Cybersecurity & Information Systems
Information Analysis Center

CSIAC TECHNICAL INQUIRY (TI) RESPONSE REPORT

The State of 5G Technology and Applications to the DoD and Military

Report Number:
CSIAC-BCO-2022-229
Completed June 2022

CSIAC is a Department of Defense Information Analysis Center

MAIN OFFICE
4695 Millennium Drive
Belcamp, MD 21017-1505
Office: 443-360-4600

REPORT PREPARED BY:
Philip Payne and Ryan Fowler
CSIAC

CSIAC is sponsored by the Defense Technical Information Center, with policy oversight provided by the Office of the Under Secretary of Defense for Research and Engineering. CSIAC is operated by the SURVICE Engineering Company.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	2. REPORT TYPE	3. DATES COVERED *(From – To)*
	Technical Research Report	

4. TITLE AND SUBTITLE
The State of 5G Technology and Applications to the DoD and Military

5a. CONTRACT NUMBER
FA8075-21-D-0001

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)

Philip Payne and Ryan Fowler

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)

Cybersecurity & Information Systems Information Analysis Center (CSIAC)
SURVICE Engineering Company
4695 Millennium Drive
Belcamp, MD 21017-1505

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)

Defense Technical Information Center (DTIC)
8725 John J. Kingman Road
Fort Belvoir, VA 22060-6218

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)
CSIAC-BCO-2022-229

12. DISTRIBUTION/AVAILABILITY STATEMENT

DISTRIBUTION A. Approved for public release: distribution unlimited.

13. SUPPLEMENTARY NOTES

14. ABSTRACT

The fifth-generation wireless communication technology abbreviated "5G" has the potential to transform communication systems. The 5G mobile network will deliver higher speeds, lower latency, increased reliability, more network capacity, and increased interconnectivity. With the deployment, modernization, and implementation of 5G technology into both preexisting and new systems, immense improvements are expected. In recent years, there has been exponential growth in investments and interest in 5G technologies as all sectors look to be innovative on the cusp of the new technology. Taking full advantage of this technology will propel industry and U.S. Department of Defense (DoD) capabilities into the future with massive improvements, such as higher performance and improved efficiency. This report focuses on the current state of this technology and specific use cases for the DoD.

15. SUBJECT TERMS
5G, fifth generation, cellular, wireless networks, networks, spectrum

16. SECURITY CLASSIFICATION OF: U			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE	UU		Ted Welsh, CSIAC Director
U	U	U			19b. TELEPHONE NUMBER *(include area code)* 443-360-4600

Standard Form 298 (Rev. 8-98)
Prescribed by ANSI Std. Z39.18

DISTRIBUTION A. Approved for public release: distribution unlimited.

ABOUT DTIC AND CSIAC

The Defense Technical Information Center (DTIC) preserves, curates, and shares knowledge from DoD's annual multibillion dollar investment in science and technology, multiplying the value and accelerating capability to the warfighter. DTIC amplifies this by collecting information and enhancing the digital search, analysis, and collaboration tools that make information widely available to decision makers, researchers, engineers, and scientists across the Department.

DTIC sponsors the DoD Information Analysis Centers, which provide critical, flexible, and cutting-edge research and analysis to produce relevant and reusable scientific and technical information for acquisition program managers, DoD laboratories, Program Executive Offices, and Combatant Commands. The IACs are staffed by or have access to hundreds of scientists, engineers, and information specialists who provide research and analysis to customers with diverse, complex, and challenging requirements.

The Cybersecurity & Information Systems Information Analysis Center (CSIAC) is a DoD IAC sponsored by DTIC to provide expertise in four technical focus areas: cybersecurity; knowledge management & information sharing; modeling & simulation; and software data & analysis. CSIAC is operated by SURVICE Engineering Company under contract FA8075-21-D-0001.

A chief service of the DoD IACs is free technical inquiry (TI) research, limited to 4 research hours per inquiry. This TI response report summarizes the research findings of one such inquiry jointly conducted by CSIAC.

ABSTRACT

The fifth-generation wireless communication technology, abbreviated “5G”, has the potential to transform communication systems. The 5G mobile network will deliver higher speeds, lower latency, increased reliability, more network capacity, and increased interconnectivity. With the deployment, modernization, and implementation of 5G technology into both preexisting and new systems, immense improvements are expected. In recent years, there has been exponential growth in investments and interest in 5G technologies as all sectors look to be innovative on the cusp of the new technology. Taking full advantage of this technology will propel industry and U.S. Department of Defense (DoD) capabilities into the future with massive improvements, such as higher performance and improved efficiency. This report focuses on the current state of this technology and specific use cases for the DoD.

Contents

List of Figures

1.0 TI Request

1.1 INQUIRY

What is the state of 5G technology (and beyond) as it applies to the U.S. Department of Defense (DoD) and military?

1.2 DESCRIPTION

This report focuses on the current state of 5G technology and specific use cases for the DoD. An introduction to the technology is given, followed by a snapshot of the status of implementation. The report then identifies multiple examples of current DoD use cases and ongoing 5G efforts.

