July 31, 2019; 1200 EDT

OVERVIEW OF RISKS INTRODUCED BY 5G ADOPTION IN THE UNITED STATES

KEY FINDINGS

The Department of Homeland Security (DHS)/Cybersecurity and Infrastructure Security Agency (CISA) assesses that Fifth Generation Mobile Network (5G) will present opportunities and challenges, and its implementation will introduce vulnerabilities related to supply chains, deployment, network security, and the loss of competition and trusted options.

- Use of 5G components manufactured by untrusted companies could 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. 5G hardware, software, and services provided by untrusted entities could increase the risk of compromise to the confidentiality, integrity, and availability of network assets. Even if U.S. networks are secure, U.S. data that travels overseas through untrusted telecommunication networks[i] is potentially at risk of interception, manipulation, disruption, and destruction.
- 5G will use more components than previous generations of wireless networks, and the proliferation of 5G infrastructure may provide malicious actors more attack vectors. The effectiveness of 5G's security enhancements will in part depend on proper implementation and configuration.
- Despite security enhancement over previous generations, it is unknown what new vulnerabilities may be discovered in 5G networks. Further, 5G builds upon previous generations of wireless networks and will initially be integrated into 4G Long-Term Evolution (LTE) networks that contain some legacy vulnerabilities.
- Untrusted companies may be less likely to participate in interoperability efforts. Custom 5G technologies that do not meet interoperability standards may be difficult to update, repair, and replace. This potentially increases the lifecycle cost of the product and delays 5G deployment if the equipment requires replacement. The lack of interoperability may also have negative impacts on the competitive market as companies could be driven out if the available competitive market decreases.

The United States Government can manage these vulnerabilities and increase the security of communications networks as 5G is adopted by:

- Encouraging continued development of trusted 5G technologies, services, and products.
- Encouraging continued trusted development of future generations of communications technologies.
- Promoting international standards and processes that are open, transparent, consensus–driven, and that do not place trusted companies at a disadvantage.
- Limiting the adoption of 5G equipment with known or suspected vulnerabilities.
- Continued engagement with the private sector on risk identification and mitigation efforts.
- Ensuring robust security capabilities for 5G applications and services.

---

[i] Untrusted equipment and networks are those manufactured, installed, serviced, managed, or otherwise handled by untrusted entities.

SCOPE NOTE: DHS/CISA produced this Critical Infrastructure Security and Resilience Note to provide an overview of 5G technology, and represents DHS/CISA's analysis of the vulnerabilities likely to affect the secure adoption and implementation of 5G technologies. This analysis represents the beginning of CISA's thinking on this issue, and not the culmination of it. It is not an exhaustive risk summary or technical review of attack methodologies. This product is derived from the considerable amount of analysis that already exists on this topic, to include public and private research and analysis. Analysis of complex, sophisticated, and distributed cyber intrusions against 5G networks is beyond the scope of this product. At the time of this product's creation, 5G standards, networks, and components are still under development.

This product was coordinated with the CISA Cybersecurity Division (CSD), Infrastructure Security Division (ISD), industry partners, and Sandia National Laboratories.

THE HISTORY OF CELLULAR COMMUNCIATIONS

In 1982, the first cellular wireless generation (G) in the United States launched, utilizing analog communications to provide basic speech service.[1] Since then, wireless providers have introduced new wireless generations approximately every 10 years, increasing data throughput[ii] and reducing latency[iii].[2] Digital transmission over the air, introduced in 2G, replaced analog and supported data services for mobile devices. 2G technologies enabled capabilities like text and picture messaging. Upgrades to existing networks and new mobile devices accompanied 3G's introduction, which introduced a data overlay to support data capabilities such as Global Positioning System (GPS), video conferencing, and multi-media streaming.[3,4]

4G changed the way media is consumed, enabling the wide scale transition from downloading content on home computers to streaming content on mobile devices.[5] As of June 2019, 4G is the primary wireless standard used in the United States, although 2G and 3G are still exclusively used in some rural areas that lack 4G coverage.[6,7] Two versions of 4G were released after the original standard: (LTE) and LTE Advanced (LTE-A). Both releases updated the existing 4G network and significantly improved upon its upload and download speeds.[8] 4G, however, is unable to support the needs of an evolving telecommunications industry with tens of billions of connected devices and increasing data requirements.[9] Table 1 shows the evolution of wireless generations since 1982, including the expected wide rollout of 5G.

TABLE 1—EVOLUTION OF WIRELESS GENERATIONS[10,11,12]

WIRELESS GENERATION	THROUGHPUT	LATENCY	YEAR	AMERICANS WITH MOBILE SUBSCRIPTIONS
1G	2.4 kilobits per second (kbps)	N/A	1982	<1%
2G	64 kbps	300-1000 Milliseconds (MS)	1992	3%
3G	2 Megabytes Per Second (Mbps)	100-500 MS	1998	45%
4G	100 Mbps	<100 MS	2011	96%
5G	20 Gigabytes Per Second (Gbps)	<5 MS[iv]	2020	N/A

[ii] Throughput refers to how much data can traverse from one location to another in a given amount of time.
[iii] Latency is the delay in transmitting and processing data, such as the delay between when a command is sent and when it is executed.
[iv] Emerging technologies like autonomous vehicles and remote surgery will be more feasible at these latencies.

WHAT IS 5G?

5G is the next generation of wireless technology that represents a complete transformation of telecommunication networks. Combining new and legacy technology and infrastructure, 5G will build upon previous generations in an evolution that will occur over many years, utilizing existing infrastructure and technology.

5G builds upon existing telecommunication infrastructure by improving the bandwidth, capacity, and reliability of wireless broadband services.[13] The evolution will take years, but the goal is to meet increasing data and communication requirements, including capacity for tens of billions of connected devices that will make up the Internet of Things (IoT),[v] ultra-low latency required for critical near-real time communications, and faster speeds to support emerging technologies.[14] As of June 2019, 5G networks and technologies are in development with a limited rollout in select cities around the world, including 20 in the United States.[15,16]

How Will 5G Work?

Wireless communications traditionally transmit data over low-band radio frequencies. Waves at these low-band frequencies are penetrative[vi] (can pass through walls and other materials) and can travel long distances, and therefore can use large, macro cellular towers to cover a large geographic area.[17] The 5G wireless system will transmit and receive radio signals over low-, medium-, and high-band radio frequencies (see figure 1). Expanding the range of wireless frequencies devices use will help minimize wireless traffic congestion by increasing capacity, and meet the growing requirements for greater throughput, lower latency, and higher speeds.[18] High frequency waves will improve speed but will be less penetrative and have shorter transmission ranges (likely hundreds of meters instead of kilometers). 5G will require the full complement of spectrum frequencies (low, mid, and high) because each frequency type offers unique benefits and challenges.

