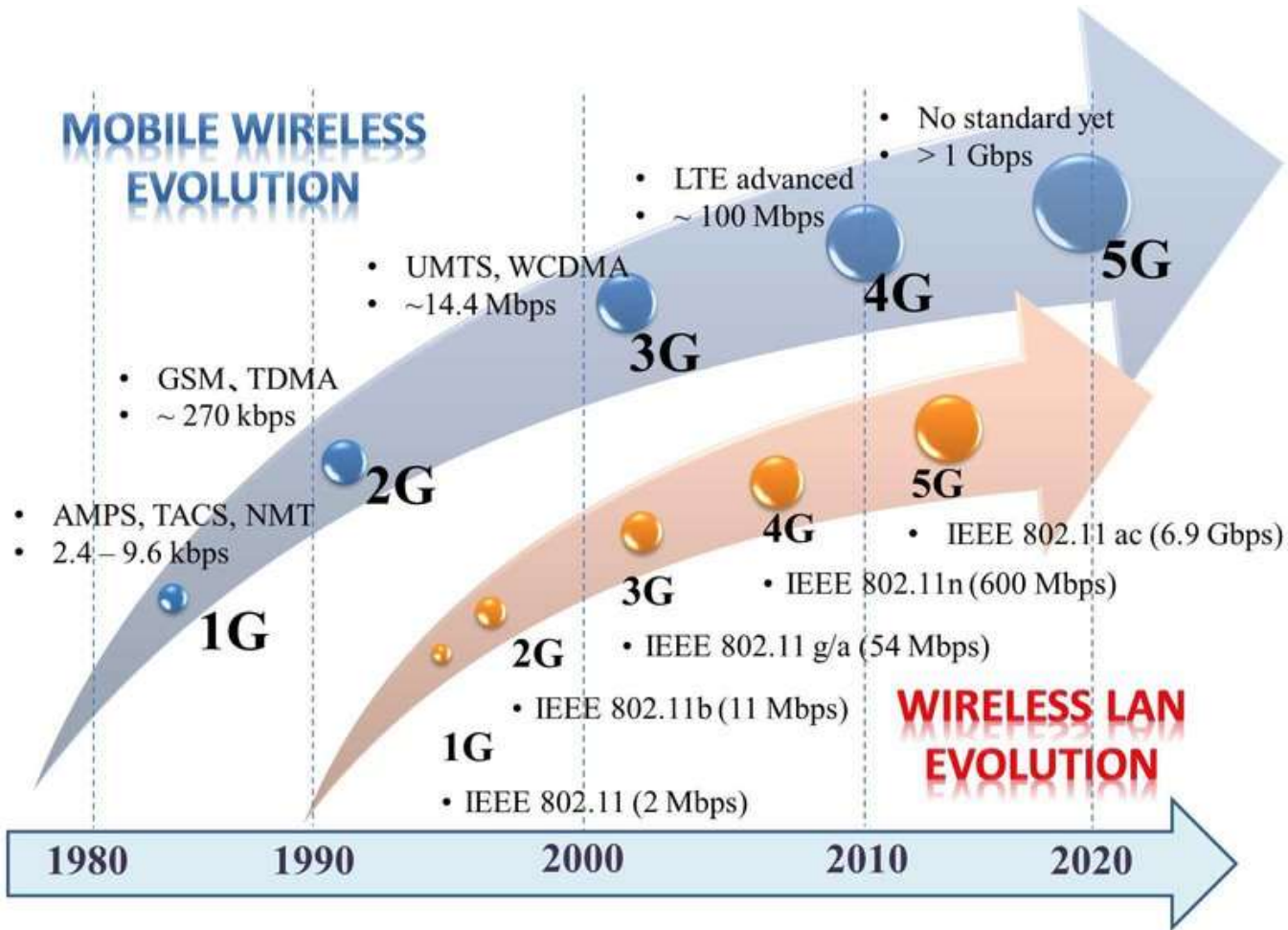
DM20-1003

Agenda

- Introduction – What is 5G?
- Spectrum & Engineering
- 5G in Practice
 - Use Cases
 - Enabling Technologies
- Security

Introduction – What is 5G?