2.0 5G Technology

2.1 WHAT IS 5G?

5G is the fifth and most recent iteration/generation of global wireless standards following 1G, 2G, 3G, and 4G networks. Similar to its predecessors, 5G networks are cellular networks in which service areas are divided into smaller areas referred to as cells. 5G devices in a cell are connected via radio waves or millimeter waves (mmWaves) through a local antenna within their given cell. 5G offers many different bands for connection of devices. These cells are often interconnected via more complicated infrastructure. The technology offered with 5G provides much better speeds and bandwidth that allows better quality and interconnectivity of devices when compared to prior generations of the technology. 5G deployment is expected to result in a 5G Internet of Things (IoT) ecosystem where devices are more interconnected than ever, while simultaneously increasing performance and lowering cost of operations. With increased speed and bandwidth compared to older generations, 5G technology can compete with preexisting infrastructure and internet service providers. This will force the introduction of new applications, infrastructure, and devices.

5G technology is primarily driven by eight specification requirements [1]. According to Thales, these key requirements are as follows [1]:

1. Up to 10 Gbps data rate – > 10 to 100× speed improvement over 4G and 4.5G networks
2. 1-ms latency
3. 1000× bandwidth per unit area
4. Up to 100× number of connected devices per unit area (compared with 4G LTE)

5. 99.999% availability
6. 100% coverage
7. 90% reduction in network energy usage
8. Up to 10-year battery life for low-power IoT devices

2.2 5G KEY ENABLING TECHNOLOGY

As 5G technology begins to be globally deployed and integrated, it brings with it a plethora of different components in both hardware and software, as well as methodologies. These components are key to ensuring the successful deployment of the new generation of 5G technology. 5G technology is extremely interwoven and communicative with other technology that exists within the 5G IoT ecosystem. Understanding these components and their interactions with one another is key to understanding what makes 5G systems the next generation.

2.2.1 5G Spectrum

Spectrum refers to the invisible radio frequencies over which wireless signals travel. The frequencies used for wireless are only a portion of what is called the electromagnetic spectrum. The 5G spectrum contains the radio frequencies that carry data from user equipment to cellular base stations to the data's endpoint. 5G technology can be implemented using low-band, mid-band, or high-band mmWaves.

High-frequency bands that are sub-6 GHz, between 24 and 100 GHz, are expected to be used for 5G, despite possessing the ability to extend up to 300 GHz. Bands that are between this range are classified as millimeter waves, as can be seen in Figure 1. These bands have the potential to support large bandwidths and high data rates and provide the potential to support increased capacity of wireless networks. The mmWave bands may have the capability of increased capacity but suffer from a lack of sustainability at range, which can be aided with the assistance of smaller and more frequent cell placement.

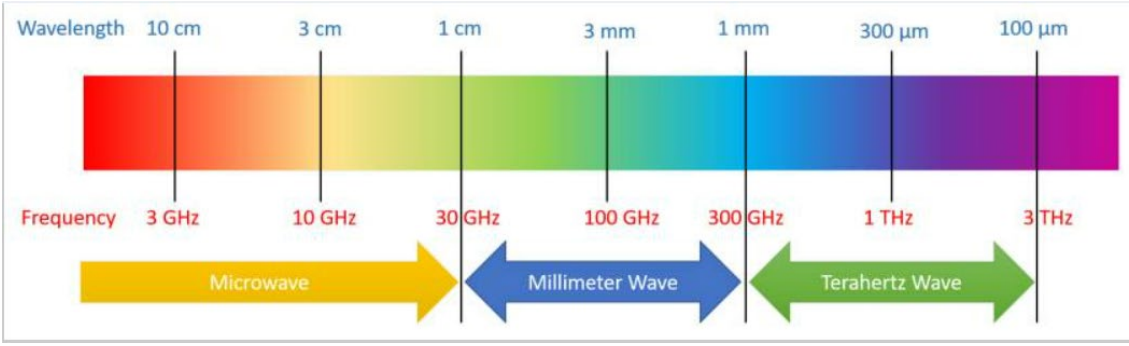


Figure 1: Microwave, Millimeter Wave, and Terahertz Wave Bands
(Source: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7284607/).

2.2.2 5G Bands and Auctions

5G technology presents the ability to exist within three types of bands—low, mid, and high bands. A frequency band is an interval that exists within the frequency domain, an available space for data to be transmitted. As more competitors in both industry and government organizations begin to invest in 5G technologies, the need to purchase availability to operate on a given band has become incredibly important. The bands are managed by the Federal Communications Commission (FCC), which also oversees the commercialization of spectrum allocations. In partner with the National Telecommunications and Information Administration (NTIA), which oversees government, international bodies, and Congress' use of the spectrum, these bands are distributed via auctions. These auctions can occur for any given portion of the spectrum, such as the C-band, which operates between 3.7 and 4 GHz. Recently, the C-band auctions had 57 qualified bidders, with only 21 walking away with the 5,684 licenses needed to operate on the band [2].

2.2.3 Centralized Radio Access Network (C-RAN)

Centralized radio access network (C-RAN) is an architecture for wireless networks. C-RAN is a primarily cloud-computing-based architecture for networks that support 5G and its predecessor's wireless communication standards. C-RAN consists of three major components, the first being baseband unit (BBU) pool. The BBU pool is at the centralized site and functions similarly to a data center. It is responsible for allocating resources to the remote radio units (RRUs) based on the current needs of the system, thus ensuring maximized efficiency. This interaction is the key processing unit in telecommunication and wireless networking systems. The RRU network, the second key component, connects the wireless devices to access points of towers within any traditional cellular or wireless network. The third and final component, the fronthaul/transport network, takes advantage of optical fiber communication, cellular communication, or mmWave communication. This layer exists between the two prior components, BBU and RRU. Between these components, the fronthaul network provides high-bandwidth links to handle the requirements of the multiple interlinked systems. Figure 2 depicts a high-level, C-RAN architecture.

