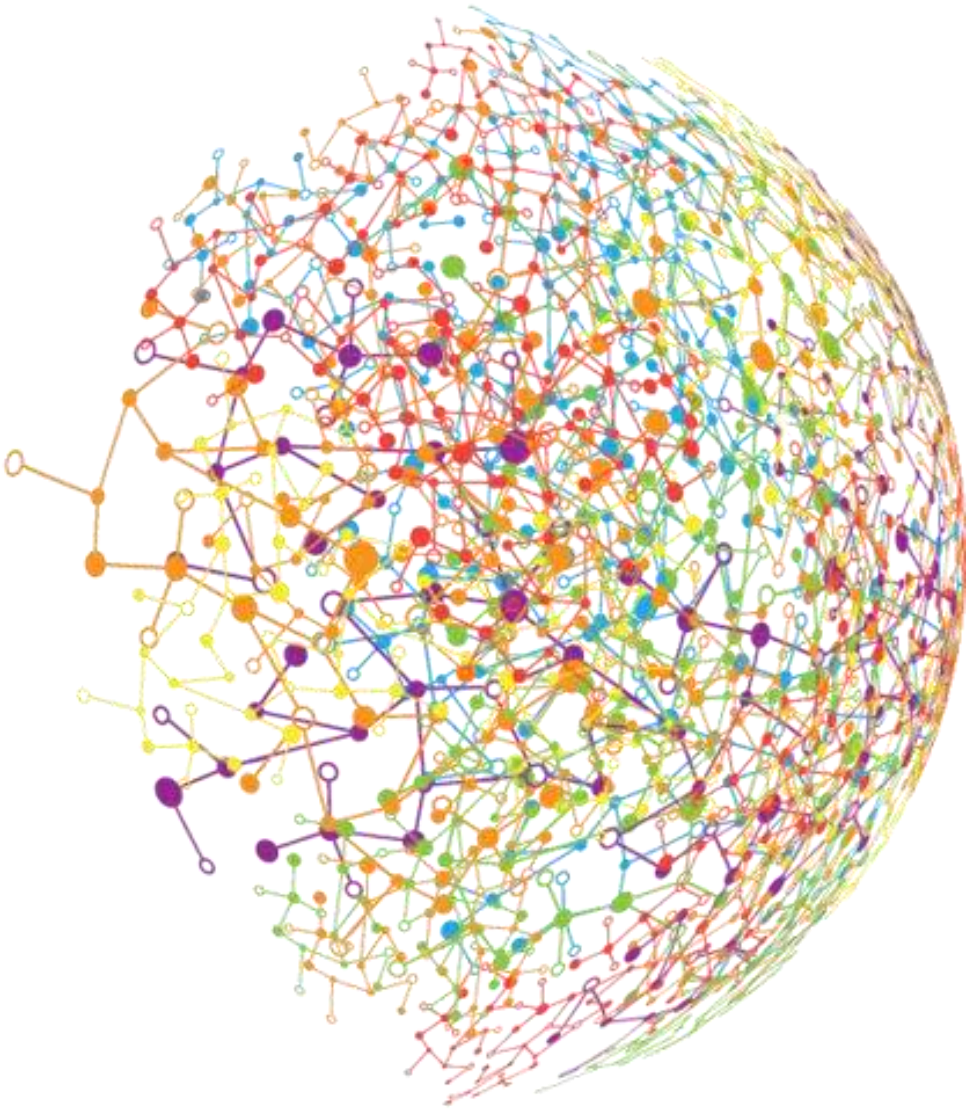
Homeland Security

Science and Technology



5G: The Telecommunications Horizon and Homeland Security

December 2021

Homeland Security
Science and Technology

Contents

Source: Shutterstock

Executive Summary

This horizon scanning report provides information and insight into the future of fifth generation (5G) and sixth generation (6G) networking technologies and the associated impacts to the Homeland Security Enterprise (HSE). The measures taken by the Department of Homeland Security (DHS) to manage and secure its networks will require continued adaptation as 5G, and subsequently 6G, standards shape the information and communications technology (ICT) environment. DHS will also be able to capitalize on new opportunities that leverage 5G and 6G communication technologies. This horizon scan provides a primer on the current state of 5G technology, reviews the expected development of 5G and 6G capabilities, and details relevant implications for DHS and the HSE.

The 5G standard began global deployment in 2019 and offers increased data transmission speed, decreased latency, improved reliability, and expanded capacity relative to previous standards (i.e. 4G, 3G, etc.). 5G achieves these capabilities by utilizing new protocols and a larger portion of the radio spectrum across an increased number of network components. These attributes make 5G suited for applications requiring mission-critical connectivity and/or very large numbers of network connections, such as autonomous vehicle operations and Internet of Things (IoT) devices. DHS and the US federal government have a critical role in shaping the development of 5G, and cooperation with telecommunication companies, hardware manufacturers, and global regulatory bodies enables efforts to define evolving standards for 5G and 6G.

The future of the ICT environment will continue to evolve over the next decade with 5G Advanced and 6G as countries actively deploy 5G network infrastructure. 5G Advanced is a planned set of technology and network upgrades that is expected to be deployed by 2025 and will expand on existing 5G capabilities with upgrades like intelligent network management. 6G is expected to begin deployment by 2030, and notable differentiators from 5G include enhanced scalability, greater use of the radio spectrum, and dynamic access to different connection types such as Wi-Fi and cellular networks.

The continued development of 5G and 6G introduces both opportunities to enhance mission capabilities as well as associated risks for the HSE, and there are present uncertainties related to these technologies that requires proactive actions to be taken by DHS. New and enhanced DHS capabilities supported by 5G and 6G infrastructure include the IoT, autonomous vehicles, and advanced sensor devices. Associated with these benefits are risks stemming from ICT component supply chain vulnerabilities, an increased network attack surface, and increasing reliance of mission critical services supported by 5G and 6G infrastructure. The future of 5G/6G network resiliency and 6G standards development is currently uncertain, and both of these factors face multiple potential scenarios that will be important for DHS to monitor to inform future decision-making.

The development of 5G and 6G capabilities is changing how companies, citizens, and governments interact with network technologies. Proactive engagement by DHS and the broader US government is critical to ensure that these technologies are shaped to best serve and safeguard the interests of the American people.