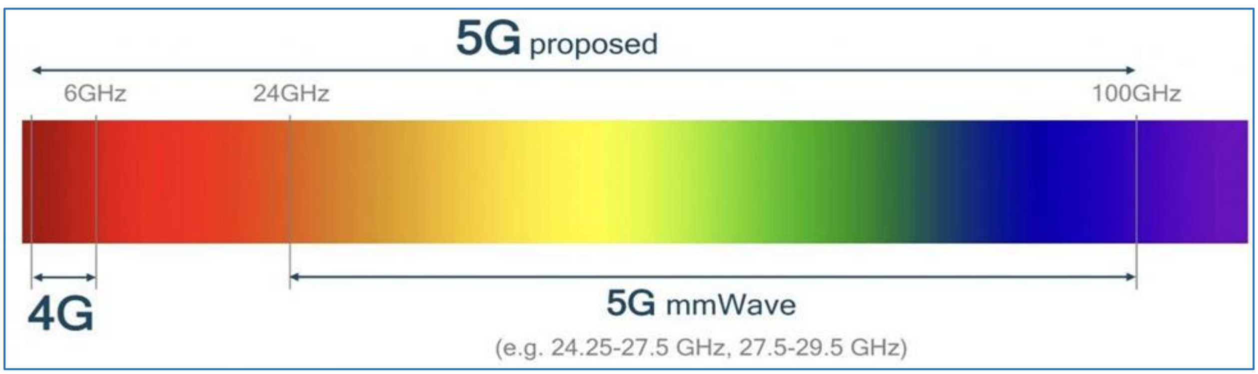

FIGURE 1—4G AND 5G WIRELESS FREQUENCIES[19]

In many instances, 5G will rely on a new physical architecture with components built on a system of both traditional macro cellular towers and non-traditional, smaller deployments, such as small cells and micro cells—miniature cellular towers that transmit short-range radio signals.[20] In addition to connecting directly to base stations, wireless cellular devices will be able to connect to local small cells, which will then relay data through additional small cells to macro cellular towers.[21] The architecture needed to support 5G will depend on the geography and spectrum bands utilized to provide service. In many instances, small cells will need to be deployed widely across cities to support 5G connectivity, transmitting and receiving signals from locations such as streetlights, street signs, homes, vehicles, and businesses.[22] Figure two shows 5G communication technologies and how they are connected.

---

[v] The connection of systems and devices with primarily physical purposes (e.g., sensing, heating and cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems. [U.S. Department of Homeland Security. (2016). "Strategic Principles for Securing the Internet of Things (IoT)." U.S. Department of Homeland Security.]

[vi] Higher frequency waves are generally unable to pass through materials, including walls and other building materials as easily as lower frequency waves.

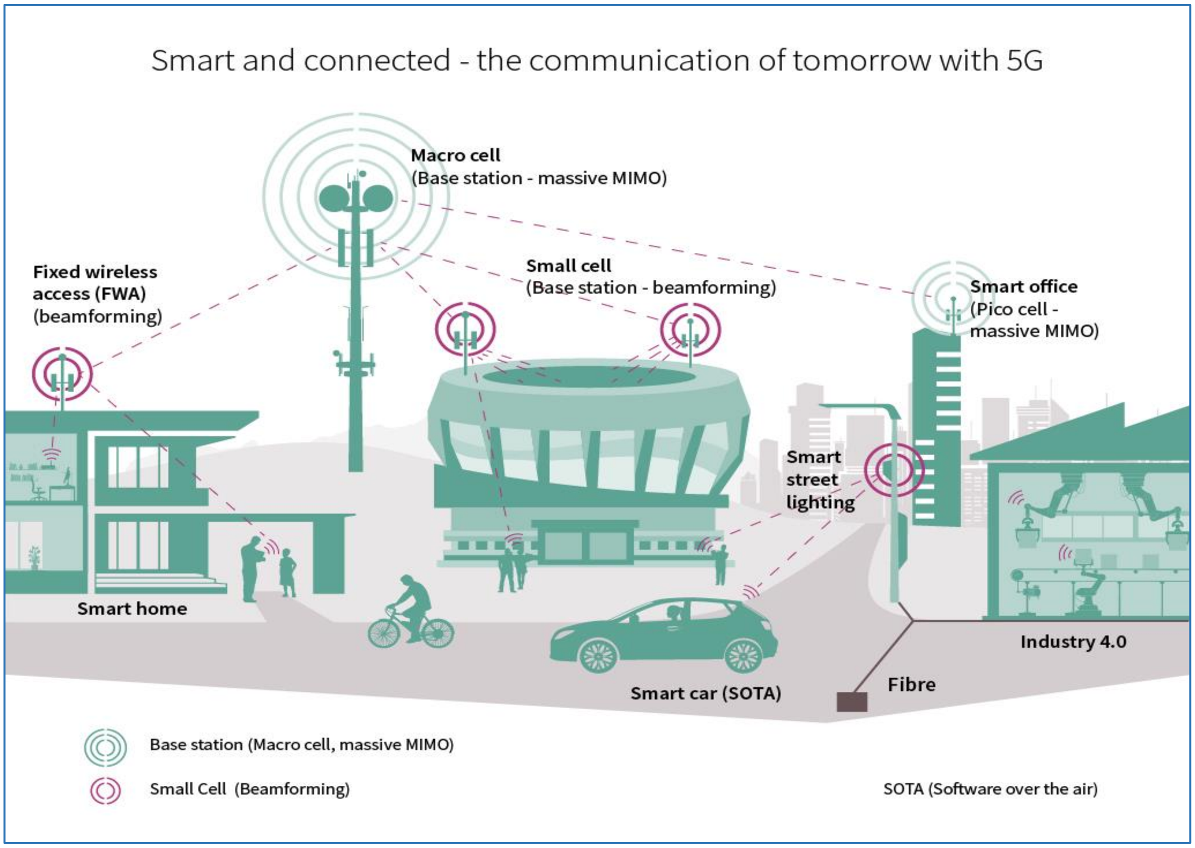

FIGURE 2—5G COMMUNICATION TECHNOLOGIES[23]

In areas with insufficient small cells to handle 5G traffic, wireless cellular devices may revert to 4G or other earlier wireless network generations. However, a lack of small cells does not mean that 5G is not possible; 5G speeds and capacity may be available through other 5G architectures. Figure three breaks down the major components of 5G networking into user equipment, radio access networks (RAN), and core network, and shows the market leaders in each area. This network architecture, with corresponding vendors, is intended to be high level. Additional granularity would result in a broader list of primary vendors, including additional American-based vendors.