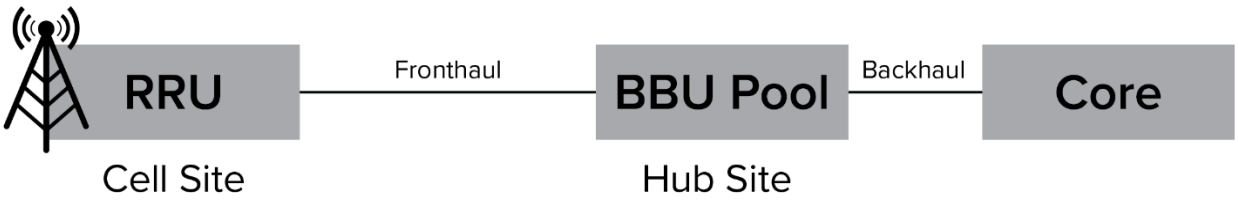


Figure 2: C-RAN Architecture.

2.2.4 Multiple Input Multiple Output (MIMO)

Multiple input multiple output (MIMO) systems use multiple antennas at the transmitter and receiver ends of a wireless communication system. "Multiple antennas use the spatial dimension for multiplexing in addition to the time and frequency ones, without changing the bandwidth requirements of the system [20]". Massive MIMO antennas increase sector throughput and capacity density using a large number of antennas. MIMO systems require the collaboration of multiple antennas and complex algorithms. MIMO systems are not anything particularly new, as they have been used in many forms of wireless communication, and even in predecessors of 5G. Examples of this are shown throughout the hardware that is used, such as mobile devices and networks that have multiple intercommunicative antennas allowing enhanced capability and connectivity. This interconnectivity that MIMO systems are built upon relies heavily on proper and secure coordination/communication, as well as the algorithms that control that hardware itself. These algorithms allow coordination between the antennas by controlling the data maps into antennas and determining where the energy is focused within that space. MIMO systems are a key enabler of 5G's full capabilities and allow the benefits to the networks and end users, such as improved coverage, user experience, quality of life, network capacity, and general speed and efficiency. For example, Figure 3 depicts a 4×4 MIMO architecture, which includes four antennas at the transmitting side and four antennas at the receiver end.

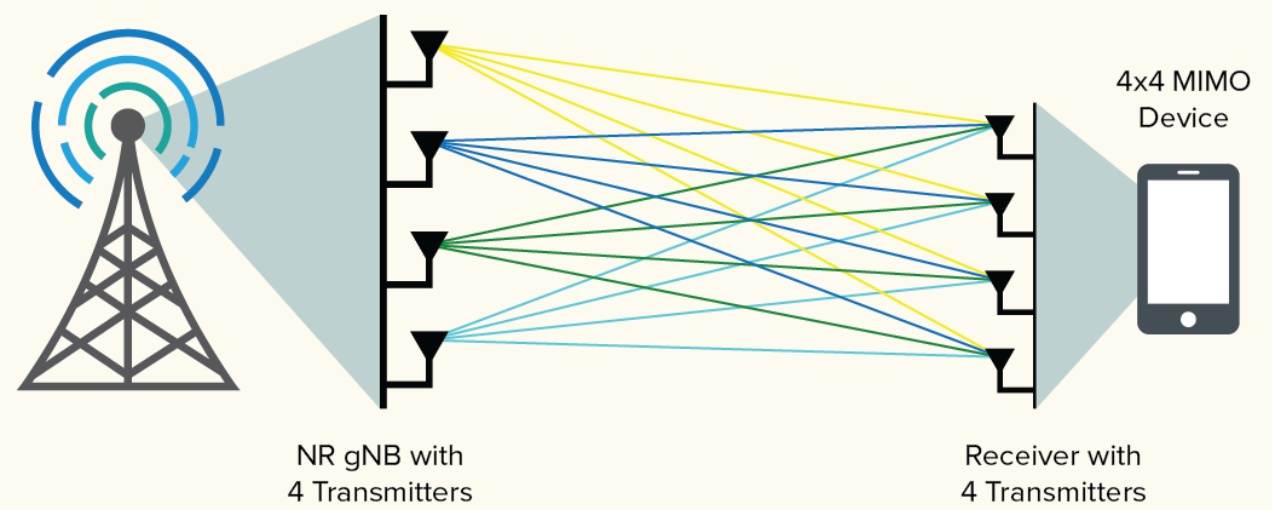


Figure 3: 4×4 MIMO.

2.2.5 Beamforming

Beamforming is another methodology that provides the full utilization of antenna technologies. It allows antennas of both mobile and base networks to have their wireless signals focused into a specific direction. This is much better than the natural alternative, which is wide-area broadcast. Wide-area broadcast dilutes the true strength of the signal as it is spread, rather

than pinpointing and having precision as allowed with the use of beamforming. Precise location of the user device is continuously tracked using advanced software algorithms, as well as base stations that transmit signals only in the direction of the user's location. In contrast, conventional base stations transmit data in multiple directions, which causes higher power consumption and unnecessary resource utilization. Beamforming helps the base station find a suitable route to deliver data to the user and also reduces interference with nearby users along the route, as shown in Figure 4.

Figure 4: Massive MIMO Beamforming
(Source: https://www.ncbi.nlm.nih.gov/pmc/articles/PMC7284607/).

