InquisIT

Transforming the Federal Government with 5G

InquisIT, LLC.
14900 Bogle Drive, Suite 203
Chantilly, VA 20151

Info@inquisitllc.com
www.inquisitllc.com

5G IS THE NEXT EVOLUTION IN MOBILE CONNECTIVITY

It is faster and more reliable than 4G, and will soon be the new standard for all mobile users. Estimates say that 32% of North American mobile connections will be 5G by 2023[1], and by 2025 5G will comprise 45% of all mobile data globally[2]. 5G improves the user experience in a variety of ways. With 5G, video conferences can be crisp and without audio delay, large files can download from office servers in a fraction of the time, applications hosted remotely can perform smoothly, and VPN connections can be stabilized.

Today, 5G already exists in at least thirty-five cities in the U.S.[3] The impact that 5G is having on American life, business and government will continue to grow as service-providers invest hundreds of billions of dollars in 5G over the next five years[4]. That impact is being accelerated by the COVID-19 pandemic, which has forced public and private sector employees to rely on home and mobile networks to perform their duties. It has been observed that internet traffic increased by as much as 100% as a consequence of COVID-19 lockdowns.[5] 5G is transforming the nature of that internet usage and will become ubiquitous in the not-so-distant future.

So, what is 5G? And what impact will it have on the federal government?

WHAT IS 5G?

5G is the fifth generation of mobile telecommunication technology. It is the successor to the fourth generation, known as 4G, which was the successor to 3G, and so on and so forth. Each generation is defined by its technical capabilities, specifically bandwidth (or "throughput") and latency. 5G transmitters (known as "base stations") must be capable of delivering at least 20 gigabits per second (Gbps) of throughput with a latency no higher than 4 milliseconds.[6] This is a tremendous leap over 4G, which requires just 100 megabits per second (Mbps) of throughput and latency below 100 milliseconds.

Transmission requirements that define 5G pertain to the base stations transmitting the data. They do not guarantee those capabilities to each device connected to the base station. Even if a device is connected to 5G, throughput and latency of that connection may be hampered by signal strength as well as the number of other devices connected to the same base station. However, 20Gbps is the minimum throughput required for 5G, and the technology has huge potential for growth beyond that. As service-providers invest more in 5G infrastructure, the performance experienced by individual users will continue to improve.

Evolution of 5g[7]

1982	1G	INTRODUCTION OF ANALOG TELECOMMUNICATIONS	2.4 KB/SEC; NA
1992	2G	TEXT MESSAGING	64 KB/SEC; 300-1000 MS
1998	3G	MOBILE & WIRELESS INTERNET CONNECTION	2 MB/SEC; 100-500 MS
2011	4G	CLOUD, IP & TRULY MOBILE BROADBAND	100 MB/SEC; <100 MS
2020	5G	UNLIMITED DATA CAPABILITY	20 GB/SEC; <5 MS

5G will literally impact every aspect of our lives. Investing in infrastructure now is critical so that we are ready to deploy 5G-enabled technologies. As we enter this new decade, I am more confident than ever that the 2020s will be defined by 5G and the other next-generation technologies that will create a smart revolution and improve the quality of life for a global population that has never been more interconnected. **-CNN Business**

THE NEW WAVE

Another defining feature of 5G is the spectrum of radio waves that are used to transmit data. 5G transmits in two primary bands: 410-7,125MHz (classified as FR1; commonly referred to as "sub-6"), and 24,250-52,600MHz, (classified as FR2; commonly known as "mmWave").[8]