Brief History of Mobile Standards



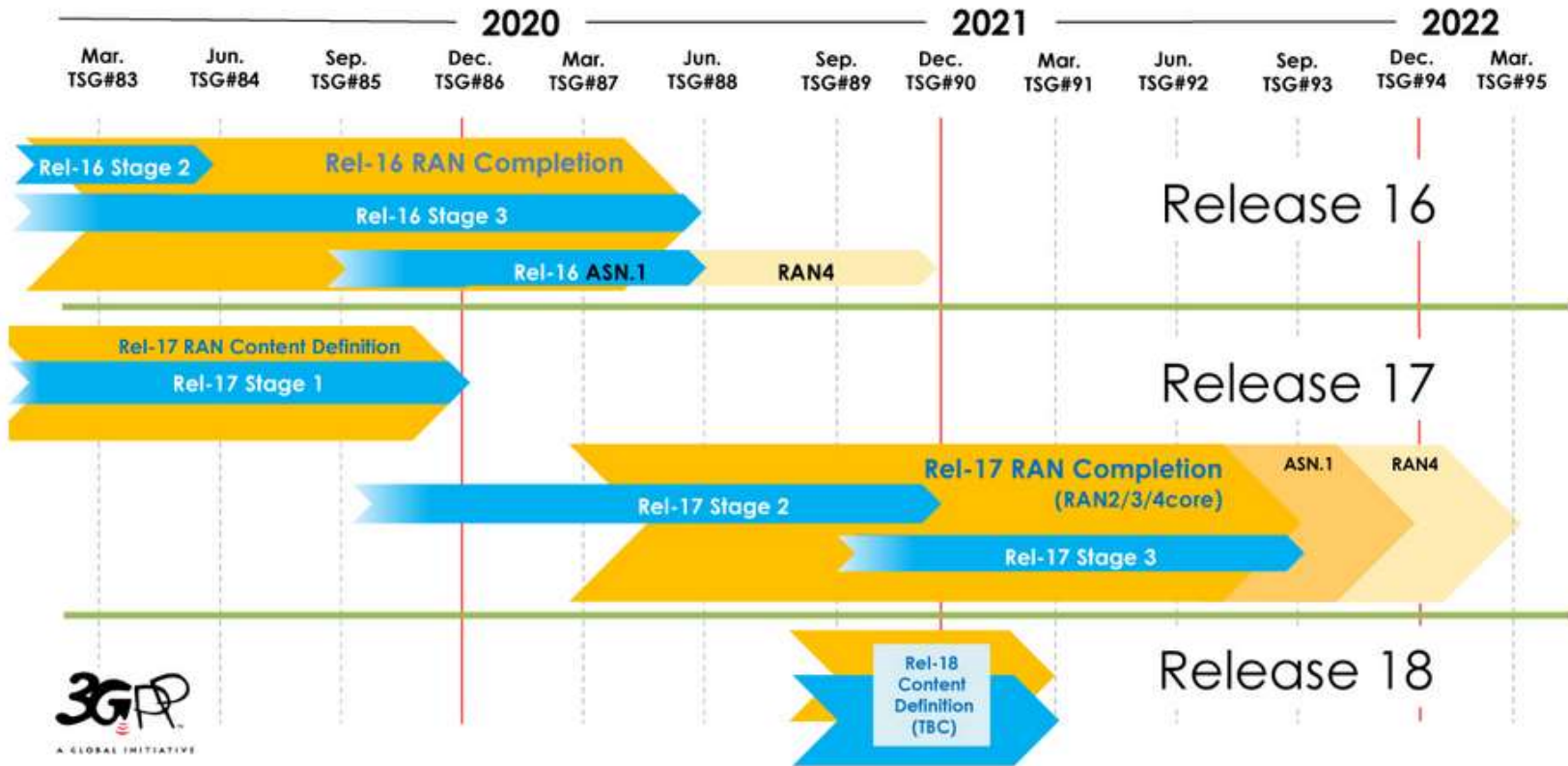
https://www.researchgate.net/figure/Wireless-technology-evolution_fig1_322584266

Who Develops 5G Standards?

- 3GPP
 - Primary standards development body
 - Cooperative, collaborative, and multinational effort
- Other standards contributors:
 - 5G Americas
 - IEEE
 - ITU