By incorporating cohabitation between MIMO systems and beamforming methodology being applied to a system, the result becomes a hybrid method known as three-dimensional beamforming. This hybrid technique creates two sets of focused signals—one horizonal and the other vertical. This dual signal allows all users to experience increased rates and capacity despite potential environmental inhibitors. This is very common in high-density cities with numerous towering buildings and overly occupied skylines.

2.3 CURRENT STATUS

5G is quickly becoming ubiquitous. Because 5G networks are cellular, the strength of the technology comes from the network coverage. In 2020, world countries picked up speed in

deploying 5G, and over 1 billion people will have access to 5G by the end of the year, according to a recent report by Swedish telecommunications company Ericsson [3]. As of 2020, countries around the world were quick to deploy commercial 5G new radio (NR). "5G NR (New Radio) is a new air interface developed for the 5G network. It is supposed to be the global standard for the air interface of 3GPP 5G networks [4]". Currently, most European and East-Asian countries, as well as many major cities in the United States, Canada, and Australia, have access to 5G technology, with the rest of the world picking up the pace in deployments. Additionally, telecom companies in many countries, such as Russia and Madagascar, experience precommercial deployments. When it comes to the number of cities where 5G is available, South Korea, China, and the United States take the lead [5].

"As of April 2019, the Global Mobile Suppliers Association had identified 224 operators in 88 countries that have demonstrated, are testing or trialing, or have been licensed to conduct field trials of 5G technologies, are deploying 5G networks or have announced service launches [6]".

According to Berry [7], the top 10 global 5G infrastructure companies are AT&T, T-Mobile, Ericsson, Huawei, Nokia, Qualcomm, Samsung, Version, Vodafone, and ZTE.

3.0 5G in the DoD and Military

The DoD has listed 5G technology as a critical strategic technology. Starting within their official DoD 5G Strategy, "…those nations that master advanced communications technologies and ubiquitous connectivity will have a long-term economic and military advantage" [8]. The future of communications and interconnective systems is 5G, which inherently makes it critically important to the DoD. By pursuing 5G technologies at their maximum potential, the DoD will be capable of hitting new heights in technology, performance, and additional capabilities.

3.1 DOD 5G POLICY

The DoD 5G Strategy and the DoD 5G Strategy Implementation Plan [9] provide a roadmap for addressing the technology, security, standards and policy, and partnering aspects of how the DoD can use and advance 5G networks and applications. The comprehensive DoD 5G Strategy Implementation Plan consists of four lines of effort. The first line of effort is to "promote technology development" by, for example, conducting 5G demonstrations, implementing mmWave and dynamic spectrum sharing technologies, promoting open architecture and virtualization, and focusing on developing a 5G workforce. The second line of effort is to "assess, mitigate, and operate through 5G." This second line of effort primarily focuses on threat intelligence, infrastructure risk, security of the supply chain, global operations, security assessments, cybersecurity, and zero trust. The third line of effort is to "influence 5G standards and policies" and includes tight integration with standards-setting bodies. Along these lines,

the DoD will create and update standards and guidelines for advanced spectrum management, 5G-enabled concept of operations (CONOPS), and technology control measures. Lastly, the fourth line of effort is to "engage partners," such as international allies, industry, and congressional members.

3.2 5G DOD USE CASES

This section identifies DoD-specific use cases of 5G technology. 5G is currently being used across all services for a variety of reasons. 5G technology is a key enabler whose capabilities will allow improved performance across the DoD in many aspects.

In October 2020, the DoD announced six-hundred million in awards for 5G research and assessment at five United States military examination sites, amounting to the biggest full-fledged 5G experiments for dual-use administration in the world. The DoD seeks to remain at the forefront of cutting-edge 5G testing and experimentation to strengthen our nation's warfighting capabilities, as well as U.S. economic competitiveness in this critical field [10]. These five tests are described within sections 3.2.1–3.2.5.

3.2.1 5G Smart Warehousing

The Marine Corps Logistics Base (MCLB) Project will develop a 5G-enabled smart warehouse focused on vehicular storage and maintenance to increase the efficiency and fidelity of MCLB Albany logistic operations, including identification, recording, organization, storage, retrieval, and inventory control of materiel and supplies. "Additionally, the project will create a proving ground for testing, refining, and validating emerging 5G-enabled technologies [10]".

3.2.2 Distributed Command and Control

Testing and experimentation at Nellis Air Force Base in Nevada has the objective to develop a testbed for the utilization of 5G systems to assist in aviation, space, and cyberspace casualty, while improving command and control (C2) survivability. Specifically, a 5G network will be employed to disaggregate and mobilize the existing C2 architectures in an agile-combat-employment scenario. This testing takes place with AT&T as a partner providing a high-capacity and low-latency mobile 5G environment.

3.2.3 Augmented and Virtual Reality

A project being tested at the Joint Base Lewis-McChord (JBLM) in Washington. "The objective of this project is to rapidly field a scalable, resilient, and secure 5G network to provide a testbed for experimentation with a 5G-enabled, augmented reality/virtual reality (AR/VR) capability for mission planning, distributed training, and operational use. [10]".

3.2.4 5G Smart Warehousing

A project at the U.S. Naval Base San Diego (NBSD) has the objective to develop a 5G-enabled smart warehouse focused on transshipment connecting land facilities and naval divisions to enhance the efficiency and fidelity of naval logistic performance, which include identification, recording, organization, storage, retrieval, and transportation of material, supplies, and other goods. Additionally, the project will create a proving ground for testing, refining, and validating emerging 5G-enabled technologies.