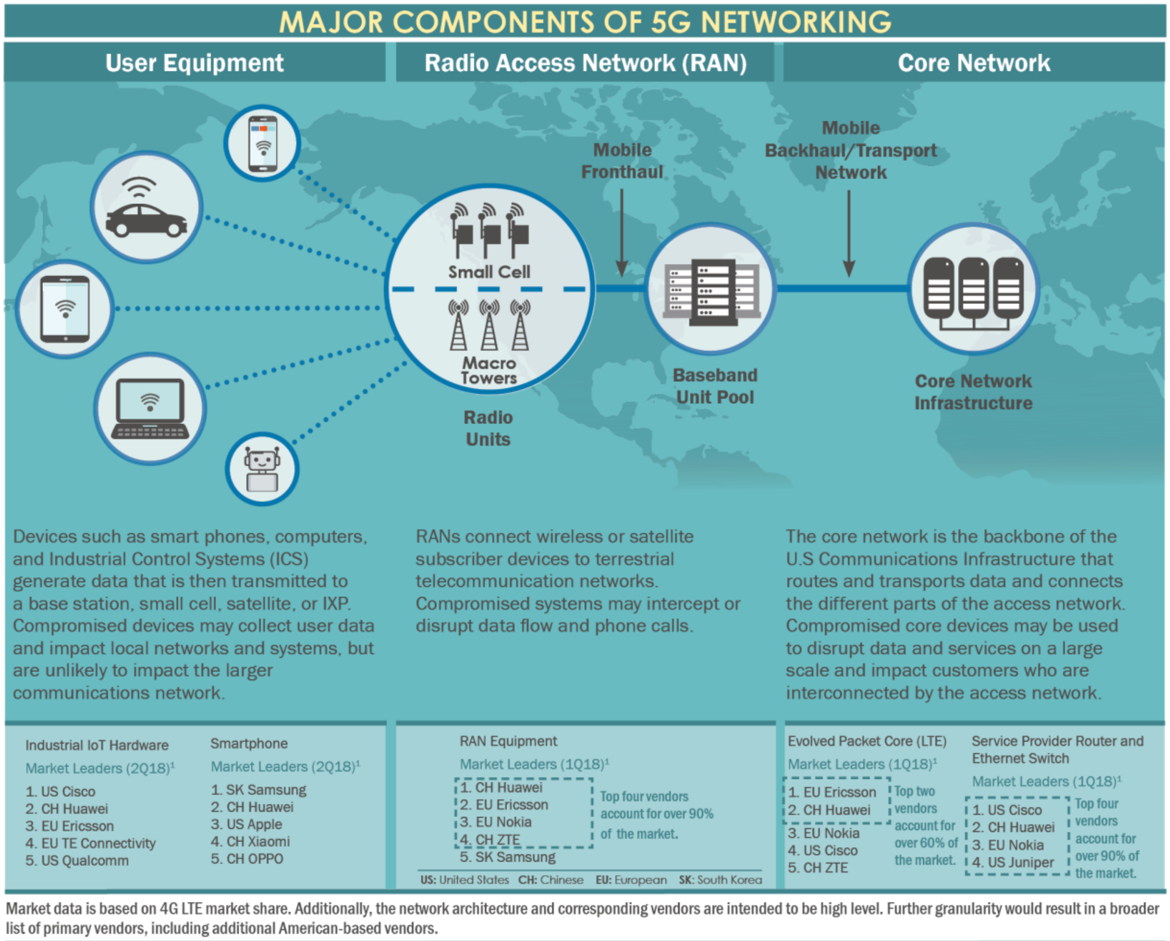

FIGURE 3—5G MAJOR COMPONENTS

How Will Technology Use 5G?

5G's higher speeds, increased bandwidth, and lower latencies will advance emerging and evolving technologies—including autonomous vehicles, augmented and virtual reality, remote medical procedures, and the IoT.[24,25,26] The low-, mid-, and high-band radio frequencies within the wireless spectrum have unique characteristics that may be utilized to meet varying use case requirements within 5G infrastructure. For example, Augmented/Virtual Reality will require high upload and download speeds, while autonomous vehicles will require ultra-low latency to ensure near-instantaneous responses. In 2016, standard and regulatory bodies categorized three primary ways[vii] technology would use 5G; Ultra-Reliable Low-Latency Communications (URLLC), Enhanced Mobile Broadband (eMBB), Massive Machine Type Communications (mMTC).[27,28,29]

[vii] Standard and regulatory bodies also identified a 4th 5G usage scenario, Network Operation, which will address system requirements, including network functions and capabilities, migration and interworking, optimizations and enhancements, and security. [3GPP (2016). "SA1 Completes its study into 5G requirements." 3GPP. http://www.3gpp.org/news-events/3gpp-news/1786-5g_reqs_sa1. Accessed on November 19, 2018.]

Table 2 summarizes the technical capabilities of each use case and provides examples of some of the technologies that will benefit.

TABLE 2—5G USE CASES[viii]

USE CASE	RADIO BAND	CAPABILITY	EXAMPLES OF 5G-ENABLED TECHNOLOGIES
eMBB	Low-Band	Low-band frequencies cover large geographic areas with penetrative signals, and can service densely populated metropolitan areas with high download speeds, likely reaching up to 20 Gbs, 20 times the speeds available from some current wireless networks.[30,31] eMBB will support data-driven applications that require high data rates across a wide coverage area, and will also support mobile connectivity, so users can access broadband consistently on the move.[32]	Augmented/Virtual Reality, Ultra High Definition Broadcasting, Home and Enterprise Broadband
URLLC	Mid-Band	Mid-band frequencies can cover large areas with the potential bandwidth to support high-capacity devices and services.[33] URLLC will support mission-critical systems and applications in which data is time-sensitive and requires high reliability.[34,35] Standard bodies have designated that end-to-end latency of 5ms or less, with an uptime of 99.999 percent.[36]	Vehicle-to-Everything (V2X)[ix], Autonomous Vehicles, Smart Grid, Tactile Feedback in Remote Medical Procedures, Unmanned Aviation, Robotics, Industrial Automation
mMTC	High-Band	High-band frequencies support fast download speeds but due to the non-penetrative signal and short range, increased infrastructure will be required to dispense signal.[37,38] mMTC will support the tens of billions of low-complexity, low-power devices that make up the IoT, and while eMBB prioritizes speed, mMTC will prioritize connectivity for a large number of devices.[39]	E-Health, Transport and Logistics, Smart Meters, Smart Agriculture

WHEN WILL 5G BE AVAILABLE?

5G began its rollout in the United States in 2018, but widespread availability is contingent on several factors, including the International Telecommunication Union's (ITU)[x] and 3rd Generation Partnership Project's (3GPP)[xi] standard finalization, federal regulation of spectrum, network implementation, and the development and production of 5G networks and devices.[40] Systems that utilize a wider range of spectrum, such as automotive and industrial automation and virtual reality, will be supported after smart phones as 5G technology and infrastructure continues to develop.[41] Widespread usage of a standalone 5G network is not expected until at

[viii] Table 2 is illustrative and is not comprehensive. Some technologies may use multiple radio bands.
[ix] V2X enables vehicles to communicate through on-board modules, small cells, road sensors, and towers.
[x] A United Nations agency responsible for Information and Communication Technologies (ICT). It allocates radio spectrum and develops global technical standards.
[xi] 3GPP is an industry based, multi-national technical organization made up of approximately 500 companies and government agencies from the U.S. Europe, China, Japan, Korea, and India.

least 2022. In the interim, the continued exponential increase of connected devices will utilize 4G, 4G LTE, and 4G/5G hybrid infrastructures for internet connectivity.

Developing 5G Standards

5G standards have addressed known security vulnerabilities from previous wireless generations and enhanced security of 5G with home routing, encryption, and network slicing[xii]. As of June 2019, Release 15 standards for 5G have been completed. Release 16 standards are expected to be finalized in December 2019 at the earliest.[42,43] 5G evolution and standard development will continue after Release 16 is completed. Standards—led by 3GPP and ITU—determine technical specifications, including spectrum bands, radio interface technologies, network architecture, and network virtualization.[44,45]

In 2015, the ITU created the International Mobile Telecommunications 2020 (IMT-2020), which detailed technical standards such as minimum speed and use cases, and designated a timeline for 5G standards development (figure 3).[46,47] 3GPP is developing and will submit candidate technologies and specifications to the IMT-2020.[48] In December 2017, 3GPP ratified the Non-Standalone (NSA)[xiii] 5G New Radio (NR) specification, which enabled vendors to start building 5G components.[49] In June 2018, the Standalone (SA)[xiv] version was completed; 5G SA defines the control plane capabilities and user specifications for the new 5G core network architecture.[50] 3GPP is targeting their final submission to IMT-2020 for the end of 2019.[51] Figure four shows the 5G standards timeline for the ITU and 3GPP.[52,53,54]