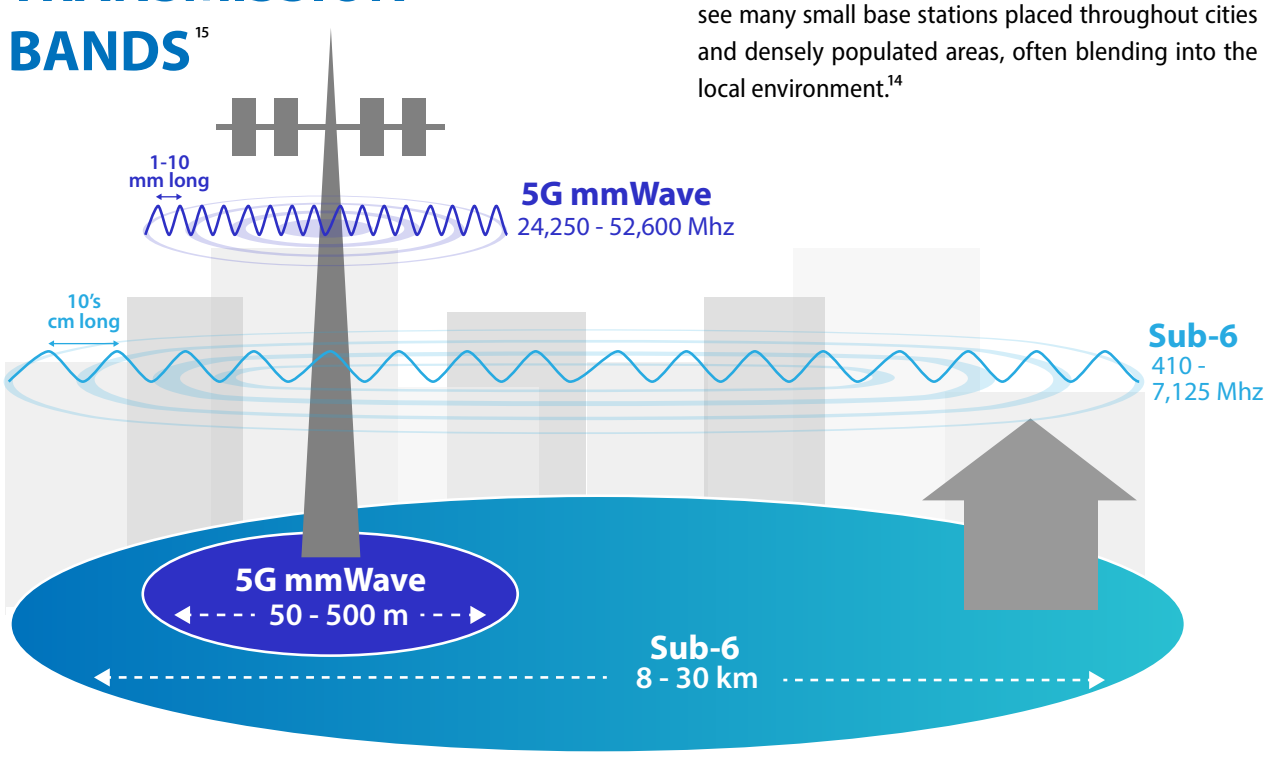
5G is the first generation of mobile telecommunications to use frequencies above 24GHz. Radio waves at this frequency are referred to as mmWave because they span between 1 to 10 millimeters in length, (Sub-6 waves are tens of centimeters long).[9] High frequency radio waves are a part of what makes high throughput possible for 5G.

More data can be transmitted in mmWave because there are more frequency channels that can be used and combined. 4G breaks sub-6 frequencies into 20MHz channels, and those 20MHz channels can be bonded together seven times to create a 140MHz channel. 5G channels are 100MHz each, and in the mmWave spectrum they can be bonded as many as eight times to create an 800MHz channel.[10]