3.2.5 5G Dynamic Spectrum Sharing Utilization

Hill Air Force Base in Utah has begun to investigate the technical feasibility, methodologies, and utility of spectrum sharing and coexistence with diverse 5G networks in a band of critical importance within commercial industry. This event demonstrates the DoD's commitment to promote U.S. economic competitiveness in a beyond-5G era by offering an allocated spectrum for use by nonfederal (commercial) systems.

Next, further examples of other 5G DoD use cases from the U.S. Army, as well as the Defense Advanced Research Projects Agency (DARPA) and MITRE, are provided in the following sections 3.2.6 through 3.2.9. These additional use cases show the breadth of work being done in the 5G space to include tactical networking, open-source initiatives, and a threat-based framework.

3.2.6 5G++ Adapting 5G for Tactical mmWave Networks

5G++ Adapting 5G for tactical mmWave networks is an ongoing U.S. Army Phase 2 Small Business Innovation Research (SBIR) Program that started in February 2021, with a projected end date of August 2022 [11]. The objective of this effort is to address the critical need and suggest creating 5G++ as a mmWave radio model that modifies 5G to tactical domain by including jamming blocking, upgraded low probability of interception/low probability of detection (LPI/LPD), and secure network communications. 5G technology is targeting very high throughput, low power, and low latency, which are expected to benefit not only commercial but also tactical communications. Operating in mmWave bands provides high bandwidths to meet the ever-growing throughput demands of emerging tactical applications in shared spectrum environments. However, 5G waveform, as it is, does not satisfy the U.S. Army's requirements on jamming resistance, LPI/LPD, and security, as well as support of device-to-device (D2D) ad-hoc networking mode without relying on cellular infrastructure. "Novel sets of algorithms across physical, link/MAC, and network layers need to be implemented on mmWave, software-defined radio (SDR) platforms, along with 5G protocol

stack, and extensively tested to accelerate the transfer of 5G benefits to the tactical domain [11]".

3.2.7 5G Technologies Implementation in a U.S. Army Tactical Environment Technical Program Support

The Project Executive Office for Command, Control, Communications Tactical (PEO C3T) conducted a study to assess current and potential communications technologies to integrate in future U.S. Army tactical networks. This study identifies and summarizes 5G features and technologies that have been standardized, as well as emerging features that have not yet been standardized. It also identifies and summarizes the various use cases and key performance indicators (KPIs) associated with existing and planned U.S. Army tactical networks. This study further narrows down the 5G features and technologies by identifying which features are under heavy commercial development and are likely to have similar applications and use cases in their commercial and DoD-deployed instances. Finally, it concludes by recommending additional research investments needed to further advance the 5G technologies for potential use in various U.S. Army tactical environments (see the September 2020 published report [12]).

3.2.8 Open, Programmable, Secure 5g (OPS-5g)

DARPA's Open, Programmable, Secure 5G (OPS-5G) project is pursuing research leading to the development of a portable standards-compliant network stack for 5G mobile that is open source and secure by design. OPS-5G seeks to create open-source software and systems that enable secure 5G and subsequent mobile networks such as 6G. OPS-5G is beneficial because [13]:

> The signature security advantage of open-source software is increased code visibility, meaning that code can be examined, analyzed, and audited, either manually or with automated tools. In addition, the portability of open source serves as a desired side effect to decouple the hardware and software ecosystems. This significantly raises the difficulty of a supply-chain attack and eases the introduction of innovative hardware into the market.

The program seeks to enable a "plug-and-play" approach to various software components, which reduces reliance on untrusted technology sources [13]. DARPA's OPS-5G program will create open-source software and systems allowing dependable 5G and follow-on cellular signals. "OPS-5G creates capabilities to address feature velocity in open-source software, a trillion-node botnet of things, network slicing on suspect gear, and adaptive adversaries operating at scale [14]". The long-term objective is a U.S.-friendly ecosystem [14]. This project started in September 2020, with an estimated completion date of September 2024.

3.2.9 MITRE Five-G Hierarchy of Threats (FiGHT) Framework

MITRE Five-G Hierarchy of Threats (FiGHT) is a threat-based framework to assess the confidentiality, integrity, and availability of 5G networks, as well as the devices, weapon systems, and applications using them for the United States and its partners. FiGHT leverages concepts from existing security frameworks and builds upon them by exploring 5G building blocks and the associated hypothesized threats, considering U.S. government critical assets. This enables cyber investment planning and prioritization by applying a comprehensive 5G threat framework to specific use cases and architectures, allowing quantification of risks and prioritization of mitigations to ensure 5G can revolutionize with minimum compromise. This work started in fiscal year 2021 (FY21), with plans for completion in FY24 [15].

4.0 5G Challenges

4.1 COST

The first major challenge of 5G deployment is the cost. Similar to investing in any other next-big technology or even a company-wide update to the next version of MS Windows, it is expensive in more ways than just currency. Considering workforce, training, time, raw materials, testing, and any other part of the life cycle of a new technology, investing and deploying 5G will be the technology with the biggest price tag and the largest payout.

In late 2019, it was stated that "the real cost of rolling out and implementing 5G telecoms technology across all sectors of the economy worldwide is expected to reach at least $2.7 trillion by the end of 2020," according to research by Greensill, the leading provider of working capital finance [16]. The finances and corresponding challenges include the following [16]:

> The telecoms sector requires an estimated $1 trillion of investment for infrastructure upgrades to accommodate 5G, a number widely accepted across the industry. Many companies are facing significant challenges in meeting these huge funding requirements, as traditional banks alone cannot provide all the necessary funding.