Introduction

"By 2025, 5G networks are likely to cover one-third of the world's population." – Global System for Mobile Communications Association

Discussion of the 5G technology standard for cellular networks has become ubiquitous in think pieces, industry marketing, and everyday lexicon. 5G is understood as the next major step forward in global connectivity by expanding capabilities like mobile broadband service, autonomous vehicles, and "smart" components of the IoT.

While the full utility of the changes enabled by 5G will not be realized for several years, firms are rolling out 5G hardware and mobile carriers continue to upgrade their networks. 5G promises faster speeds and better connectivity, with the most significant impacts of the network transformation expected in novel applications across emerging industries.

It is important for private and public sector organizations to understand the technology underpinning 5G networks and the devices that will operate on them as the 5G rollout continues. This document explores the fundamentals of 5G protocols and technologies and examines the benefits and drawbacks enabled by their capabilities. This primer includes an outlook of 5G deployment, future technology developments, and impacts to national security and the broader HSE.

Understanding 5G

The 5G Standard

5G is the fifth-generation standard for cellular networks, developed by the 3rd Generation Partnership Project (3GPP) in 2016. 3GPP is an international consortium of standards organizations and industry groups that developed earlier 4G and 3G standards. The 5G standard began global deployment in 2019, with increases in data transmission speeds and capacities over previous standards. 5G utilizes new protocols and a larger portion of the radio spectrum across more network components.

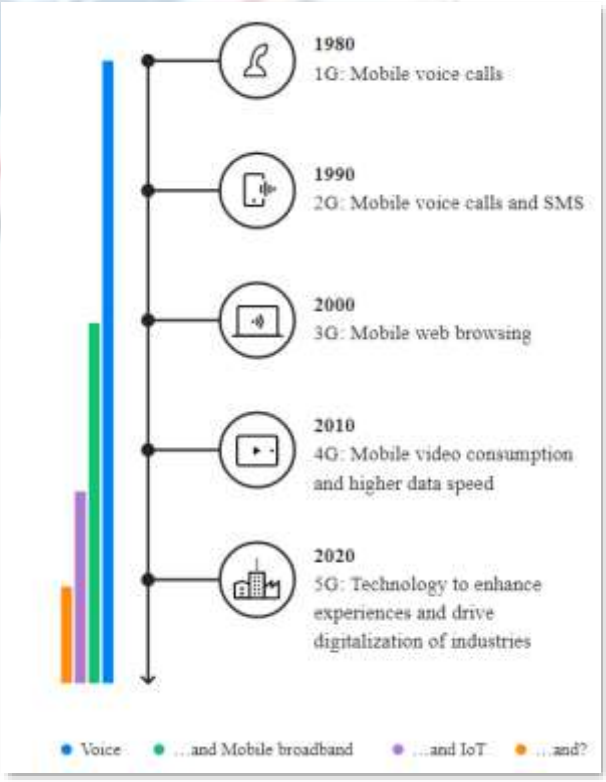


Figure 1: Wireless Standard Timeline (Courtesy of Ericsson)

First generation cellular technologies were analogue, while 2G enabled digital transmission over Code Division Multiple Access (CDMA), Global System for Mobiles (GSM), and Time Division Multiple Access (TDMA) methods and standards. 3G facilitated an increase in mobile internet usage through increased speed. 4G technologies like Worldwide Interoperability for Microwave Access (WiMAX) and Long-Term Evolution (LTE) offered increased data speeds and capacities. These enabled the growth of new categories of businesses and technologies not feasible given the constraints of earlier network capabilities, such as Uber,

TikTok, and mobile video chat.[1] 5G is designed to enable additional changes for emerging technologies like driverless vehicles, delivery robots, and smart infrastructure through further increases in speed, capacity, and reliability and reductions in latency.

The 5G protocol does not restrict transmission to any single frequency of the electromagnetic spectrum. Rather, 5G introduces wider channels across existing telecommunications frequencies and some previously unused parts of the spectrum. In practice, 5G networks will generally operate in three frequency bands: low, middle (Sub-6GHz), and high. Low-band 5G operates at frequencies below 2GHz, which are shared with the oldest cellular and TV frequencies. These frequencies have long ranges and can more easily penetrate obstacles like buildings, but there are only limited and narrow channels available. Mid-band 5G is between 2 and 10GHz and covers most existing cellular and Wi-Fi frequencies. The majority of 5G traffic will be mid-band, as it enables sufficient range and channel space.

High band frequencies are located in the previously unused 20-100GHz range and are often referred to as millimeter wave (mmWave). These frequencies are very short range, but the large amount of airspace available allows for high speeds over wide bands. These shorter wavelengths have difficulty passing through buildings, and even rain and foliage can disrupt signals. Research indicates high levels of attenuation for the higher frequency bands (50-60GHz) at moderate rainfall rates and similar losses observed in forested areas.[2] Due to the limited range of these frequencies, transmission equipment must be densely distributed. Current applications have been primarily restricted to places like stadiums where large numbers of users are concentrated in close proximity with limited physical obstruction to signals.