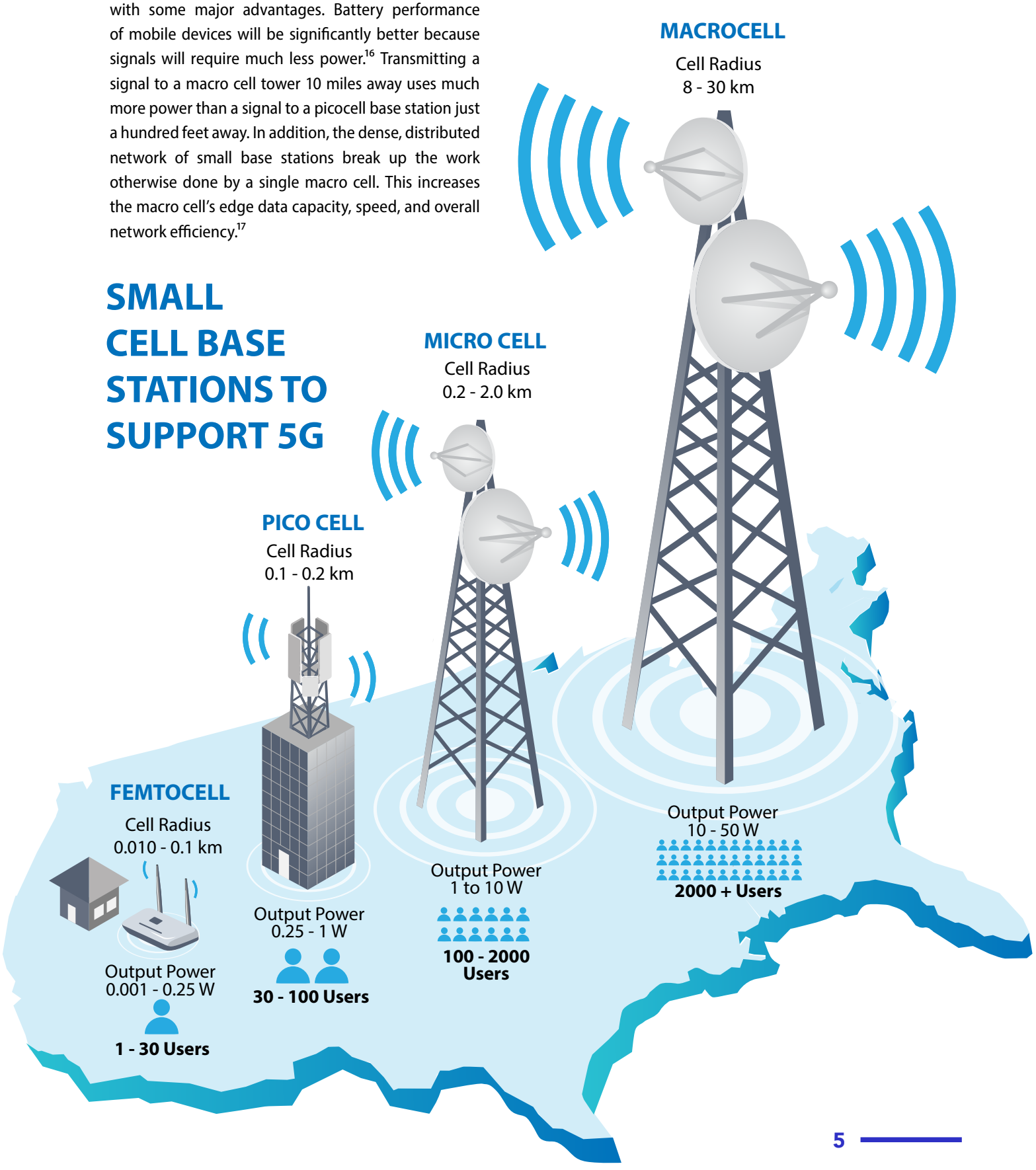
Using mmWave frequencies comes at a cost, however, due to the fragile nature of millimeter waves. Higher frequency radio waves do not penetrate surfaces as well as lower frequency radio waves. While sub-6 transmissions deliver a strong signal through walls and other obstacles, mmWave transmissions can be absorbed by foliage, rain, and any other dense object.[11] This means that 5G base stations need to be as close as possible to cell phones and other devices hoping to receive a signal, often fewer than 800 feet.[12]

5G therefore requires the installation of "small cell" base stations. The concept is that, in addition to "macro" cell radio towers transmitting high-power, low-frequency beams over huge areas, there also need to be many "micro," "pico," and "femto" cell base stations transmitting low-power, high frequency beams in small areas.[13] Consumers of 5G can expect to see many small base stations placed throughout cities and densely populated areas, often blending into the local environment.[14]

5G RADIO TRANSMISSION BANDS[15]



Installing vast numbers of small base stations is a challenge for making 5G ubiquitous, but it also comes with some major advantages. Battery performance of mobile devices will be significantly better because signals will require much less power.[16] Transmitting a signal to a macro cell tower 10 miles away uses much more power than a signal to a picocell base station just a hundred feet away. In addition, the dense, distributed network of small base stations break up the work otherwise done by a single macro cell. This increases the macro cell's edge data capacity, speed, and overall network efficiency.[17]



THE OLD WAVE

While mmWave is a major component of 5G technology, 5G also operates in sub-6 frequencies. Sub-6 frequencies have unique properties and use-cases, and 5G takes advantage of this. Higher frequencies carry more data at a faster rate, but lower frequencies are more reliable and can travel further. In order to bring 5G coverage to all consumers, service-providers must make use of sub-6 frequencies.