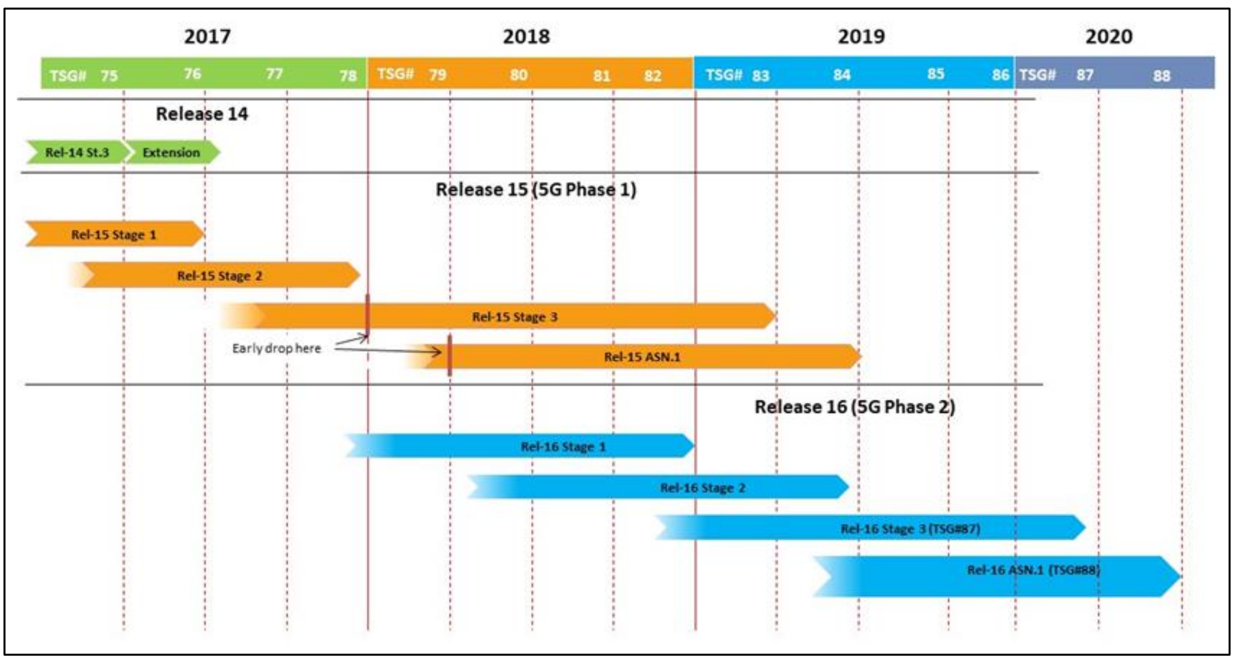

FIGURE 4—3GPP RELEASE TIMELINE AS OF JUNE 2019[55]

Federal Regulations and Activities

The Federal Communications Commission (FCC) is the U.S. Government agency that manages commercial spectrum usage.[56] The FCC has designated a large block of the underutilized high band spectrum for 5G and is auctioning 6,000 licenses in the 28 GHz and 24 GHz bands to communication companies.[57] The FCC has concluded its first high-band 5G spectrum auctions in both the 28GHz and 24GHz bands on May 28th, 2019.[58]

[xii] Network slicing will enable 5G networks to be segregated based on service or security requirements and will allow services to be created or deleted quickly.
[xiii] Non-Standalone Standards will allow devices to rest on the 4G network and will only jump up to 5G when the network is available.
[xiv] Standalone Standards will allow devices to rest on the 5G network and will only drop down when 5G is unavailable.

Additional auctions of different spectrum bands are planned for 2019. The FCC will make additional spectrum available for 5G services, to include:[59]

- **Low-band**: The FCC is acting to improve use of low-band spectrum (useful for wider coverage) for 5G services, with targeted changes to the 600 MHz, 800 MHz, and 900 MHz bands.
- **Mid-band**: Exploring, among other bands, a shared service framework in the 3.5 GHz band and developing next steps for terrestrial use in the 3.7 GHz band.
- **High-band**: Releasing spectrum at the frontiers of the spectrum chart, including spectrum auctions in the 24 and 28 GHz bands, and 2019 auctions planned in the 37, 39, and 47 GHz bands with additional bands still being explorer for potential terrestrial wireless use.[60]

A key venue for collaborative work between government and the private sector is the FCC's Communications Security, Reliability and Interoperability Council (CSRIC). The CSRIC is a federal advisory committee made up of members from both the private sector and government. Its mission is to provide recommendations to the FCC to ensure, among other things, security and reliability of communications systems, including telecommunications, media, and public safety. DHS participates in CSRIC efforts on cybersecurity and communications network security, complementing DHS' role as the sector-specific agency for the communications sector.

5G Deployment in the United States

As of June 2019, 5G networks and technologies are still in development and have rolled out on a limited basis in cities.[61] The full benefits of 5G may not be available during this initial deployment, either because users do not have 5G enabled devices that can use the 5G networks, or because there is inadequate base infrastructure for 5G enabled devices to access.[62]

One U.S. carrier deployed a fixed 5G network to four U.S. cities in October 2018, which will have the benefits of 5G signal but will not provide mobile access to a 5G network.[63] This home broadband service is a pre-standards deployment and does not meet the globally recognized 5G standard, although the company says it will adopt the industry standard in 2019 while it rolls out 5G mobile service for phones. A second U.S. carrier deployed a mobile 5G network in 12 U.S. cities in December 2018, although limited availability 5G mobile hotspots are the only devices capable of using the 5G network; 5G capable smartphones are expected to be available in 2019. Two additional U.S. carriers are targeting 2020 for full nationwide 5G coverage with limited rollouts beginning in 2019.[64,65] Many of these devices are enabled by a 5G modem developed by a leading U.S. chip manufacturer, which 18 international Original Equipment Manufacturer (OEM) companies and 19 wireless network operators have committed to using in trials.[66]

5G VULNERABILITIES

The move to 5G presents opportunities to enhance security and create a better user experience; however, it may result in vulnerabilities related to supply chains, deployment, network security, and the loss of competition and choice. While not all inclusive, there are a range of vulnerabilities that could increase risk for the United States as the country's networks migrate to 5G, including: reliance on untrusted entities and the global supply chain, lack of participation by untrusted companies in interoperability efforts, increased size of 5G infrastructure, integration within existing vulnerable networks, and untrusted company development of custom code for ICT components.

Supply Chain

USE OF 5G COMPONENTS MANUFACTURED BY UNTRUSTED COMPANIES COULD 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.

Though equipment designed and manufactured by trusted suppliers is not immune to manipulation, equipment produced or otherwise handled by untrusted partners presents more risk of malicious or inadvertent introduction of vulnerabilities. Counterfeit components and the insertion of malicious software and hardware are a few examples of such vulnerabilities. Even if ICT components are purchased from trusted companies, the company may maintain production facilities overseas which may be vulnerable to supply chain risk.

Compromised components could affect network performance and compromise the confidentiality, integrity, and availability of network assets. Furthermore, compromised devices may provide malicious actors with persistent access to 5G networks and the capability to intercept data that routes through the devices. Compromised devices may infect connected computers, phones, and other devices with malware and may have data rerouted, changed, or deleted.

Untrusted companies that have significant international market share within telecommunication networks may introduce risks even if they do not have a large presence within the U.S networks. Therefore, even if the U.S. network were completely secure, data traveling overseas may pass through untrusted telecommunication networks and potentially be vulnerable to interception, manipulation, disruption, or destruction.

Network Security

DESPITE SECURITY ENHANCEMENT OVER PREVIOUS GENERATIONS, IT IS UNKNOWN WHAT NEW VULNERABILITIES MAY BE DISCOVERED IN 5G NETWORKS.