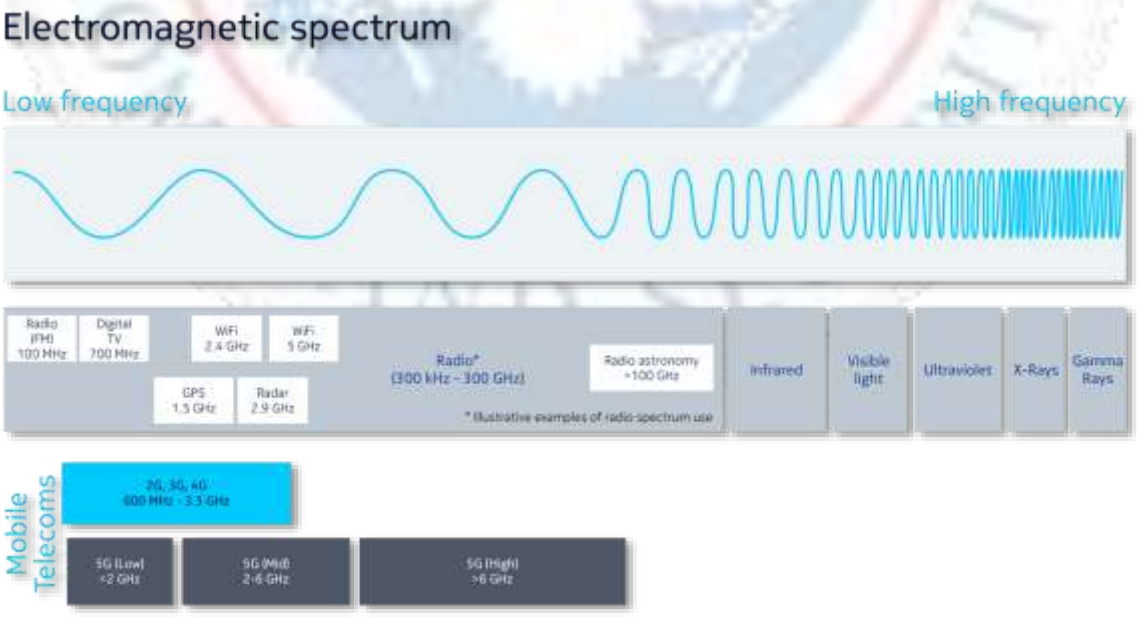


Figure 1: Electromagnetic Spectrum (Courtesy of Qualcomm)[3]

Like 4G LTE, 5G is based on orthogonal frequency-division multiplexing (OFDM), which modulates signals across several different channels to reduce interference. The 5G protocol introduces changes that will facilitate improved capabilities for both existing and previously unused frequencies. 5G enables devices to operate across broader frequency ranges for increased traffic capacity. This is accomplished by stacking 5G channels and combining 4G and 5G capabilities. Dynamic spectrum sharing (DSS) allows

[1] What Is 5G? | PCMag
[2] https://www.ursi.org/proceedings/procAP19/papers2019/ ManuscriptDaliaAPRASC2019.pdf
[3] What is 5G | Everything You Need to Know About 5G | 5G FAQ | Qualcomm

carriers to split traffic along both 4G and 5G channels based on demand. Additionally, most 5G networks still use 4G networks to establish initial connections (although some stand-alone 5G networks are beginning to be rolled out). Accordingly, existing 4G networks will still be fundamental to the deployment and operations of 5G capabilities for the near to mid-term future.

The Benefits of 5G

The updates facilitated by 5G align to enable several significant advances in network performance and applications. Data transmission at some frequencies is up to 100 times faster than 4G networks, and the transformative impact of the standard is enabled by the decreased latency, improved reliability, and expanded capacity of 5G networks.[4] These attributes will support applications requiring mission-critical connectivity and/or very large numbers of connections such as autonomous vehicle operations and IoT.

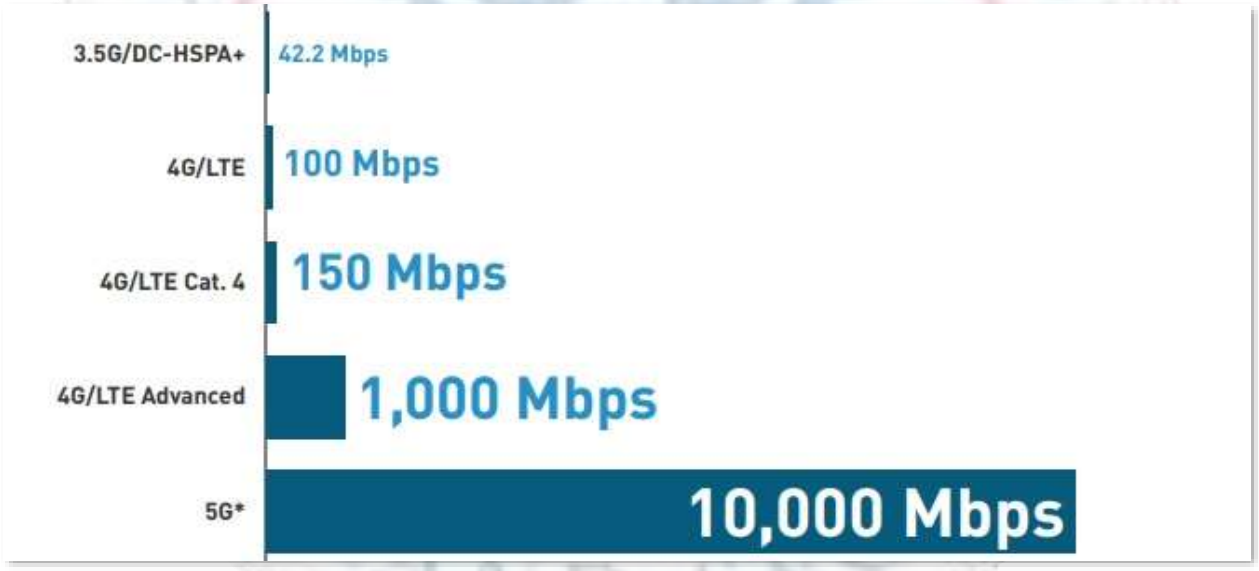
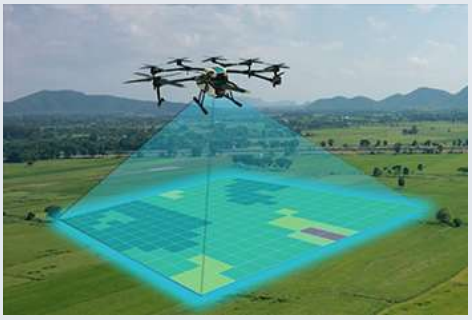


Figure 2: Comparing Network Speeds (Courtesy of 5G Americas)[5]

Applications with mission-critical connectivity requirements include those for which breaks in coverage or a significant latency could prove catastrophic, such as remote or autonomous operations of unmanned aircraft vehicles (UAVs), medical equipment, or security systems. The channel stacking, spectrum sharing, coverage redundancies, and improved networks handoffs enabled by 5G make 5G much more reliable at certain frequencies than earlier generations. The new standard also reduces latency by a factor of 10 to less than one millisecond, enabling 5G services over cellular networks.[6] 5G's increased

[4] What is 5G? How will it transform our world? - Ericsson
[5] Home - 5G Americas
[6] What is 5G | Everything You Need to Know About 5G | 5G FAQ | Qualcomm

How 5G Enables Autonomous Systems



Flying drones on cellular networks, particularly 5G networks, is a viable option for delivering low-latency and high-performing applications such as emergency supply delivery, search and rescue missions, and border surveillance operations. 5G cellular data may enable three prominent drone technologies in particular – Unmanned Aircraft Systems Traffic Management (UTM), Beyond Visual Line of Sight (BVLOS) flights, and Sensor Data Transmission (SDTX).