Standards Timeline



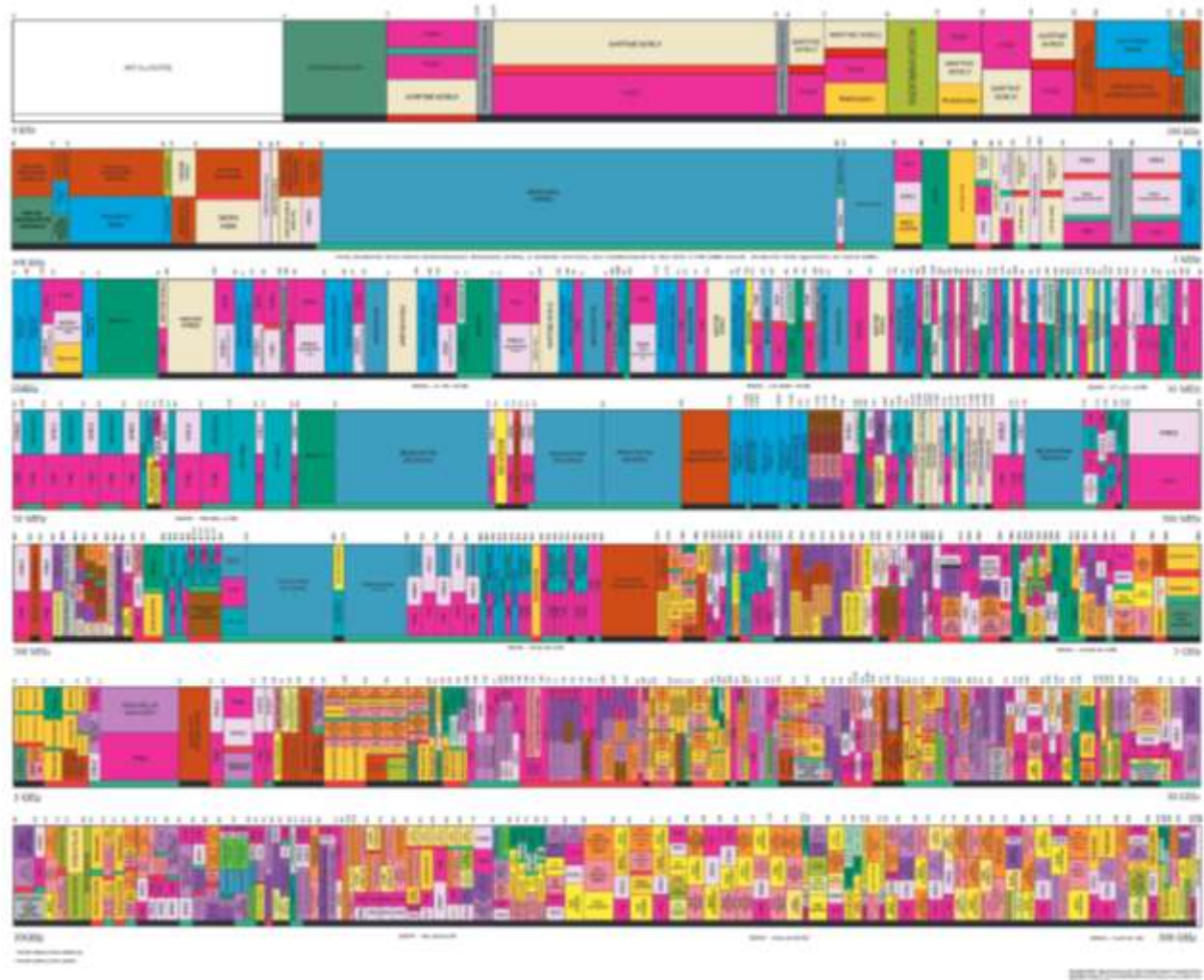
Source: 3GPP TSG SA#87e, 17-20 March 2020, e-meeting document SP-200222

© 3GPP 2020

Spectrum & Engineering

Spectrum: A Finite Resource

UNITED STATES FREQUENCY ALLOCATIONS THE RADIO SPECTRUM



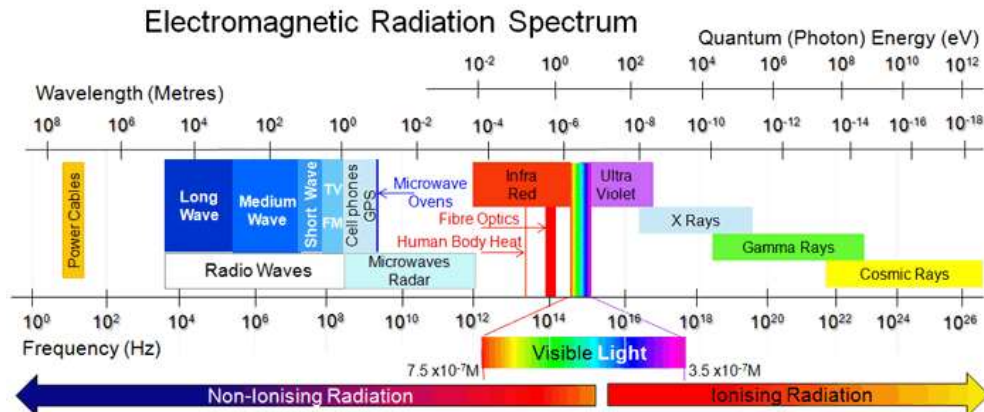
Two Paths for 5G Engineering Investment

Sub-6 GHz:

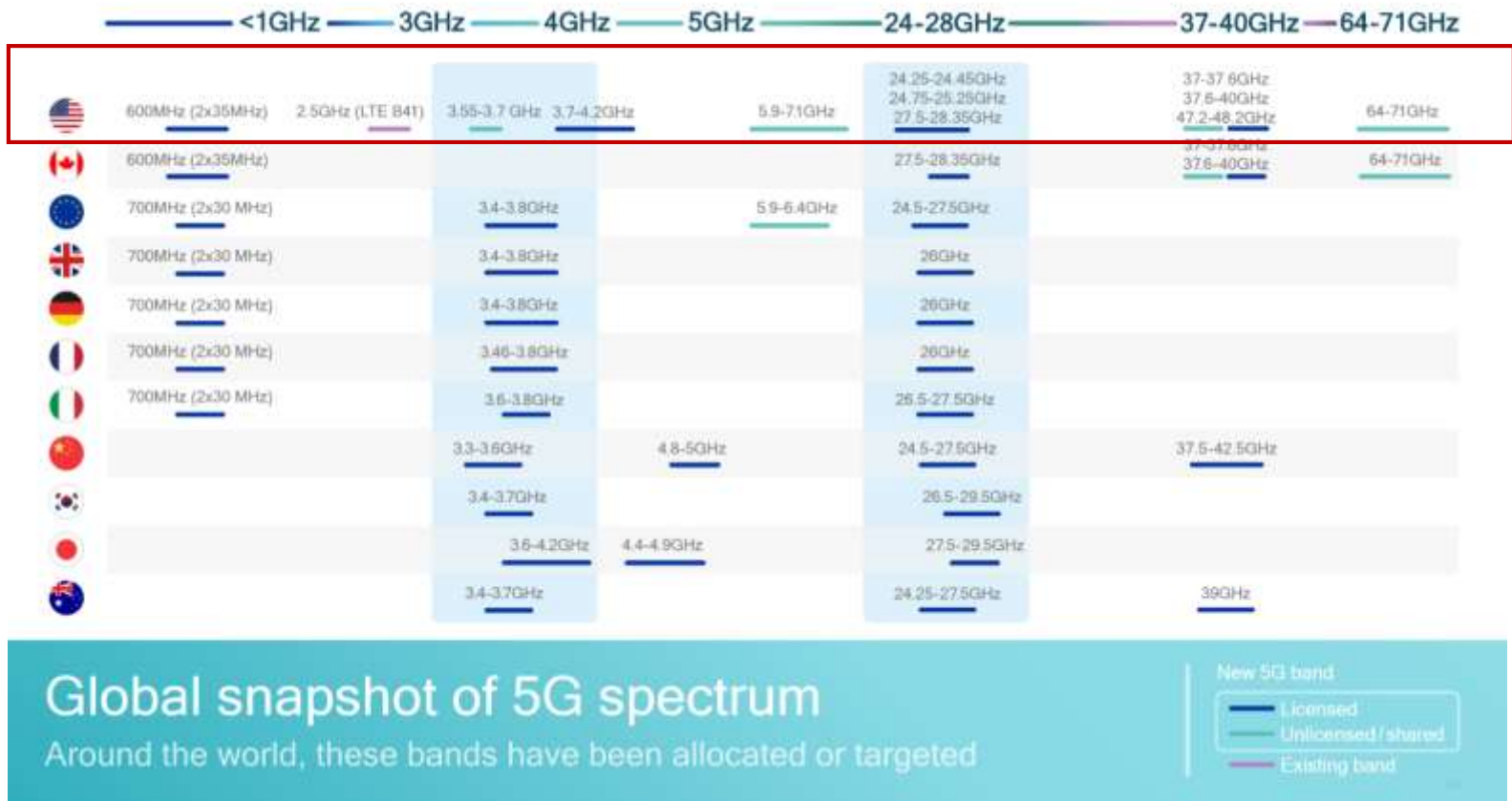
- Mostly 3 to 4 GHz Spectrum
- Lower power, therefore greater range
- Fewer number of base stations needed
- Majority of countries pursuing Sub-6 GHz options

mmWave:

- ~24 to 100 GHz Spectrum
- Higher power, but smaller range
- Greater number of base stations needed
- Few countries pursuing mmWave options