However, 4G/LTE also uses sub-6 frequencies and competes for channel-space with 5G. This problem is solved with Dynamic Spectrum Sharing (DSS). DSS enables service-providers to dynamically split channels between 4G and 5G based on demand.[18] When DSS is implemented, service-providers can carry 4G and 5G on the same channels.

DSS allows for a smoother transition from 4G to 5G, but it also blurs the lines between the two. Some service-providers have begun advertising services that have "5G" in the title but are actually 4G service.[19] 4G and 5G can share the same frequencies, but the technologies that power the two are still separate and unique.

So, What is "True" 5G?

"True" 5G may be better understood as **5G NR (New Radio)**. 5G NR refers to the "new radio" interface and radio access technology for mobile cellular networks.[20] It is the method of connection for 5G, much like LTE has become the method of connection for 4G. A 5G NR connection is a true 5G connection.

Much as DSS enables overlap between 4G and 5G, there is also overlap during the transition from LTE to 5G NR. Service-providers want to make use of their early 5G installations without needing to wait for the entire infrastructure to be completed. The goal is to offer partial 5G service as soon as possible and then watch their 5G offerings become more powerful as the infrastructure is completed and expanded.

The first iteration of 5G uses 5G NR base stations at the edge, but rides an LTE backbone in the core. This is known as **Non-standalone, (NSA)**, because the 5G service provided is reliant on existing LTE infrastructure.[21] Once this legacy infrastructure is no longer necessary, and the service is provided entirely by 5G technologies, the final iteration is called **Standalone (SA)** and is where the true potential of 5G will begin to be unlocked.

THE WIRELESS FEDERAL WORKFORCE

The COVID-19 pandemic has changed the nature of work in both the public and private sectors. Mass telework is currently the norm for a large section of the economy. As the nation recovers from COVID-19, the massive change in the workforce may well continue.

The power of home networks now shape and influence workforce productivity. Large file transfers, video conferencing, remote applications, and VPNs are common use-cases for federal workers. Each use-case requires high throughput and reliability, which not all home networks currently have. It has quickly become mission-critical for the federal government to assure that home networks are reliable and provide ample throughput.

Most home networks today are connected by broadband internet. Hardwired broadband connectivity is currently found in 80% of homes.[22] Service-providers still have limited fiber networks outside of densely populated areas, and 51% of Americans only have one option for any broadband service at all.[23]

5G is being offered not just for mobile devices, but also for homes. It can replace broadband service entirely. This is possible because of a service called Fixed Wireless Access (FWA). FWA enables 5G to be transmitted to a modem, which then provides connectivity to the consumer's home network.[24] FWA is beneficial not only for bringing the power of 5G, but also because it requires no physical connection to the home. Just like a mobile device, an FWA modem receives its signal from a nearby 5G base station via radio waves. Installation for FWA is much easier than broadband because there is no cabling required.

5G networks are significantly faster and more reliable than even the best broadband connections today. 5G FWA is bringing massive improvements to telework productivity. Federal agencies exercising mass-telework will be the beneficiaries of this new technology. It is estimated that 10% of US households will rely on 5G FWA by 2024,[25] and that will certainly include a large number of federal employees.

SECURING FEDERAL AGENCIES FOR 5G

Because many federal employees are working remotely, 5G networks are inadvertently providing connectivity to at least some government phones and laptops. In a handful of years, 5G will be providing connectivity to greater numbers of government computers, including a massive quantity of IoT (Internet of Things) devices. Fully embracing 5G technology into the federal government requires a sober evaluation of the security vulnerabilities - especially for agencies that handle sensitive data.