UTM will deliver a globally standardized technology, allowing 5G networks to be integrated with traffic management systems to enhance the safety and security of commercial drone operations. BVLOS will open applications for UAVs that are currently restricted in most jurisdictions around the world to low-altitude operations (below 120m or 400ft) within the visual line of sight of a human pilot. Finally, SDTX is used when data is transmitted to ground stations beyond the remote-control station of the pilot. This allows for live broadcasting of the drone's sensor payload data and it saves data processing time.

Additionally, 5G technology may enable passive radar drone tracking and targeting. As more 5G mmWave transceivers are deployed in city centers, the ability to detect and track drones in complex urban geometries becomes easier, while not contributing to an already crowded radio frequency spectrum.

capacity and frequency management enable it to support one million connected devices per square kilometer, more than 100 times the capacity of 4G. This means that 5G will support a major expansion of massive IoT systems, ranging from industrial control systems, long distance smart vehicles, 'smart factory' sensors, and 'smart cities' with greater digital infrastructure.[7]

5G Infrastructure and Components

Telecommunications transmission infrastructure consists of two main elements: core network components, which knit together to provide a consistent connection through mobile, fixed, and converged connectivity, and radio access network (RAN) components, which are used by devices to communicate across a network. Presently, most 5G infrastructure deployment is focused on the RAN components, since existing base stations and antenna arrays require upgrades to achieve true 5G connectivity. New base stations are fixed points within a cellular network and are mostly unnecessary for low and middle band 5G, as these frequencies have the same range and penetration properties under 4G protocols. Some components like attached antenna arrays will need to be upgraded or replaced altogether to deliver higher speeds and lower latency. New and densely distributed stations will be necessary to provide areas with mmWave coverage.

Manufacturers of transmission equipment like Ericsson, Nokia, Samsung, or Qualcomm are focused on Multiple-Input, Multiple-Output (MIMO) technology with their mobile carrier clients. MIMO combines many antennas into one array to improve efficiency and provide better 5G coverage. MIMO arrays are necessary as mmWave 5G antennas are highly directional and require a line of sight for a connection to occur.[8] These antennas are smaller but require greater quantities to ensure full coverage.

At the device level, specific receivers and chipsets are required for 5G connectivity. The telecom chipset marketplace has contracted since 4G first launched a decade ago. Due to high R&D costs and stagnant technological advancement, many manufacturers chose to abandon their products or sell to larger companies, resulting in only a handful of remaining market players.

A divide is growing between manufacturers that can produce the necessary hardware (such as mmWave chipsets) and those that cannot, as expectations for greater mmWave connectivity with 5G deployment will continue. Companies like Qualcomm (US) and

[7] What is 5G? A helpful illustrated Q&A (2021) (thalesgroup.com)
[8] https://www.thomasnet.com/articles/top-suppliers/5g-antenna-manufacturers-and-suppliers/

Samsung (South Korea) are producing and shipping both Sub-6 and mmWave chips. US-based Skyworks and Qorvo are two of the largest radio frequency front-end component fabricators, and each company supplies necessary equipment to achieve 5G connections to companies that do not produce them. While the Chinese firm Huawei was among the first companies to promote their 5G technologies, the US ban on Huawei components and growing international concern has decreased its global market share. Huawei does not build their own front-end components, which has limited their market penetration.

The threats posed by foreign 5G infrastructure and components include espionage and coordinated attacks on infrastructure and are a serious national security consideration discussed in greater depth later in this report. Additionally, there are significant security challenges in ensuring that the technology is genuine and not tampered with as the manufacturing of 5G components is a worldwide enterprise. Components are vulnerable to unwanted alterations in materials, coding, or packaging during the transport process. This could leave end users susceptible to cyberattacks, ransomware, and other cybersecurity concerns. Monitoring the 5G supply chain as parts move around the world is necessary to track components and new entrants into the marketplace. Several of the key players in 5G infrastructure have conducted research and development on supply chain security, while several commercial-off-the-shelf (COTS) tools and service providers offer supply chain monitoring capabilities. Additional concerns surround protecting networks from non-state Distributed Denial of Service (DDoS), Telephony Denial of Service (TDoS), and massive IoT attacks.

The Tech Scouting team has conducted previous research on supply chain risk management tools, along with tools for 5G mobile, infrastructure, and supply chain security. For more information about these research efforts, please contact the TS Program Office.

The Huawei Ban

China's Huawei Technologies Co. continues to lead the $90 billion annual market for telecommunications equipment. Under China's 2017 National Intelligence Law, Huawei, like all Chinese companies and entities, appears legally required to conduct intelligence work on behalf of the Chinese government. According to defense analysts, the Chinese government may have the ability to use Huawei-built 5G networks to collect intelligence, monitor critics, and steal intellectual property. There are also concerns that the company could disable entire regional networks to exert coercive pressure on a country. As of 2019 estimates, 25% of rural US cellular cites contain some portion of Huawei network hardware.

In 2019, the Department of Commerce placed Huawei on its Entity List, restricting US companies from selling goods and technology to the company. In 2021, the Trump administration revoked licenses for US companies to sell products to Huawei that had previously been allowed even under the 2019 entity designation. These restrictions have mostly halted Huawei's integration into the US. A notable exception can be found in the rural communities which have relied on cheaper Chinese infrastructure to build out their networks. Large portions of existing network hardware in rural US states are currently being extracted and replaced due to security concerns. Starting in 2022, hardware from Huawei (and several other Chinese companies) such as chips, switches, and RAN equipment will need to be replaced in rural communities, as currently directed under the Federal Communications Commission's (FCC's) $1.9 billion reimbursement plan for rural carriers. While Huawei is the major provider applicable to this plan, ZTE, Hytera, Hangzhou Hikvision, and Zhejiang Dahua all have a small presence in rural US networks that will be impacted.