Figure 5 details the breakdown of the $2.7 trillion to include subtotals for each portion.

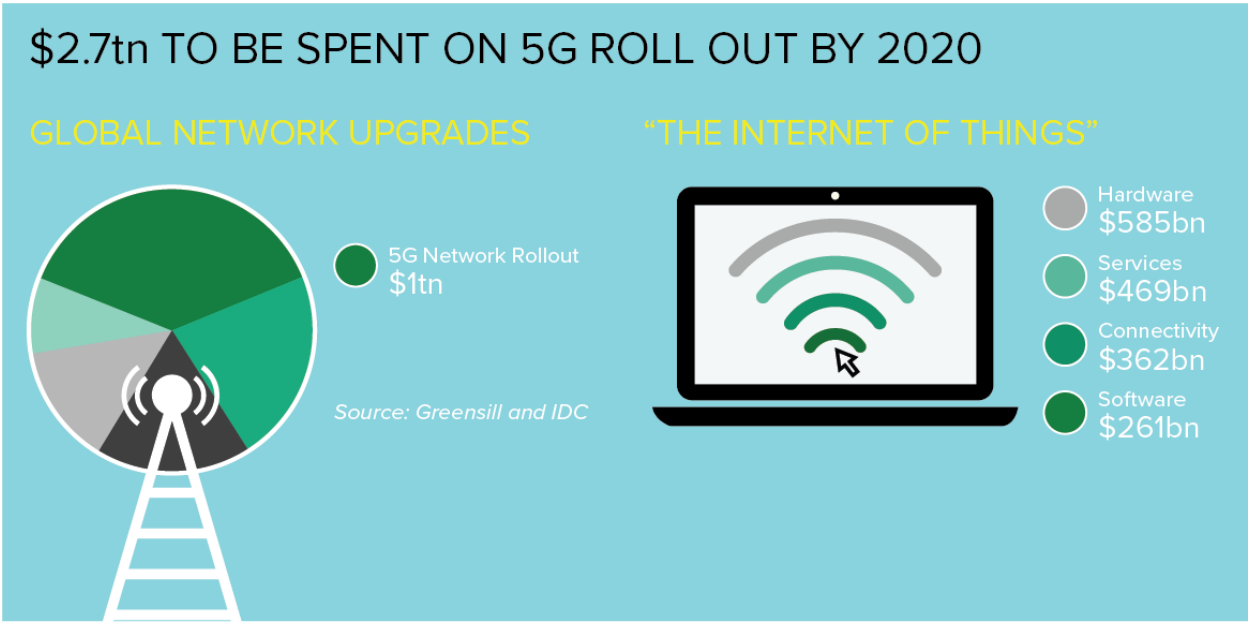


Figure 5: Cost of 5G Rollout.

4.2 CYBERSECURITY

4.2.1 Assessments

The DoD will take advantage of assessments that are specially catered to the given system to determine the potential effect that unsecure networks and devices could have on DoD operations. These assessments are developed by the Cybersecurity and Infrastructure Security Agency (CISA) and the DoD for the use of testing federal agencies with 5G capabilities. Some portions of general cybersecurity testing are automated but will also require strenuous testing by hand, as 5G vulnerabilities are still appearing every day. This assessment process also allows for the potential to learn about threat developments in 5G attack vectors, thus providing an extra mitigation layer to potential threats to come. Naturally, this assessment process would also provide for better relations between military and private sectors as cooperation and connectivity will be key to harnessing the full potential of 5G technology.

4.2.2 Operate Through

The DoD has developed a concept label "Operate Through" within the 5G Implementation Strategy Plan to represent the resilience of the DoD's use of 5G technology. The DoD 5G "Operate Through" concept represents the ideology and methodology that the DoD can gain significant advantages by simply leveraging preexisting 5G infrastructure. It is not always possible or efficient to create new infrastructure for every operation of the DoD. Instead, taking advantage of that which is already established and functional is much more beneficial. Of course, these preexisting systems can be adapted and retrofitted to meet the goals of the

DoD, but having a baseline setup to begin operations on the move is the key to success. The "Operate Through" concept is divided into four distinct categories of network infrastructure, according to the DoD 5G Strategy Implementation Plan [9].

The first and least challenging of the four is the necessity for the DoD to be able to conduct sustained operations on the existing U.S. telecommunications infrastructure. The second category requires that DoD operations in coalition partner countries operate through the coalition partners national communication system. In the first two categories, long-term bases and spontaneous developments could both benefit from access to preexisting infrastructure. The third of the four categories is more challenging than the first two and covers the potential operability over "gray zone" network infrastructure that is influenced or controlled by organizations considered incompatible with DoD mission objectives. The term "grey zone" normally is defined as a term of warfare, a set of activities that occurs between peace/cooperation and war/conflict. For this case, however, it is more likely alluding to the lack of certain or absolute control over the operational network or infrastructure at hand. The fourth and final category is the ability for the DoD to operate in contested areas. Overall, these four categories consist of U.S., ally, grey, and enemy infrastructure operability.

While the DoD requires the ability to operate in all scenarios, it is important to understand that each of the categories of infrastructure present their own unique set of challenges and security threats. The amount of potential attack vectors and general vulnerabilities that can be exposed and acted on become exponentially larger when considering a telecommunications technology that is presented and used on a global scale. Each category offers its own level of trust that can be associated with the given system that the DoD is expected to be operational on. While each system will have its own level of security on it, the DoD must assume that nearly all underlying networks are untrusted. This concept also applies to those who are operating the network as well. The DoD is placing emphasis on techniques that ensure that U.S. forces can operate through adversary threats to 5G networks, no matter the location, by leveraging a variety of components, such as dynamic spectrum access, mitigation of adversary threats, and the full exploitation of 5G technology.