5G Proposed Spectrum Allocation

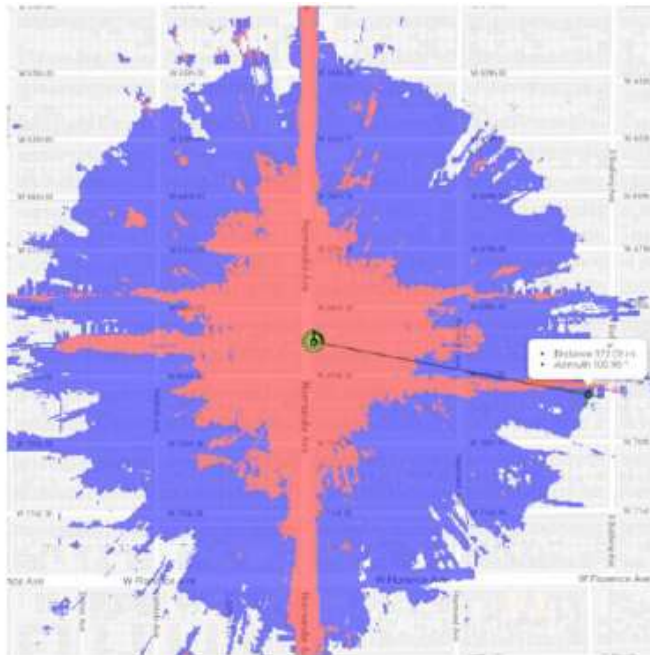


<https://www.qualcomm.com/media/documents/files/spectrum-for-4g-and-5g.pdf>

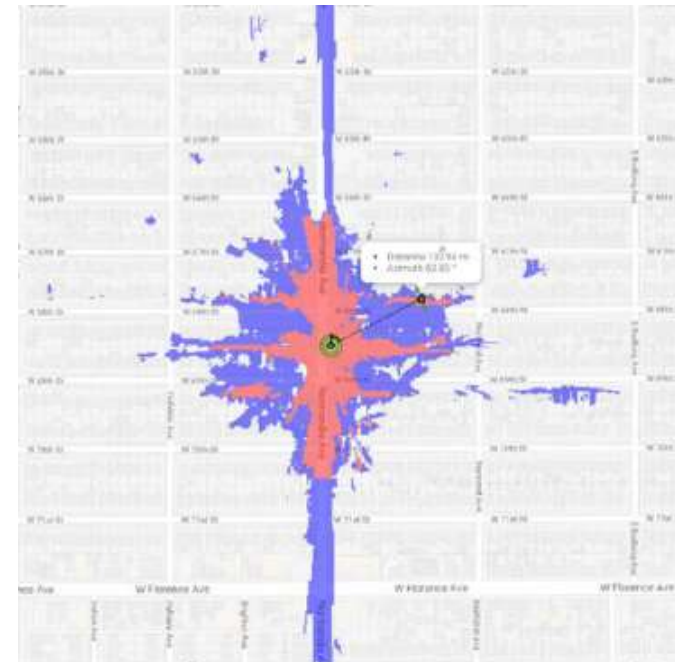
Propagation Challenges

100 Mbps

1 Gbps



Sub-6 GHz Propagation
(3.4 GHz)

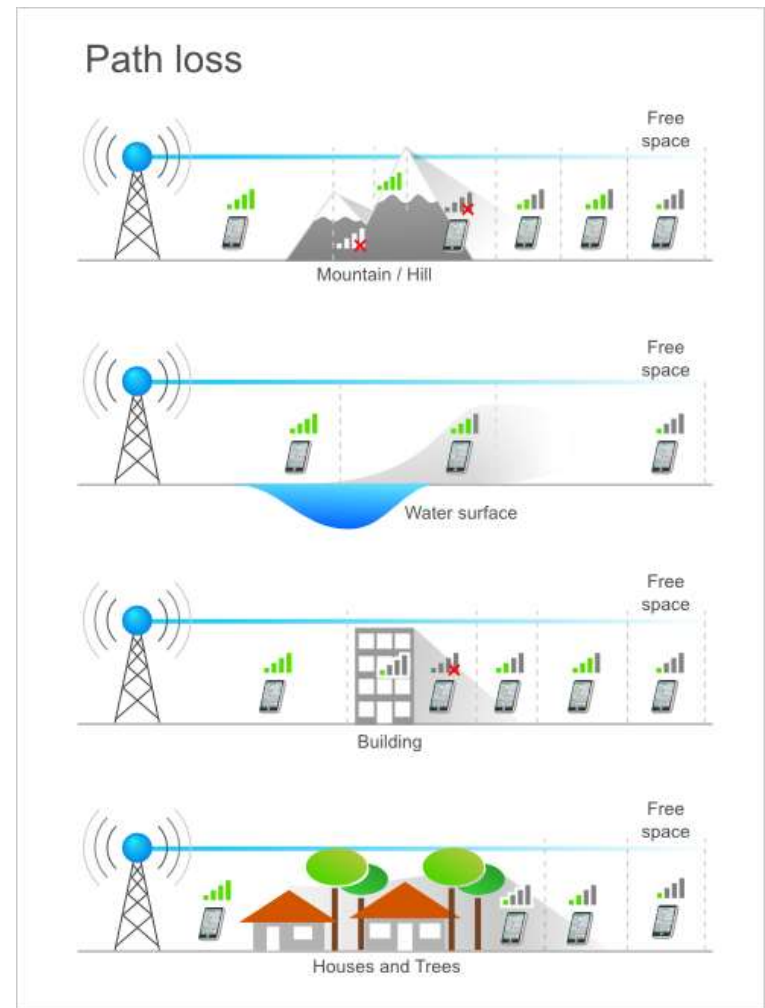


mmWave Propagation
(28 GHz)

https://media.defense.gov/2019/Apr/03/2002109302/-/1/1/0/DIB_5G_STUDY_04.03.19.PDF

New Tech – Same Problems

- Interoperability Challenges:
 - 3.3 GHz to 3.65 GHz previously reserved for exclusive federal use
 - mmWave development emphasized in US, because of greater spectrum availability
 - Rest of world focusing on Sub-6 development
- Engineering standards still being finalized
- Physical limitations to effective propagation