5G Deployment

The deployment of 5G technologies and networks has been rapid but uneven globally. Adoption is occurring at a faster rate than 4G, supported by aggressive industry and government investments in the United States, China, and South Korea. Infrastructure deployment has received opposition from communities for concerns over regional network market shares, national security, and disputes over the allocation of spectrum bands.

The number of global 5G subscribers is anticipated to surpass one billion in 2022 and quickly accelerate to include most of the world within the decade.[9] It is anticipated that the deployment will amount to $13.1 trillion of global economic output, with $265 billion in 5G capital expenditures, research, and development over the next 15 years that does not include the market and technology transformations anticipated from 5G deployment.[10]

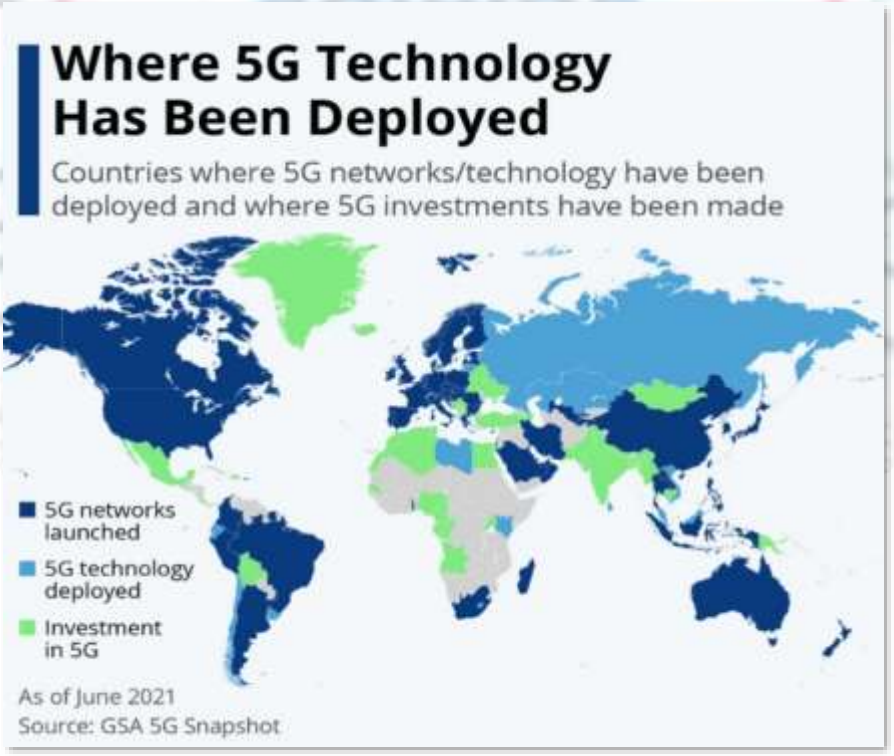


Figure 4: Global Deployment of 5G Networks

[9] Home - 5G Americas
[10] What is 5G? How will it transform our world? - Ericsson

The Future of 5G and 6G

"From enabling remote robotic surgery and autonomous cars to improving crop management, 5G is poised to transform many of the world's biggest industries." - CB Insights

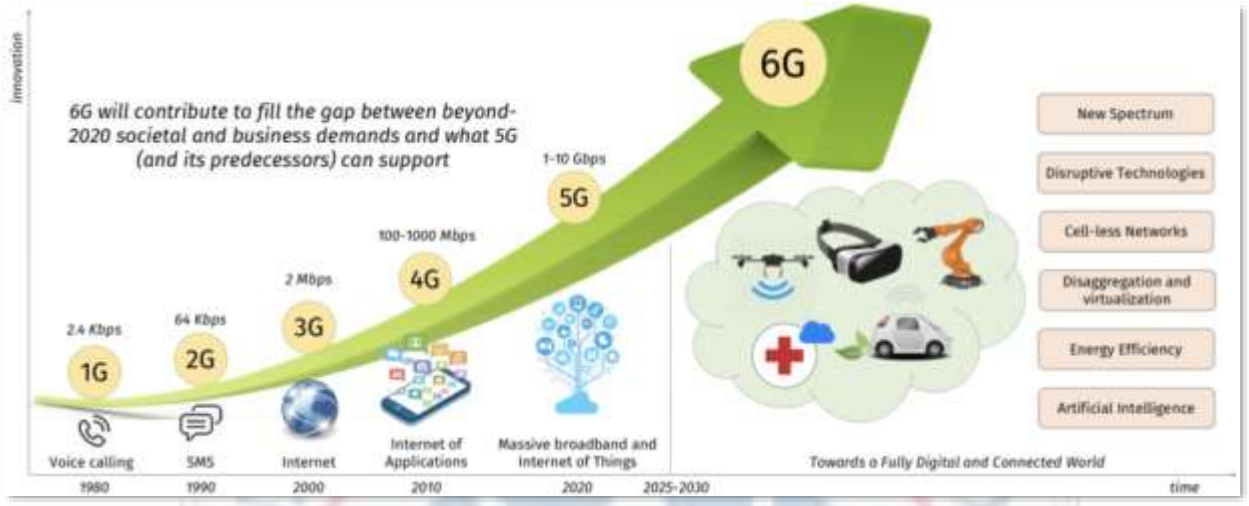


Figure 5: 5G/6G Development; Source: Navixy

5G Advanced

5G Advanced is a planned set of technology and network upgrades that will expand on the existing capabilities of 5G technology and is predicted to be deployed by 2025. One key component of 5G Advanced is the application of artificial intelligence (AI) and machine learning (ML) solutions to introduce more intelligent network management capabilities to cloud, edge, and IoT environments while efficiently managing more connected devices, enabling much higher download speeds, and preserving low latency.[11] These upgrades will support 5G's enterprise use cases like connected vehicles, real-time automation for manufacturing, and autonomous robotics. These enterprise applications will be the primary driver of 5G growth and adoption, while the commercial market for enterprise uses of 5G is expected to exceed $180 billion in North America by 2030[12].