4.2.3 Threat intelligence

The DoD will have a strong focus on developing an in-depth understanding of the potential threats and vulnerabilities that 5G technologies will introduce on a global and local scale. With the added consideration of adversary use of these technologies, the capabilities and intent to use this technology maliciously poses a major concern to the DoD as well. Understanding adversary intentions, technical developments, and networks/infrastructure will give insight to how the United States, allies, and partner collaborations should approach the new technology. Similarly, to any new technology or new iteration of something established prior, there will always be the potential for new threats as the cyber landscape is everchanging. While 5G

presents the opportunity for a much more secure operation when compared to preexisting commercial wireless networks, these features must also be balanced and considered with the new threats and attack vectors they open. The DoD also must consider that despite 5G standards usually incorporating these new security standards and features, it does not inherently mean they actively exist within every system. Due to this, among many other factors, the DoD will need to understand 5G security from systemic vulnerabilities and potential adversary threats.

According to the DoD 5G Strategy Implementation Plan, the DoD, in collaboration with allies and interagency partners, will accomplish this through four different methods. The first is the development of techniques to identify, track, and mitigate threats and vulnerabilities that arise from different choices, configurations, and combinations of network equipment, software components, and deployment environments. The next method is providing evidence-based information to regulatory agencies, standards groups, and network operators to make informed choices on network equipment. The third demonstrates how vulnerabilities in underlying hardware could be exploited by an adversary to impact 5G-enabled capabilities and operations. The fourth and final methodology is tracking how novel 5G features, such as network slices and spectrum sharing, are being used and identify threats and vulnerabilities associated with these features. With the use of these methodologies, the DoD can provide and understand threat intelligence on 5G networks globally, no matter the environment physical or virtual environment.

4.2.4 Minimizing 5G Infrastructure Risk

As 5G technology develops, the infrastructure surrounding supply chains can be more easily reduced and managed through cooperation with allies and interagency connections. Further steps are being taken by the DoD to ensure that the risk to 5G infrastructure is minimized through standards that guarantee the DoD will not acquire, import, transfer, install, deal in, or use 5G technologies that are produced by foreign adversaries. This can be found in targeted executive orders such as Order 13873, Section 889 of the FY National Defense Authorization Act, which prohibits federal procurement of certain Chinese telecommunications equipment and services.

In further preparation for potential supply chain events that may occur during the upswing of 5G implementation and deployment, the DoD has been tasked with the development and execution of a detailed plan for supply chain risk management (SCRM), as detailed in “Securing Defense-Critical Supply Chains – An action plan developed in response to President Biden’s Executive Order 14017” [17]. The DoD is developing risk-management strategies, guidelines, and procedures in cooperation with other agencies, industry, and standard bodies to promote and establish the best possible guidance for 5G deployment. Recently, the DoD has become a member of the Federal Acquisition Security Council (FASC), whose purpose is to identify and

recommend supply chain, risk-mitigation strategies that support a comprehensive and consistent approach across the whole of government. FASC efforts will directly apply to mitigating 5G supply chain risk.

4.2.5 Security Assessments

CISA and the DoD have recently released their 5G Security Evaluation Process Investigation Study for federal agencies [18]. This document demonstrates new features, capabilities, and services offered by 5G cellular network technologies and how they can transform mission and business operations. The experiment gives a recap of the suggested 5G Security Evaluation Process and executes this process to a private 5G network case study to show contemplations for every stage in the entire process. The study is a joint effort among CISA, the Department of Homeland Security's (DHS) Science and Technology Directorate, and the DoD's Under Secretary of Defense for Research and Engineering. This study has provided an overview of the proposed 5G Security Evaluation Process and applies it to a private 5G network use case to demonstrate considerations for each step of the process.

The 5G Security Evaluation Process itself consists of five steps. The first step is defining the federal use case. Second is to identify the assessment boundary. These first two steps are simply establishing and identifying what the system is and at what limit testing can be done as far as system diversity, such as single boundary, system of systems, or something more hybrid. The third step involves identifying the security requirements of the system. This step is multistage and includes a high-level threat analysis of each 5G subsystem and cybersecurity requirements that would potentially need to be addressed. This step requires a thorough understanding of systems and technologies employed within the assessment boundary and includes a risk-assessment analysis. Categories of such technologies that would need to be assessed include user equipment, 5G radio access networks (RANs), 5G core networks, deployment environments, and operational responsibility considerations. Step four involves mapping the prior steps security requirements in accordance with federal guidance and standards. Federal security requirements extend beyond those that exist in international industry specifications. These systems may be required to comply with the following capabilities: SCRM; risk management framework (RMF); federal information processing standards (FIPS); system hardening; architectural constructs; roots of trust via DoD public key infrastructure (PKI) and identity, credential, and access management (ICAM); 5G infrastructure security guidance via the National Security Agency (NSA)-CISA; and continuous diagnostics and mitigation programs via DHS and the National Institute of Standards and technology (NIST). The fifth and final step is to assess security guidance gaps and the alternative solutions to these gaps. This step examines the alignment between security capabilities and available federal security guidance to guide assessment and authorization (A&A) activities. If security capabilities are required to mitigate identified threats and reduce risk to the federal enterprise, there must be a means to assess the effectiveness of their implementation.