CISA WARNINGS

In 2019, the U.S. Cybersecurity and Infrastructure Security Agency (CISA) identified a few key vulnerabilities within 5G deployment. Their assessment regards the supply chain, network security, and deployment of 5G.

Most 5G manufacturing is based outside the U.S. and is performed by companies that CISA describes as "untrusted." 5G components provided by such companies "expose U.S. entities to risks introduced by malicious software and hardware; counterfeit components; and component flaws caused by poor manufacturing processes and maintenance procedures."[26] Federal agencies need to exercise caution when provisioning 5G technologies from foreign companies, and in many cases will be unable to patronize certain manufacturers entirely. This will present an additional challenge, as it severely limits the 5G resources available for use and may cause the U.S. government to lag behind nations with greater 5G manufacturing capabilities.[27]

5G networks are vulnerable in early stages due to the nature of 5G Non-standalone (NSA). Vulnerabilities within LTE could compromise the security of 5G networks until 5G becomes independent of that legacy backbone. CISA notes that "inheritance of security settings, permissions, and technical specifications from an untrusted [LTE] core network may negate built-in 5G device security."[28] Even beyond 5G NSA, 5G SA deployments are also at risk due to a lack of diligence in applying security updates. CISA writes, "Even as security updates are released, some entities may be slow to implement them for a variety of reasons, such as the potential impact to operations from taking systems offline."[29] 5G is a new technology, and it will inevitably introduce security fixes over time that must be applied with haste in order to remain secure.

Federal agencies need to exercise caution when provisioning 5G technologies from foreign companies, and in many cases will be unable to patronize certain manufacturers entirely.

"Small cell" infrastructure is another risk because of the accessibility of base stations that will transmit 5G signals. It is much easier to secure macro cell towers that stand on private property than it is to secure 5G base stations installed in public locations, many as small as a backpack. Physical access to 5G base stations "may provide malicious actors with [...] the ability to intercept data routed through the device, [...] conduct Denial of Service (DOS) attacks, [...and] clone devices, allowing the replica to make calls, use data, and add charges."[30] It is also easier for hackers to install a fake base station that could be used to steal or alter data.[31] Hardening the physical security of base stations will be a crucial step in making 5G safe for federal use.

INTERNET OF VULNERABLE THINGS

The Internet of Things (IoT) refers to items/objects that are connected to the internet. This includes refrigerators, traffic lights, cars, and security cameras, to name a few. Vast quantities of mundane objects are being connected to the internet as it becomes easier to attach network receivers to any smart device. 5G is accelerating the expansion of IoT by offering lower latency, increased bandwidth, and the ability to cater to specific use cases with network slicing.[32] Adding huge numbers of unsophisticated items to the internet introduces a handful of security issues.

Unsophisticated items are ripe for hacking when they are accessible from the internet. Hackers can scan hundreds of thousands of objects that may be using default passwords, as there is a high likelihood of finding an unhardened IoT device.[33] Once a vulnerable device has been compromised, 5G makes it even more of a liability by providing high-speed connectivity. Hackers can quickly extract sensitive information that the IoT device may be carrying or to which it may have access.

IoT devices may also lack the security provided by a home or corporate network. IoT devices can be connected directly to the internet via their mobile receiver. In those cases they are not protected by the firewalls and other security measures typically present in a federal enterprise.[34] It is critical that U.S. agencies take measures to place IoT devices within their own intranets so that assets are not exposed to the open internet.

CONCLUSION

5G is changing what is possible with mobile communications, and that change over the next few years will be transformative. Cell phones will stream 4k videos seamlessly, autonomous vehicles will talk to each other in real time to ease traffic flow, and augmented and virtual reality applications will be more powerful and immersive.