In the commercial market, there is an expected shift towards a more dominant role in 5G technology and standards development for Hyperscaler (scalable/agile network solutions) cloud and network services from companies like Amazon, Google, and Facebook. Rather than build the cellular network sites, these Hyperscalers rely on 5G to support mobile connectivity of users for their applications, and they will continue to expand ongoing activities and R&D investments in 5G. Hyperscalers will both create demand for new uses of the 5G network through their applications and compete with communications service providers (CSPs) in shaping the development of 5G network architecture with a focus on open architecture.

[11] https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/5g-evolution-toward-5g-advanced
[12] https://www.jpmorgan.com/insights/research/future-of-5g-adoption

6G Development and Launch

The 6G wireless communication network will be the successor to 5G and is expected to begin launch in 2030. Notable differentiators of 6G from 5G include enhanced scalability, greater use of the radio spectrum, and dynamic access to different connection types. Enhanced scalability will be achieved by the low power consumption and long connection ranges expected of 6G. 6G is expected to access a broader range of the radio spectrum to support greater connectivity and reliability, with some estimates of the 6G spectrum ranging from 95GHz to 3THz. Dynamic access to connection types will enable greater reliability and limit drops in connection, which is critical to support advanced technologies like drones and robots; this dynamic access will enable connected devices to use multiple connections concurrently (e.g., Wi-Fi and cellular) to stay connected even if one source is interrupted. 6G is also expected to make greater use of techniques like MIMO to re-use radio spectrum and improve efficiencies. The effect of 6G's deployment will be to further drive digitization and connectivity beyond what will be achieved under 5G and 5G Advanced.

The transition from 5G Advanced to 6G is expected to begin by 2030, and several aspects of development (and potential barriers) will need to be addressed to enable this. As explained in the 5G Infrastructure and Components section, hardware requirements will increase in the shift towards 6G along with new requirements to ensure that the connectivity allocation of all devices will not be disrupted when new network protocols are introduced. Legacy radio access technology (RAT) devices, such as Wi-Fi and Bluetooth, can also be transitioned into the early stages of the 6G rollout.[13] Additionally, the issue of Chinese hardware in rural 5G networks will need to be addressed as 6G will rely on hyper-connectivity across all US networks.

DHS Implications of 5G and 6G

Opportunities for DHS

As the launch of 5G promises radical new capabilities for consumers and industry, so too does it present opportunities to enhance HSE operations and support the DHS mission space. 5G will enable an expansion in the number of connected devices and help to realize IoT on a massive scale. This capability has the potential to enable the deployment of autonomous systems like reconnaissance drones and support the strengthening of communications infrastructure, including systems utilized by first responders. The proliferation of millions of wireless sensors could accelerate DHS missions already supported by remote sensing, detecting, and tracking devices. Relevant use cases include enhanced surveillance capabilities along US borders, at government facilities, and in response to emergency events.

Along the border, this could mean denser deployment of trail cameras to alert Border Patrol officers of illegal entry or smuggling, or greater numbers of rescue beacons to assist migrants in distress. In crowded places like transportation hubs and sporting events, intensive coverage by cameras combined with real-time facial recognition and person-tracking (enabled by the high capacities and low latencies of 5G) could help law enforcement identify, locate, and respond to threats and nefarious actors. Proliferation of gunshot detection audio sensors could bring the benefits of event triangulation and rapid response to law enforcement across broader swaths of communities than have previously been piloted. Customs Enforcement could utilize mass deployment of inexpensive sensors to ports of entry to monitor individual pieces of cargo across supply chains, while the Transportation Security Administration (TSA) and other law enforcement could monitor distributed networks of sensors capable of detecting chemical, biological,

[13] https://hcis-journal.springeropen.com/articles/10.1186/s13673-020-00258-2

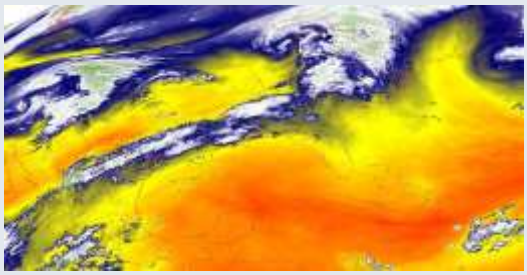
radiological, nuclear, and explosive (CBRNE) threats at airports and transit hubs or even across entire cities.

Widely distributed sensors could also monitor critical infrastructure for early indications of failure, including during natural disasters, with flood sensors along levees or wildfire detectors helping to inform incident response and planning. Internally, DHS components could improve enterprise-wide fleet and asset management with onboard tracking and could enable real-time monitoring of the location and safety of personnel in the field with person tracking and performance monitoring devices. These capabilities are all enabled by 5G's capacity to connect billions of communicating devices that could help make mission-focused IoT possible for DHS.

6G technology is expected to provide wider bandwidth, which would support high-speed communications and enhanced sensing networks. Sensing networks are formed when physical infrastructure is equipped with sensing capabilities such as touch panels, cameras, infrared sensors, and gyroscopes. These sensors can continue to be improved by incorporating millimeter wave radar chips. These chips are currently capable of detecting the range, velocity, and angle of objects in the sensor's environment, and researchers are working to add motion recognition, material detection, and three-dimensional scanning capabilities. As sensing requires significant bandwidth capabilities to continuously collect and transmit information in a mobile network, 6G's wider bandwidth capabilities could enable this complex sensing network to support DHS's diverse mission space.

Known DHS mission needs include advanced sensing technology in contexts including CBRNE threat sensing and autonomous vehicles. Technology which currently supports CBRNE threat-sensing use cases are often highly specific and unable to detect and identify a wide range of potential threat agents. Consequently, government agencies are required to purchase and maintain a large quantity of equipment to ensure mission success. Similarly, autonomous vehicles require sensors to continuously evaluate their environment. Current bandwidth capabilities limit the speed at which these sensors can transmit and process the information, reducing the ability to react to changing environments in real-time. With the advanced sensors and bandwidth that 6G capabilities provide, technology may be developed to enable fewer CBRNE sensors to scan for a broader range of threat agents. 6G will allow sensors to be interconnected, providing information to a central hub that integrates sensor data for a broad picture of ongoing scenarios and broadcasts these findings to support information sharing during a crisis. This new system would simplify and reduce the cost of CBRNE threat detection and the number of agents required to oversee and interpret the results from these environmental sensors.