Component manufacturers and service providers are developing technologies and security specifications to mitigate vulnerabilities in wireless networks. 5G will push ICT components and data management to the edge of the network, which will enhance security through network slicing, edge computing power, device management, authentication functions, and automated threat detection and response. Network slicing, if implemented properly, should limit an attacker's ability to access critical areas within a network. The migration of functions to the edge of the network will increase computing and network management power, which will secure traffic and prevent intrusions to core network systems.

Despite 5G's security improvements, as with all new technologies it is likely that 5G equipment and protocols will inadvertently contain vulnerabilities that could expose components and data to exploitation. 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. Therefore any vulnerabilities inherent in 5G technologies may be exploitable even after fixes are developed.

5G BUILDS UPON PREVIOUS GENERATIONS OF WIRELESS NETWORKS AND WILL INITIALLY BE INTEGRATED WITH 4G LTE NETWORKS THAT CONTAIN SOME LEGACY VULNERABILITIES, POTENTIALLY INCLUDING UNTRUSTED COMPONENTS.

5G network technologies are being designed to be more secure than previous mobile network generations, and organizations and standard bodies continue to enhance security in previous wireless networks, including protecting core networking systems from malicious edge networking devices. 5G technologies will, however, initially be overlaid on the existing 4G Long-Term Evolution (LTE) network that contains legacy vulnerabilities. These could be inadvertent, technical vulnerabilities inherent to the network, or due to 5G technologies' integration into untrusted 4G and 4G LTE networks. The inheritance of security settings, permissions, and technical specifications from an untrusted core network may negate built-in 5G device security.

5G Deployment

THE PROLIFERATION OF 5G NETWORKS COULD PROVIDE MALICIOUS ACTORS MORE ATTACK VECTORS TO INTERCEPT, MANIPULATE, DISRUPT, AND DESTROY CRITICAL DATA.

5G will use more components than previous generations of wireless networks and malicious actors may have addtional vectors to intercept, manipulate, disrupt, and destroy critical data. This infrastructure will likely include, but is not limited to cellular towers, beamforming, small cells, and mobile devices.

Unlike traditional cellular towers, small cells will be densely deployed in metropolitan areas, residing on light poles, trees, homes, building corners, and retail shops.[67] Although small cells are designed with physical security features, they still could be compromised through physical access. This may provide malicious actors with persistent illicit access to the 5G network, the ability to intercept data routed through the device, and an avenue to conduct Denial of Service (DOS) attacks on devices communicating with that small cell. Compromised small cells may also provide malicious actors the capability to clone devices, allowing the replica to make calls, use data, and add charges.

While the use of small cells for information extraction or disruption is possible, the use of such a method would likely require a high level of sophistication and is unlikely to provide access to large volumes of data. As of June 2019, there are no confirmed incidents utilizing 5G small cells to exploit wireless systems, however, researchers have demonstrated this capability with small cells in a 4G wireless system.

- In 2013, a pair of security researchers detailed their ability to use a small cell to intercept voice calls, data, and SMS text messages of any handset that connects to the device. The security researchers also demonstrated the ability to clone a cell phone, allowing hackers to impersonate the device to make calls, send texts, and use data.[68]

THE EFFECTIVENESS OF 5G SECURITY ENHANCEMENTS WILL IN PART DEPEND ON PROPER IMPLEMENTATION AND CONFIGURATION.

Advanced security features in 5G protocols and technologies will improve communications security but will require proper configuration and implementation. As municipalities, companies, and organizations build their own local 5G networks, it is possible they will not properly implement 5G network security. Improperly deployed, configured, or managed 5G equipment and networks may be vulnerable to interception, disruption, and manipulation.

Loss of Competition and Trusted Options

UNTRUSTED COMPANIES MAY BE LESS LIKELY TO PARTICIPATE IN INTEROPERABILITY EFFORTS, POTENTIALLY MAKING IT DIFFICULT FOR TRUSTED COMPANIES TO COMPETE AND LIMITING THE AVAILABILITY OF TRUSTED COMMUNICATIONS TECHNOLOGIES.

Section 889 of the 2019 National Defense Authorization Act (NDAA) prohibits federal agencies from procuring certain equipment and services from Huawei and ZTE, two of the world’s largest manufacturers of telecommunications equipment.[69] Although limited in their share of the U.S. telecommunications market, these companies have significant market share internationally and may be less likely to participate in interoperability efforts. This is evidenced by the lack of involvement in the O-RAN Alliance, a collection of telecommunication organizations that work towards open and interoperable architectures.[70]

Communication network operators that previously purchased 4G equipment from a company like Huawei that uses proprietary interfaces in their technologies cannot easily use other vendors’ equipment for 5G. The proprietary interfaces lock customers into a single vendor procurement cycle, which could negatively affect competitive balance within the 5G market. Loss of market share could limit trusted companies’ ability to invest in research and development and could eventually drive them out of the market. Loss of trusted suppliers could potentially lead to a situation where untrusted entities are the only options.

CUSTOM 5G TECHNOLOGIES THAT DO NOT MEET INTEROPERABILITY STANDARDS MAY BE MORE DIFFICULT TO UPDATE AND REPAIR, POTENTIALLY INCREASING THE LIFECYCLE COST OF THE PRODUCT.

Custom 5G equipment, that does not meet interoperability standards, may be more difficult to update and repair. Poorly developed code makes vulnerability management significantly more difficult and can lead to unsupportable software. If a critical outage occurs, systems, programs, and data with custom code are more difficult to recover and may lead to extended outage times.

Slowing or blocking interoperability between networks could also substantially delay or increase the cost of deploying 5G. A customer currently using Huawei equipment who wants to use a new vendor for 5G may have to first remove and replace all their equipment from the network.

Huawei Cyber Security Evaluation Centre (HCSEC) Oversight Board Annual Report

On March 28, 2019, the British National Cyber Security Centre (NCSC) released an assessment on the security risks posed by Huawei. The report identified "significant, concerning issues in Huawei's approach to software development, which brings significantly increased risk to UK operators, and requires ongoing management and mitigation." The report also states that "The Oversight Board continues to be able to provide only limited assurance that the long-term security risks can be managed in the Huawei equipment currently deployed in the UK."

NATIONAL OPPORTUNITIES TO MITIGATE 5G RISK

With the above in mind, there is an opportunity for the U.S. government and industry to work together to maximize the benefits of next generation communication networks and to promote security and resilience associated with emerging 5G technologies. Given the expected rollout schedule, 2019 presents a window of time in which the United States and allied countries can advance risk mitigation efforts that may be more difficult to address as the deployment of 5G networks advance. The below presents a range of opportunities at the strategic level. Follow on efforts and discussions are necessary to expand on specific potential actions.

Encouraging continued trusted development of 5G technologies, services, and products

Reliance on untrusted 5G technologies is likely, in part, because of relatively low costs. Additionally, if untrusted companies' equipment is already installed as part of the 4G LTE network, lack of interoperability may make it impossible to install other companies' 5G equipment without replacing the existing 4G LTE equipment, which may be extremely costly. National investment in research and development, economic incentives for manufacturing and buying trusted components, or economic deterrents for purchasing and installing untrusted components, could increase trusted production and lower the risks of malicious untrusted technologies.

Encouraging continued trusted development of the next generations of communications technologies

Next generation communication technologies and standards will build upon themselves over time and security enhancements will continue for 5G into the future. This development will occur in individual companies and in standards bodies as markets for new services take shape, but the United States can encourage and investin in such development. This will likely position the United States to be a leading player in their rollout, potentially decreasing the influence of adversarial nations and decreasing U.S. reliance on untrusted technologies.