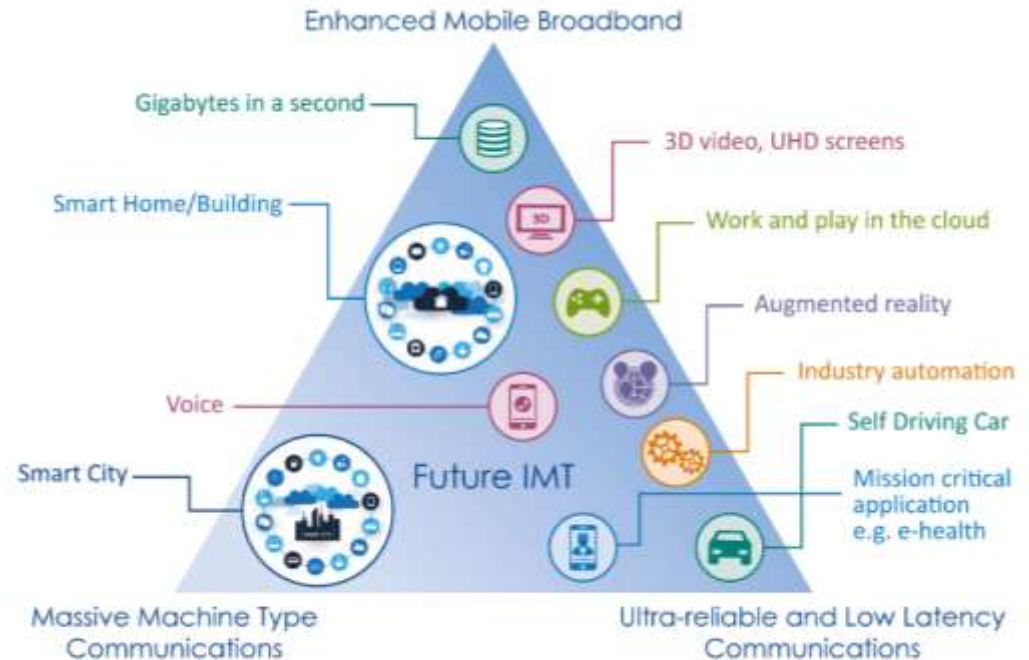
https://wiki.yatebs.com/index.php/Radio_Propagation_Concepts

5G in Practice

5G Use Cases

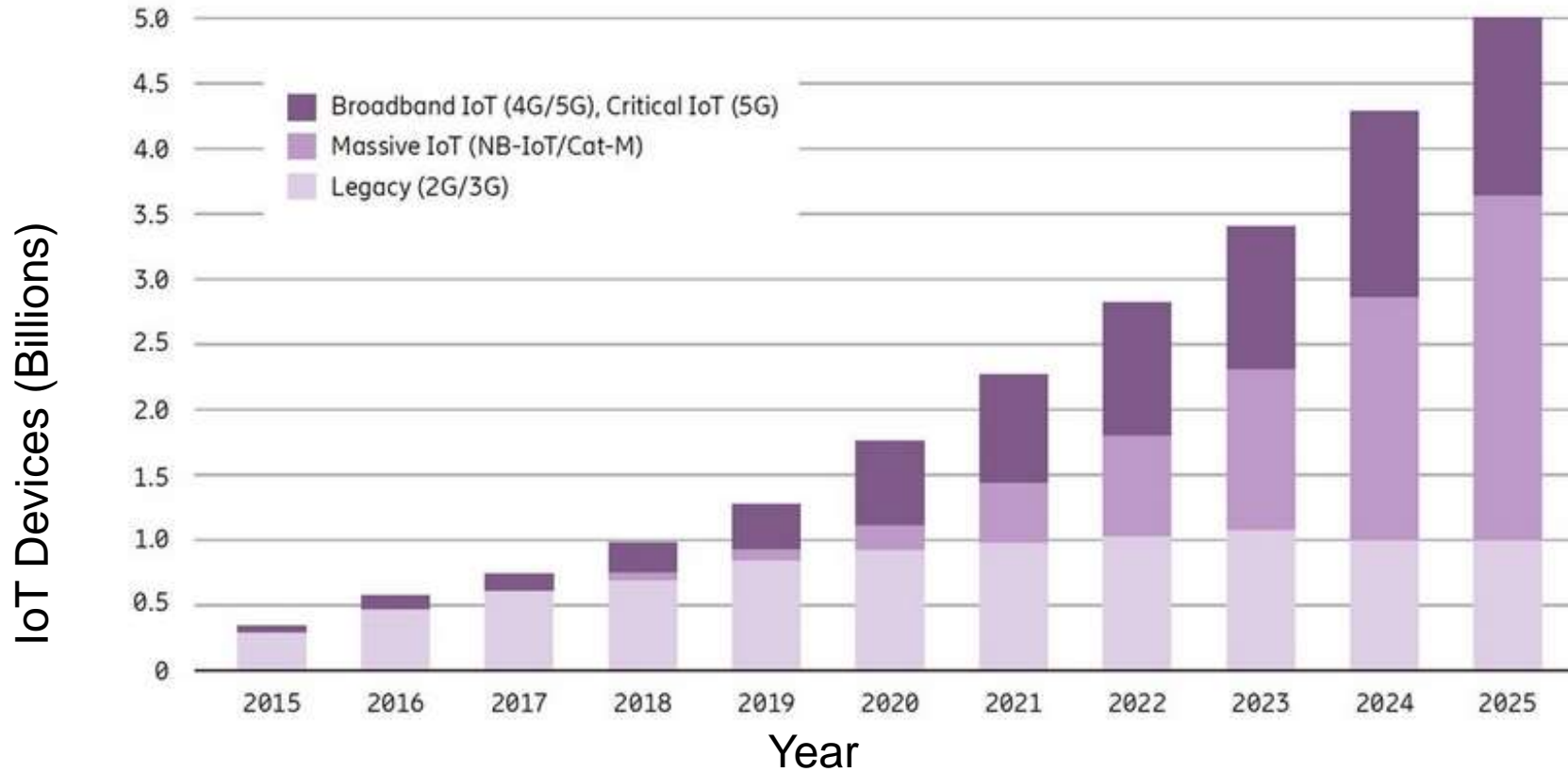
Three Main Use Cases:

1. Enhanced Mobile Broadband (eMBB)
 - *Example: Mobile streaming*
2. Massive Machine Type Communications (mMTC)
 - *Example: Agricultural sensors*
3. Ultra-Reliable & Low Latency Communications (URLLC)
 - *Example: Autonomous vehicles*



Internet of Everything

Ericsson Predicts Massive Growth in IoT Devices



<https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-networks-for-massive-iot--enabling-low-power-wide-area-applications>

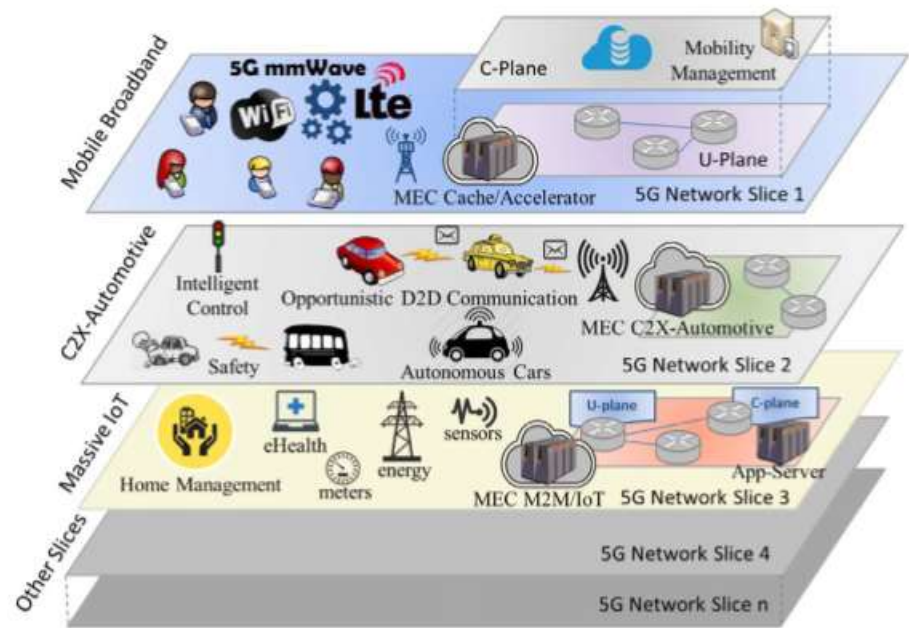
Key Enabling Technologies

SDN – Software Defined Networking

NFV – Network Function Virtualization

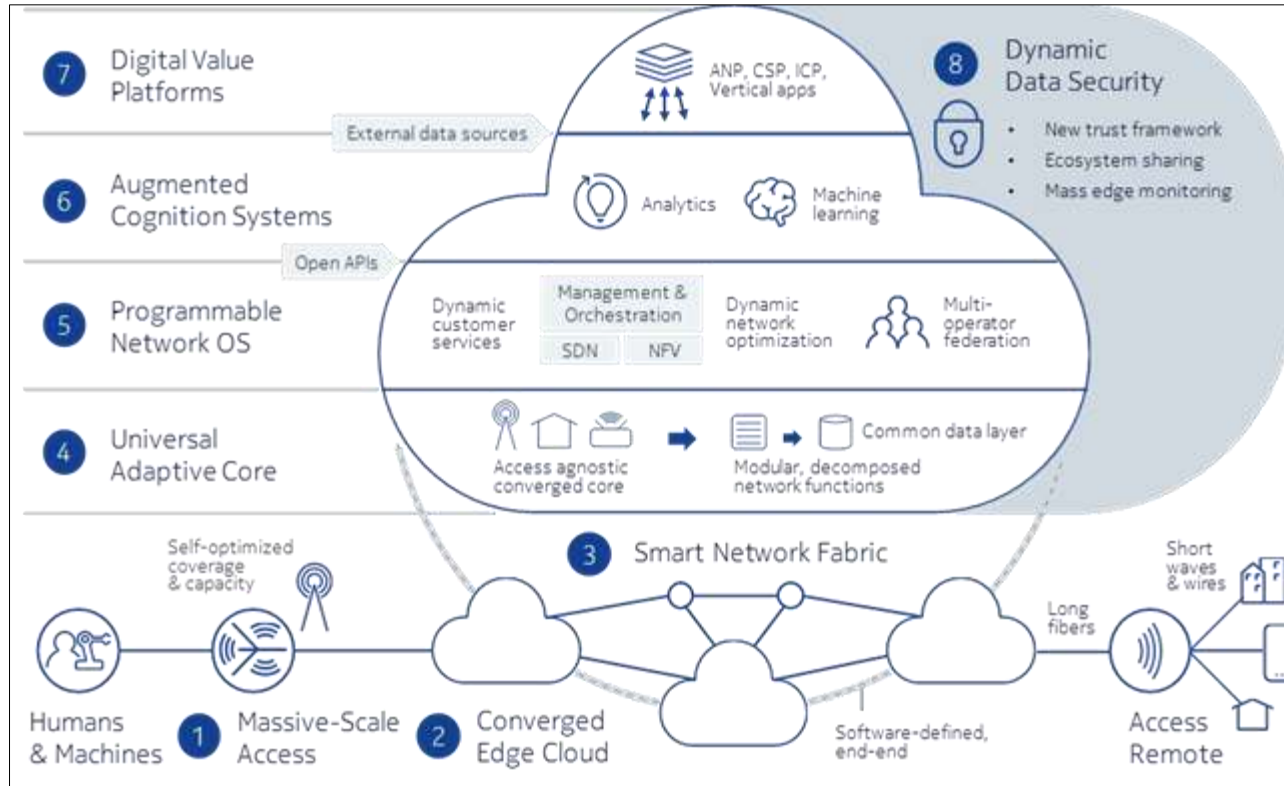
MEC – Multi-Access Edge Computing

- Network slices logically separated
- Multi-tenant scenario
- Slices provisioned with different requirements



5G Network Slices

5G & SDN Ecosystem



<https://networks.nokia.com/5g/get-ready>

Security

Key Security Considerations

- 5G will be pervasive & ubiquitous
- Attack Surface:
 - Millions of devices and connections