5G: A Threat to Forecasting Natural Disasters?



5G-enabled expansion of wireless frequencies deep into the mmWave spectrum is a central component of the protocol's enhanced capabilities and applications, but this also presents serious threats to other established uses in the spectrum. Among these are satellite based meteorological observations, which are central to weather forecasting models and inform the Government's planning and response for natural disasters.

The NASA Geostationary Operational Environmental Satellites (GOES), the backbone of American meteorological remote sensing, rely on specific reflectivity signatures to detect and infer the presence and concentration of water vapor, a fundamental factor in storm development and weather system tracks. Some mmWave frequencies bleed into those used to identify water vapor and could render GOES data unreliable or even unusable. The National Oceanic and Atmospheric Administration (NOAA) has warned that the level of interference from mmWave transmissions could seriously impact forecast quality and the Commerce Department has asked the FCC to limit transmission around certain frequencies, but an agreement has not been reached yet.

Scientists believe there are solutions that can preserve functionalities for both technologies, but until these are established, 5G proliferation may hinder the HSE's ability to respond to natural disasters.

6G-enabled capabilities would also support autonomous vehicles and intelligent transportation. Autonomous vehicles can be equipped with radar that enables them to sense the positioning of objects in the vehicle's surroundings and detect potential obstacles. This data would be uploaded to a central network via a wireless connection, and this network would guide the vehicle's driving. Due to resolution limitations, mmWave radar in a real environment is too slow to provide satisfactory results. Therefore, the additional bandwidth available using 6G will support these new autonomous vehicle capabilities, and the sensors and bandwidth enabled by 6G could support broader intelligent transportation systems like traffic pattern tracking to support first responder operations.

Security Threats

5G wireless technology represents a transformation of telecommunication networks, and these developments introduce risks that threaten homeland security, economic security, and other national and global interests that will continue to evolve through the transition to 6G. Undue influence from nation-states in standards development can negatively affect the competitive balance within the information and communications technology (ICT) market, potentially limiting the availability of trusted suppliers and leading to a situation where untrusted suppliers are the only market options. Additionally, 5G networks are an attractive target for criminals and foreign adversaries to exploit for valuable information and intelligence, and these challenges may become more acute with the deployment of 6G. Strong technology standards and cybersecurity practices will need to be incorporated within the design and development of ICT technology for DHS to leverage and secure the full scope of 5G and 6G use cases. Many of the opportunities that are enabled by 5G and 6G (e.g., drone teaming, enhanced communications, edge computing) will be utilized by US adversaries as well. There are various security considerations to note within the current 5G framework that will also relate to the eventual deployment of 6G.

With the potential for the connection of billions of 5G devices, there is an increased risk for untrusted or counterfeit components to be introduced within the ICT supply chain. This could include compromised devices or infrastructure that impact end-user systems, such as government computers, phones, and other devices. Inherited components may come from extended supply chains consisting of third-party suppliers, vendors, and service providers. Supply chains may be compromised via attacks on DHS suppliers, including lower tiered suppliers, who may have weaker security controls and audits on their development, production, or delivery channels. Flaws or malware inserted early in the development phases are more difficult to detect and could lead to the developer marking the component as legitimate through digital signatures or other approvals. These vulnerabilities could then later be exploited by malicious actors. Over time, new exploitable weaknesses will be discovered as new components and technologies are developed and deployed under 5G and the transition to 6G.

In addition to supply chain security risks, future ICT system architecture may introduce an increased attack surface for malicious actors to exploit. These vulnerabilities could be used by malicious threat actors to negatively impact the HSE. For example, current 5G deployments leverage legacy infrastructure and untrusted components with known vulnerabilities. 5G builds upon previous generations of wireless networks and is currently being integrated with 4G LTE networks that contain some legacy vulnerabilities. Some of these legacy vulnerabilities, whether accidental or maliciously inserted, may affect 5G equipment and networks despite the integration of additional security enhancements. Evolving vulnerabilities will increase the impact of cyber incidents and necessitate continuous focus on threat vectors and early identification of weaknesses in 5G and 6G system architectures.

Finally, reliance on mobile networks to deliver government services puts missions at risk if networks are damaged or service degraded. Some of the greatest threats posed by existing and emerging ICT technology involve mission-critical applications. For example, 5G will enable smart cities and self-driving cars with 5G networks underpinning services such as emergency response and border crossings. If the ICT networks enabling these applications are interfered with by malicious actors, the results could be

How Changing Standards Can Upend Dependencies in Homeland Security

Some of the most consequential changes brought about by 5G (and eventually 6G) do not stem from technological advancements or updated hardware, but from small changes to network protocols. For example, updates to the 5G protocol have shifted how devices identify themselves to networks, encrypting identifying information and changing the order of information exchange to enhance security and consumer privacy. 5G also enables devices to simultaneously connect to multiple base stations at a time for reduced latency and enhanced reliability. Neither of these changes were designed to disrupt lawful uses of data, but they nonetheless impact commercial and governmental practices in geolocation that were built upon more open disclosure of information between users and networks, such as methodologies for locating criminal actors.

Unforeseen consequences like these may disrupt existing dependencies and protocols in HSE communications, threat detection, and security. Further protocol updates to 5G and the development of 6G may accelerate these challenges. Because of the potential for collateral damage, industry representatives for mobile carriers and equipment manufacturers are heavily involved in the development of wireless standards, and increasingly, as is the government. The involvement of law enforcement groups and governments in the standards development process could protect or counteract national security and geopolitical interests and will be especially consequential in the upcoming development of 6G. The US government has a stake in global 6G protocols to support its security and economic interests through compatibility and consistency across nations. With the Chinese government widely expected to yield major influence on the development of future protocols under threat of creating its own incompatible standards, proactive US leadership in 6G standards development will have a critical impact on supporting preferable outcomes for the US and its allies.

hazardous to the public and DHS personnel. DHS will need to implement end-to-end encryption from user equipment to a secure node within the core operating network to ensure security. With the promise of connectivity between billions of IoT devices, it is critical that DHS and industry collaborate to ensure that cybersecurity is prioritized within the design and development of 5G and 6G technologies.