Promoting international standards and processes that are open, transparent, and consensus-driven and that do not place trusted companies at a disadvantage

The ITU and 3GPP both have U.S. members, including the director of ITU's Telecommunication Development Bureau, one of ITU's five top elected officials serving 2019-2022.[71] Members of the two groups representing trusted suppliers' interests can promote standards that are currently being adopted and collaborate on their development. The United States could also work at achieving greater representation in the ITU, 3GPP, and other standard organizations.

Limiting the use of 5G equipment with known or suspected vulnerabilities

The United States can take action to limit the adoption of 5G equipment that may contain vulnerabilities. For example, Section 889 of the 2019 NDAA prohibits federal agencies from procuring certain telecommunications equipment and services. The recently enacted Federal Acquisition Supply Chain Security Act provides the government with important new authorities. These authorities address risks presented by the purchase of technologies developed or supplied by entities whose manufacturing and development processes, obligations to foreign governments, and other factors raise supply chain concerns.[72] In May 2019, the President also issued an Executive Order on Securing the Information and Communications Technology and Services Supply Chain, which authorizes the Secretary of Commerce, in consultation with other agencies, to issue regulations to address the installation and use of information and communications technology and services, by any person subject to the jurisdiction of the United States, that present security risks. The United States can help secure its overseas communications by working with international partners to limit the installation of untrusted equipment abroad. The United States can also promulgate and promote technical best practices for mitigating aspects of 5G risk.

Continued engagement with the private sector on risk identification and mitigation efforts

The U.S. Government can continue to work with the private sector—to include information and communication technology providers—to help mitigate vulnerabilities. The private sector can provide insights on where government support or intervention—such as through the development of best practices, the convening of industry and government partners, and the prohibition on untrusted equipment—will help secure 5G technologies and the 5G network.

Ensure robust security capabilities for 5G applications and services

The U.S. Government and industry partners can develop security capabilities that protect not only the 5G infrastructure, but also the applications and services that utilize it. The U.S. Government can do this by incorporating a prevention-focused approach that focuses on visibility and security across the mobile network. Secure 5G applications and services will likely mitigate the risk of malware being transported across protected devices and defend against unauthorized command and control from exploited connected devices. The U.S. Government and its industry partners can also encourage secure infrastructure to guard against these threats and mitigate lateral threat movement within the 5G network.

GLOSSARY OF TERMS

TERM	DESCRIPTION
3rd Generation Partnership Project (3GPP)	3GPP is an industry based, multi-national technical organization made up of approximately 500 companies and government agencies from the U.S. Europe, China, Japan, Korea, and India.
Baseband Unit Pool (BBU)	BBUs are the baseband processing units within telecom systems that comprise cloud radio access networks (C-RAN). BBUs are located at centralized sites and function as a cloud or a data center.
Beamforming	Beamforming is a radio frequency management function in which radio access locations use multiple antennas to focuses radio signals in a specific direction. This enhances the uplink and downlink capabilities as well as the overall network capacity of the signal.
Communications Security, Reliability and Interoperability Council (CSRIC)	CSRIC is a joint federal and industry partnership that aims to provide recommendations to the FCC to ensure, among other things, optimal security and reliability of communications systems, including telecommunications, media, and public safety.
Device-To-Device (D2D)	D2D is a communication technology that enables direct data transfer between nearby mobile devices in an ad-hoc network. Devices would act as data transfer points, relaying data between end users, small cells, and base stations.[73]
Internet of Things (IoT)	The connection of systems and devices with primarily physical purposes (e.g., sensing, heating and cooling, lighting, motor actuation, transportation) to information networks (including the Internet) via interoperable protocols, often built into embedded systems
International Telecommunications Union (ITU)	A United Nations agency responsible for information and communication technologies. It allocates radio spectrum and develops global technical standards.
Latency	The delay in transmitting and processing data, such as the delay between when a command is sent and when it is executed.
Macro Cell	Macro cell towers reside on a base station and deliver wireless radio signal in a large geographic area. 5G macro cells will operate in similar frequency bands as 4G Long-Term Evolution (LTE).
Machine-To-Machine (M2M)	M2M communication occurs between two directly connected machines without human interference. M2M will support 5G use cases; including the large number of low-cost/low-energy IoT devices, as well as enabling critical machine type communications in smart factory, automotive, and e-health systems.
Massive MIMO (Multiple-Input, Multiple-Output)	Massive MIMO technology increases the capabilities of wireless internet by putting significantly more antennae on a base station. 4G base stations have twelve antennae, whereas 5G massive MIMO base stations can support an estimated one hundred antennae, increasing capacity of mobile networks by a factor of 22 or greater.[74]

Mobile Backhaul	Mobile Backhaul is the back-end part of a cellular network that connects the edge or fronthaul networks to the core network via fiber optic cables.
Mobile Fronthaul	Mobile Fronthaul is the front-end or edge interfacing portion of the cellular network that connects the radio access network to the mobile backhaul network via fiber optic cables.
Small Cell/Micro Cell	A small cell is miniature base station that transmits short-range radio signals. Due to the limited range and non-penetrative signal of high frequency radio wave bands, 5G will require numerous small cells to support its infrastructure. Together, these cells would form a dense network that relays data through multiple small cells.[75]
Vehicle-To-Everything (V2X)	Similar to D2D, V2X is a communication technology in which vehicles act as data relay points between 5G enabled vehicles, end-user devices, and smart city components like smart sensors or meters.
Wave Penetration	The ability to pass through materials, such as walls. Waves at low-band frequencies are generally penetrative, while higher frequency waves are often unable to pass through materials, including walls and other building materials.

The National Risk Management Center (NRMC), Cybersecurity and Information Security Agency (CISA), is the planning, analysis, and collaboration center working in close coordination with the critical infrastructure community to Identify; Analyze; Prioritize; and Manage the most strategic risks to National Critical Functions. These are the functions of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating impact on security, national economic security, national public health or safety, or any combination thereof. All NRMC products are visible to authorized users at HSIN-CI and Intelink. For more information, contact NRMC@hq.dhs.gov or visit https://www.dhs.gov/cisa/national-risk-management-center.

[1] Segan, S. (2015). “3G vs. 4G: What’s the Difference?” PC Mag. https://www.pcmag.com/article2/0,2817,2399984,00.asp. Accessed on June 5, 2019.
[2] Sharma, P. (2013). “Evolution of Mobile Wireless CommunicationNetworks-1G to 5G as well as Future Prospective of Next Generation Communication Network.” International Journal of Computer Science and Mobile Computing.
[3] Rouse, M. (2009). “3G (third generation of mobile telephony).” Tech Target. https://searchtelecom.techtarget.com/definition/3G. Accessed on June 5, 2019.
[4] Thangham, Chris. (2008). “New Apple iPhone will have 3G, GPS, Video Conferencing, Live TV, more memory, colors.” Digital Journal. http://www.digitaljournal.com/article/254685. Accessed on June 5, 2019.
[5] Granados, N. (2017) “5G: The Next Tech Disruption In Media And Entertainment Is Coming.” Forbes. https://www.forbes.com/sites/nelsongranados/2017/07/17/5g-the-next-tech-disruption-in-media-and-entertainment-is-coming/#4bc886037026. Accessed on June 5, 2019.
[6] Nperf. (2018). “2G/3G/4G coverage map, United States.” https://www.nperf.com/en/map/US/-/-/signal/. Accessed on June 5, 2019.
[7] Segan, S. (2018). “Fastest Mobile Networks 2018.” PC Mag. https://www.pcmag.com/Fastest-Mobile-Networks/4. Accessed on June 5, 2019.
[8] Segan, S. (2015). “3G vs. 4G: What’s the Difference?” PC Mag. https://www.pcmag.com/article2/0,2817,2399984,00.asp. Accessed on June 5, 2019.
[9] Fisher, T. (2018). “How are 4G and 5G Different?” Lifewire. https://www.lifewire.com/5g-vs-4g-4156322. Accessed on June 5, 2019.
[10] Phone Arena. (2013). “1G, 2G, 3G, 4G: The evolution of wireless generations.” https://www.phonearena.com/news/1G-2G-3G-4G-The-evolution-of-wireless-generations_id46952. Accessed on June 5, 2019.
[11] Grigorik, I. (2013). “High Performance Browser Networking.” https://hpbn.co/#toc. Accessed on June 5, 2019.
[12] Intel. (2014) “The Evolution of Wireless Technology.” http://download.intel.com/newsroom/kits/atom/comms/pdfs/Final-EvolutionOfWireless.pdf. p. 1. Accessed on June 5, 2019.