 - Unprecedented amounts of data
- Two different deployments:
 - Standalone (SA)
 - Non-Standalone (NSA)
 - Co-exists with 4G LTE
- NSA deployments vulnerable to exploit of legacy protocols (GTP, SS7, and Diameter)
 - Disclosure of subscriber information & spoofing



<https://newsroom.intel.com/editorials/intel-building-5g-revolution-today/>

5G Component Marketplace

Huawei



Ericsson



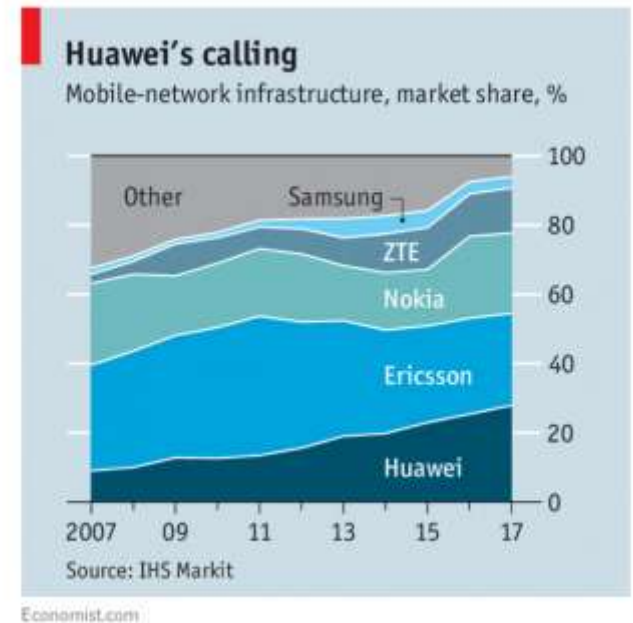
Nokia



?



No American company currently can provide 5G core infrastructure components at scale



“By the end of March, Huawei said it had signed 40 commercial 5G contracts with carriers, shipped more than 70,000 5G base stations to markets around the world and expects to have shipped 100,000 by May.”

-Reuters, April 21 2019

5G - Areas of Future Research

- Zero trust architecture models
- SDN, NFV, & MEC
- Vulnerability research
- Provisioning best practices
- Data protection & privacy
- And so much more



The sky is the limit!



Questions?