Evolving Future Scenarios

While the opportunities and threats detailed above address known implications of 5G for DHS, uncertain and evolving developments in the 5G ecosystem present varying future scenarios for DHS. Uncertainties regarding 5G's future necessitate DHS consideration of how various scenarios will impact its mission over the next five to 10 years. Consideration of the likelihood of these scenarios and the implications of potential outcomes can inform DHS planning efforts for emerging circumstances in the 5G and 6G ecosystem. Evolving areas with implications for the DHS mission space include 5G network resiliency and 6G standards development.

The enhanced interconnectedness enabled by 5G increases the significance of network resiliency as mission-critical devices and capabilities will be powered by 5G. Existing 5G network security protocols are strong, but these protocols are focused on issues that impact the businesses of network operators. While resiliency is important to the business models of 5G network providers, additional protocols will likely be necessary to address emerging national security issues. As DHS transitions mission-critical technologies to 5G infrastructure, the availability, reliability, and capacity of 5G networks to rapidly recover from disturbances is critical for DHS users. 5G network providers will continue to develop capabilities to meet evolving threats to network operations, and DHS can plan for impacts of varying resiliency scenarios into the future.

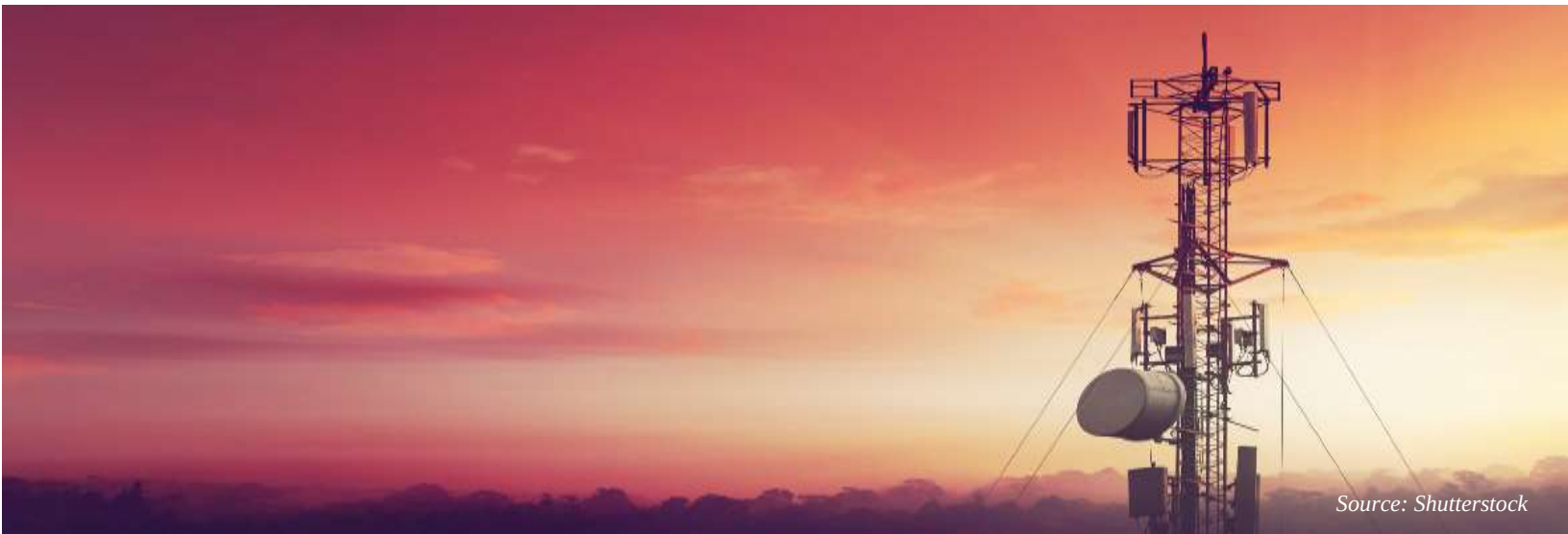
Under conditions of improved 5G/6G network resiliency, DHS will be able to transition more mission critical capabilities to networked devices and improve its ability to prepare and respond quickly to emerging threats. Security capabilities for DHS users would be enhanced due to the elevated security protocols as compared to legacy networks. Under conditions of degraded 5G/6G network resiliency, these issues of reliability and security will be magnified for DHS users due to the expanded role of networked technologies in mission-critical functions. Networked devices will need to be augmented with robust security protocols to ensure continuity in the case of wider network failures. Expanding 5G/6G networked technologies into mission critical applications will bring greater opportunities to the HSE.

While 5G incorporated the first global set of network protocols, the development of 6G standards is expected to be fragmented between countries. The relative influence of dominant state actors like the US and China in developing these standards will have implications for DHS. With the Chinese government expected to wield major influence on 6G protocols under the threat of creating its own incompatible standards, the US government must take a leading role in the development and proliferation of secure, global networking standards in the years to come. A fragmented matrix of differing standards globally will have both operational and threat-based implications that DHS will need to adapt to in preparation for the deployment of 6G.

Under circumstances of US-led 6G standards development, the US government will enable a global, unified 6G standard that meets US concerns for security standards and economic competitiveness while enabling global market access to US firms. Under a bifurcated 6G standard between the US and China and each country's allies, the US will have considerably less influence in ensuring that policies aligned with its interests are broadly implemented. Variable security standards will impact DHS's security posture for networked systems, and US firms will face challenges entering global markets and achieving compatibility with infrastructure adhering to varying 6G standards.

Conclusion

The future of 5G and 6G technology will advance the interconnectedness of society and support the proliferation of emerging technologies. New and enhanced capabilities supported by 5G and 6G infrastructure include IoT, autonomous vehicles, and advanced sensor devices. These technologies will provide opportunities like enhanced surveillance and communication for DHS to more comprehensively safeguard the American people and the homeland. These advancements also present security challenges across the HSE, including supply chain and systems architecture risks. Expanded awareness and understanding of these novel opportunities and threats across DHS is critical to ensuring that the organization is adequately prepared for the future enabled by 5G and 6G technology.



Source: Shutterstock