[13] Downes, L. (2018). “5G: What is it good for?” Washington Post. https://www.washingtonpost.com/news/innovations/wp/2018/06/05/5g-what-is-it-good-for/?utm_term=.681b76b740ff. Accessed on June 5, 2019.
[14] Wired. (2018). “What is 5G, and When Do I Get it?” https://www.wired.com/2017/02/what-is-5g-and-when-do-i-get-it/. Accessed on June 5, 2019.
[15] Garcia, A. (2019). “Looking for 5G? Here are the US Cities that have it.” https://www.cnn.com/2019/04/09/tech/5g-network-us-cities/index.html. Accessed on June 4, 2019.
[16] Blumenthal, Eli. (2018). “AT&T turns on its mobile 5G network on Dec. 21, starting with 12 cities and mobile hotspot.” USA Today. https://www.usatoday.com/story/tech/2018/12/18/att-opens-its-5-g-network-december-21-starting-12-cities/2339042002/. Accessed June 5, 2019.
[17] Greenemeier, L. (2015). “Will Millimeter Waves Maximize 5G Wireless?” Scientific American. https://www.scientificamerican.com/article/will-millimeter-waves-maximize-5g-wireless/. Accessed June 5, 2019.
[18] Valdez, D. (2019). “5G expected to ease network congestion.” Business World. https://www.bworldonline.com/5g-expected-to-ease-network-congestion/. Accessed on June 4, 2019.
[19] Moorhead, Patrick (2016) “Qualcomm Demonstrates First Sub-6 GHz 5G New Radio Prototype At MWC Shanghai 2016” https://www.forbes.com/sites/patrickmoorhead/2016/06/26/qualcomm-demonstrates-first-sub-6-ghz-5g-new-radio-prototype-at-mwc-shanghai-2016/#7a8b45fd194b. Accessed on June 12, 2019.
[20] FCC. (2018). “The FCC's 5G FAST Plan.” https://www.fcc.gov/5G. Accessed on June 5, 2019.
[21] Nordrum, A, Clark, K. (2018). “5G Bytes: Small Cells Explained.” IEEE. https://spectrum.ieee.org/video/telecom/wireless/5g-bytes-small-cells-explained. Accessed on June 5, 2019.
[22] Ibid.
[23] Infineon (2017) “Infineon RF solutions for fast, efficient and reliable 5G” https://www.infineon.com/cms/en/about-infineon/press/market-news/2017/INFPMM201702-034.html. Accessed on June 12, 2019.
[24] Athow, D. (2018). “5G to Open Up New Healthcare Possibilities.” Tech Radar. https://www.techradar.com/news/5g-to-open-up-new-healthcare-possibilities. Accessed on June 5, 2019.
[25] Electric Light & Power. (2017) “5G Communication to Enhance Power Grid Networking.” Electric Light & Power. https://www.elp.com/articles/2017/12/5g-communications-to-enhance-power-grid-networking.html. Accessed on June 5, 2019.
[26] Nichols, M. (2017). “Why 5G Will Disrupt the Robotics and Manufacturing Industries?” Robotics Business Review. https://www.roboticsbusinessreview.com/manufacturing/will-5g-disrupt-robotics-manufacturing-industries/. Accessed on June 5, 2019.
[27] 3GPP (2016). “SA1 Completes its study into 5G requirements.” 3GPP. http://www.3gpp.org/news-events/3gpp-news/1786-5g_reqs_sa1. Accessed on June 5, 2019.
[28] Sagam, P. (2018). “What is the killer use case for 5G?” Forbes. https://www.forbes.com/sites/forbescommunicationscouncil/2018/06/04/what-is-the-killer-use-case-for-5g/. Accessed on June 5, 2019.
[29] Kavanagh, S. (2018). “What is enhanced Mobile Broadband (eMBB).” 5G.CO.UK. https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/. Accessed on June 5, 2019.
[30] Kavanagh, S. (2018). “What is enhanced Mobile Broadband (eMBB).” 5G.CO.UK. https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/. Accessed on June 5, 2019.
[31] Wang, B. (2015). “5G network defined by ITU as 20 GBs per second.” Next Big Future. https://www.nextbigfuture.com/2015/06/5g-network-defined-by-itu-as-20-gbs-per.html. Accessed on June 5, 2019.
[32] Kavanagh, S. (2018). “What is enhanced Mobile Broadband (eMBB).” 5G.CO.UK. https://5g.co.uk/guides/what-is-enhanced-mobile-broadband-embb/. Accessed on June 5, 2019.
[33] Layton, R. (2018). “The U.S. Must Move Quickly On Mid-Band Spectrum If It Wants To Lead In 5G.” Forbes. https://www.forbes.com/sites/roslynlayton/2018/05/23/the-us-must-move-quickly-on-mid-band-spectrum-if-it-wants-to-lead-in-5g/#fb740c67462a. Accessed on June 5, 2019.
[34] Popovski, P. Nielsen, J.Stefanovic, C. Carvalho, E.Stro¨my, E. Trillingsgaard, K. Bana, A. Kim, D. Kotaba, R. Park, J. Sørensen, R. “Wireless Access for Ultra-Reliable Low-Latency Communication (URLLC): Principles and Building Blocks.” https://arxiv.org/pdf/1708.07862.pdf. p. 1. Accessed on June 5, 2019.
[35] Fulton, S. (2018). “What is 5G? The definitive guide to next generation wireless technology.” ZDNet. https://www.zdnet.com/article/what-is-5g-everything-you-need-to-know/. Accessed on June 5, 2019.
[36] McLaughlin, R. (2019). “5G Low Latency Requirements”. Broadband Library. https://broadbandlibrary.com/5g-low-latency-requirements/. Accessed on June 5, 2019.
[37] Brodkin, J. (2018). “AT&T’s 5G trials produce gigabit speeds and 9ms latency.” Arstechnica. https://arstechnica.com/information-technology/2018/04/atts-5g-trials-produce-gigabit-speeds-and-9ms-latency/. Accessed on June 5, 2019.
[38] Small Cell Forum. (2018). “MMwave small cells boost capacity tenfold, but where are the use cases?” https://www.smallcellforum.org/blog/mmwave-small-cells-boost-capacity-tenfold-use-cases/. Accessed on June 5, 2019.
[39] Bockelmann, C. Pratas, N. Nikopour, H. Au, K. Svensson, T. Stefanovic, C. Popovski, P. Dekorsy, A. (2017). “Massive Machine-type Communications in 5G.” https://arxiv.org/ftp/arxiv/papers/1606/1606.03893.pdf. pp.1-2. Accessed on June 5, 2019.
[40] McGarry, C. (2019). “The Truth About 5G: What’s Coming (and What’s Not) in 2019”. Tom’s Guide. https://www.tomsguide.com/us/5g-release-date,review-5063.html. Accessed on June 5, 2019.
[41] Jones, Dan. (2019). “A 5G Device Timeline for 2018 & Beyond” https://www.lightreading.com/mobile/5g/a-5g-device-timeline-for-2018-and-beyond/d/d-id/745191. Accessed on June 5, 2019.
[42] 3GPP. (2019). “Release 15”. 3GPP. https://www.3gpp.org/release-15. Accessed on June 5, 2019.
[43] 3GPP. (2018). “Release 16”. 3GPP. https://www.3gpp.org/release-16. Accessed on June 5, 2019.
[44] 3GPP. (2016). “3GPP on Track to 5G.” http://www.3gpp.org/news-events/3gpp-news/1787-ontrack_5g. Accessed on July 5, 2018.
[45] Gutierrez, P. Haeffner, W. (2017). “Service Function Chaining Dataplane Elements in Mobile Networks.” IETF. https://tools.ietf.org/id/draft-aranda-sfc-dp-mobile-03.txt. Accessed on June 5, 2019.
[46] Blanchard, N. (2017). “How ITU, 5GPPP, NGMN and others will create the standard for 5G.” Fierce Wireless. https://www.fiercewireless.com/special-report/how-itu-5gppp-ngmn-and-others-will-create-standard-for-5g. Accessed on June 5, 2019.
[47] ITU-R. (2015). “IMT Vision – Framework and overall objectives of the future development of IMT for 2020 and beyond.” https://www.itu.int/dms_pubrec/itu-r/rec/m/R-REC-M.2083-0-201509-I!!PDF-E.pdf. p. 4-21. Accessed on June 5, 2019.
[48] Flore, D. (2015). “Tentative 3GPP timeline for 5G.” 3GPP. http://www.3gpp.org/news-events/3gpp-news/1674-timeline_5g. Accessed on June 5, 2019.
[49] Alleven, M. (2017). “3GPP declares first 5G NR spec complete.” Fierce Wireless. https://www.fiercewireless.com/wireless/3gpp-declares-first-5g-nr-spec-complete. Accessed on June 5, 2019.