This bright future already exists in certain major cities across the globe. South Korea has close to seven million 5G subscribers[35], and China expects to install over 600,000 5G base stations by the end of the year.[36] Domestically, the federal government is also poised to benefit from 5G technology. An appropriate security posture in the federal enterprise and an early 5G adoption in the private sector will be the keys to a successful 5G deployment. ■

REFERENCES

1. Fisher, T. "5G Availability Around the World." *Lifewire*, August, 2020. https://www.lifewire.com/5g-availability-world-4156244.
2. Jejdling, F., et al. "Ericsson Mobility Report June 2020." *Ericsson*, June, 2020. https://www.ericsson.com/en/mobility-report/reports/june-2020.
3. "5G Coverage Map." *Verizon*. https://www.verizon.com/5g/coverage-map/.
4. Fisher, T. "5G Challenges: Why It Isn't Rolling Out Faster." *Lifewire*, March, 2020. https://www.lifewire.com/5g-challenges-4580354.
5. Ibid, 2.
6. Fisher, T. "5G Speed: How to Understand the Numbers." *Lifewire*, March, 2020. https://www.lifewire.com/5g-speed-4180992.
7. "Critical Infrastructure Security and Resilience Note: Overview of Risks Introduced by 5G Adoption in the United States." *Cybersecurity and Infrastructure Security Agency*, July 31, 2019. https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.
8. "5G Frequency Bands, Channels for FR1 & FR2." *Electronics Notes*. https://www.electronics-notes.com/articles/connectivity/5g-mobile-wireless-cellular/frequency-bands-channels-fr1-fr2.php. (Date Accessed: August 18, 2020).
9. Nordrum, A., Clark, K., et. al. "5G Bytes: Millimeter Waves Explained." *IEEE Spectrum*, May 17, 2017. https://spectrum.ieee.org/video/telecom/wireless/5g-bytes-millimeter-waves-explained.
10. Segan, S. "What Is 5G?" *PC Magazine*, April 6, 2020. https://www.pcmag.com/news/what-is-5g.
11. Ibid, 9.
12. Ibid, 10.
13. Nguyen, T. "Small Cell Networks and the Evolution of 5G." *Qorvo*, May 17, 2017. https://www.qorvo.com/design-hub/blog/small-cell-networks-and-the-evolution-of-5g.
14. "Key Elements for 5G Networks." *SDX Central*, October 20, 2017. https://www.sdxcentral.com/5g/definitions/key-elements-5g-network/.
15. Ibid, 13.
16. Ibid.
17. Ibid, 14.
18. Ibid, 10.
19. Ibid.
20. "What is 5G NR?" *Verizon*, December 6, 2019. https://www.verizon.com/about/our-company/5g/what-is-5g-nr.
21. Malizia, M. "Why do you need a 5G Core network and 5G NR Standalone?" *Ericsson*, May 19, 2020. https://www.ericsson.com/en/blog/2020/5/why-do-you-need-a-5g-core-network-and-5g-nr-standalone.
22. Chitkara, H. "Qualcomm's 5G fixed wireless access will help telecoms disrupt the home-internet market." *Business Insider,* October 15, 2019. https://www.businessinsider.com/qualcomms-5g-fixed-wireless-access-will-shift-telecom-competition-2019-10.
23. Ibid, 10.
24. Ibid, 22.
25. Ibid.
26. Ibid, 7.

REFERENCES

27. Rosenberg, B. "Unsafe At Any Speed: Multiple Vulnerabilities Afflict 5G." *Breaking Defense,* August 12, 2019. https://breakingdefense.com/2019/08/unsafe-at-any-speed-multiple-vulnerabilities-afflict-5g/.
28. Ibid, 26.
29. Ibid.
30. Ibid.
31. "Impact of 5G network on IoT Security." *Lifars*, March 11, 2020. https://lifars.com/2020/03/impact-of-5g-network-on-iot-security/.
32. Ibid.
33. Ibid.
34. Ibid.
35. Tomas, J.P. "South Korea nears 7 million 5G subscribers." *RCR Wireless News*, July 2, 2020. https://www.rcrwireless.com/20200702/5g/south-korea-nears-7-million-5g-subscribers.
36. Wang, M. "China's 5G surge: All major cities to have 5G network coverage by year-end." *CGTN*, May 28, 2020. https://news.cgtn.com/news/2020-05-28/China-s-5G-surge-All-major-cities-to-have-5G-network-by-year-end-QRGKU2CheE/index.html.

InquisIT

InquisIT, LLC.
14900 Bogle Drive, Suite 203
Chantilly, VA 20151

Info@inquisitllc.com
www.inquisitllc.com