[50] 3GPP. (2018). “Rel-15 success spans 3GPP groups.” http://www.3gpp.org/news-events/3gpp-news/1965-rel-15_news. Accessed on June 5, 2019.
[51] 3GPP. (2018). “Release 16.” http://www.3gpp.org/release-16. Accessed on June 5, 2019.
[52] Flore, D. (2015). “Tentative 3GPP timeline for 5G.” http://www.3gpp.org/news-events/3gpp-news/1674-timeline_5g. Accessed on June 5, 2019.
[53] Johnson, D. (2018). “5G Poised for Commercial Rollout by 2020.” IEEE. https://spectrum.ieee.org/tech-talk/telecom/wireless/5g-is-meeting-its-targets-for-2020-commercial-rollout. Accessed on June 5, 2019.
[54] SDX Central. “5G Standards: What You Need to Know.” SDX Central. https://www.sdxcentral.com/5g/definitions/5g-standards/. Accessed on June 5, 2019.
[55] Netmanis (2017) “Timeline of 5G in ITU-R and 3GPP” https://www.netmanias.com/en/post/oneshot/11147/5g/timeline-of-5g-standardization-in-itu-r-and-3gpp. Accessed June 4, 2019.
[56] FCC (2019). “Radio Spectrum Allocation.” FCC. https://www.fcc.gov/engineering-technology/policy-and-rules-division/general/radio-spectrum-allocation. Accessed on June 4, 2019.
[57] FCC. (2018). “FCC Public notice” FCC. https://docs.fcc.gov/public/attachments/FCC-18-109A1_Rcd.pdf/. Accessed on June 4, 2019.
[58] FCC. (2018). “”FCC concludes first High-Band 5G Airwaves Auctions”. FCC. https://docs.fcc.gov/public/attachments/DOC-357702A1.pdf. Accessed on June 4, 2019.
[59] FCC. (2018). “The FCC's 5G FAST Plan.” https://www.fcc.gov/5G. Accessed on June 5, 2019.
[60] FCC. (2018). “FCC’s First-Ever High-Band 5G Spectrum Auction Begins Today.” https://docs.fcc.gov/public/attachments/DOC-355073A1.pdf. Accessed June 5, 2019.
[61] Blumenthal, Eli. (2018). “AT&T turns on its mobile 5G network on Dec. 21, starting with 12 cities and mobile hotspot.” USA Today. https://www.usatoday.com/story/tech/2018/12/18/att-opens-its-5-g-network-december-21-starting-12-cities/2339042002/. Accessed June 5, 2019.
[62] McGarry, C. (2018). “The Truth About 5G: What's Coming (and What's Not) in 2018.” Tom’s Guide. https://www.tomsguide.com/us/5g-release-date,review-5063.html. Accessed on June 5, 2019.
[63] Ibid
[64] AT&T. (2018). “AT&T First to Make Mobile 5G Service Live in the U.S. on Dec. 21.” AT&T. https://about.att.com/story/2018/att_brings_5g_service_to_us.html. Accessed June 5, 2019.
[65] Cheng, R. (2018). “Sprint targets first mobile 5G nationwide network by early 2019.” CNet https://www.cnet.com/news/sprint-targets-first-mobile-5g-nationwide-network-by-early-2019/. Accessed on June 5, 2019.
[66] Michaels, P. (2018). “Qualcomm's Blazing 5G Modem Coming to Phones in 2019.” Tom’s Guide. https://www.tomsguide.com/us/qualcomm-x50-5g-modem,news-26584.html. Accessed on June 5, 2019.
[67] Wall, M. (2018). “What is 5G and what will it mean for you?” BBC. https://www.bbc.com/news/business-44871448. Accessed on June 5, 2019.
[68] Couts, A. (2013). “Meet the $250 Verizon device that lets hackers take over your phone.” Digital Trends. https://www.digitaltrends.com/mobile/femtocell-verizon-hack/. Accessed on June 5, 2019.
[69] 115th Congress. (2017). “H.R.2810 - National Defense Authorization Act for Fiscal Year 2018.” https://www.congress.gov/bill/115th-congress/house-bill/2810/text. Accessed on June 5, 2019.
[70] O-RAN Alliance (2019). “Operator Defined Next Generation RAN Architecture and Interfaces”. ORAN. https://www.o-ran.org/. Accessed on June 5, 2019.
[71] ITU. (2019). “ITU Management Team 2019-2022.” https://www.itu.int/en/osg/Pages/itu-management-team.aspx. Accessed on June 5, 2019.
[72] 115th Congress. (2017). “H.R.2810 - National Defense Authorization Act for Fiscal Year 2018.” https://www.congress.gov/bill/115th-congress/house-bill/2810/text. Accessed on June 5, 2019.
[73] IEEE Spectrum. (2018). “Applications of Device-to-Device Communication in 5G Networks.” https://spectrum.ieee.org/computing/networks/applications-of-devicetodevice-communication-in-5g-networks. Accessed on June 5, 2019.
[74] Ibid.
[75] Nordrum, A, Clark, K. (2018). “5G Bytes: Small Cells Explained.” IEEE. https://spectrum.ieee.org/video/telecom/wireless/5g-bytes-small-cells-explained. Accessed on June 5, 2019.