4.2.6 Zero Trust

With 5G technology becoming widespread and enabling the connection of multiple devices, many of which are untrusted, there is an increased demand for security. Sometimes known as perimeterless security, the zero-trust security model is an approach to the design and implementation of information technology/information communications technology (IT/ICT) systems, with the main concept to "never trust, always verify." NIST SP 800-207 defines zero trust as a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least-privilege, per-request access decisions in information systems and services in the face of a network viewed as compromised [19].

Most importantly, 5G as standardized by 3rd Generation Partnership Project (3GPP) gives mobile network operators a standardized and well-defined way to deploy zero-trust functions. Examples include authentication and authorization of application programming interface (API) usage and protected communication between and to the 5G network functions using hypertext transfer protocol secure (HTTPS), datagram transport layer security (DTLS), or internet protocol security (IPsec).

4.3 STANDARD AND POLICIES

As 5G technology becomes more prevalent and interwoven into the current systems and infrastructure, it is important to ensure that the standards and policies surrounding it keeping the technology in check. As with any other technology of the modern era, it is always changing and adapting to better fill its role. As 5G technology continues to be developed and deployed throughout various systems, it will begin to be regulated and structured around policies and standards set by several bodies globally. At the forefront is the 3GPP, which is an umbrella term for several standards organizations that develop protocols for mobile telecommunications. "3GPP is a consortium with seven national or regional telecommunication standards organizations as primary members (organizational partners) and a variety of other organizations as associate members (market representation partners) [20]". The seven 3GPP organizational partners are from countries throughout Asia, Europe, and North America. The 3GPP organizes its work into three different streams—radio access networks, services and systems aspects, and core network and terminals [20].

4.4 INTERNATIONAL COLLOBARATION

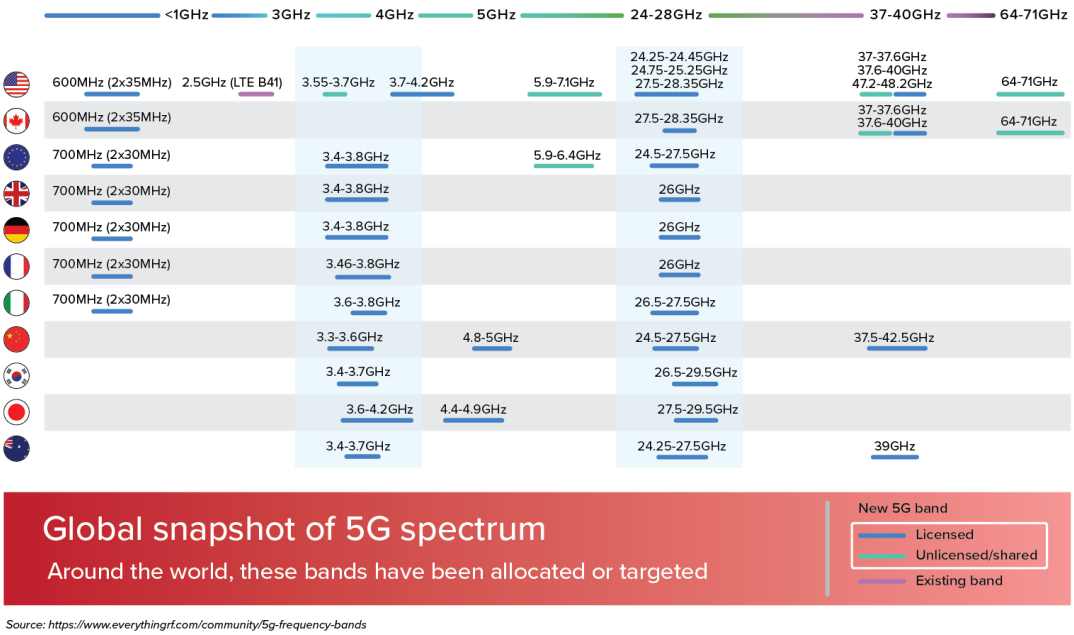
The DoD must promote a shared understanding of the importance of protecting these systems and 5G infrastructure while also recognizing the severity of threats that pose possible unauthorized access to these networks. Nations are already beginning to invest in 5G auctions and infrastructure. As 5G band auctions continue and different bands start becoming standard for different powers of the globe, it is important that, regardless of which the DoD uses, accessibility to all spectrums is possible with DoD-owned equipment. This is to ensure that

trusted, secure, and private access to these channels can be granted without the use of a proxy country or its equipment. The Prague Proposals on 5G Security [21] and the National Strategy to Secure 5G [22] both provide further information on taking on this task of securing 5G networks and platforms, while accounting for outside powers.

In the current state, the telecom business is not near its goal of harmonized, acceptable, 5G spectrum assets. There are two camps—one is favored by China and the other by the United States. Disagreements are not settled easily at this stage, as there is a first mover advantage in developing mobile wireless generations.

The battle hovers around the sub-6-GHz and mmWave bands. China is looking toward 3.5 GHz, whereas the United States is focusing on multiple millimeter bands.

The mid band, particularly the 3.5 GHz band that ranges from 3.3 to 3.8 GHz, is the most sought-after band for use as a core band for 5G. That is due to the band's availability and lower deployment costs as compared to mmWave bands. China has already assigned 200 MHz in this mid band. Contrastingly, both Japan and South Korea are delving in mid and mmWave bands. The rest of the world is playing catch-up on 5G spectrum assignments [23]. A global snapshot of 5G spectrum is shown in Figure 6 to include licensed, unlicensed, shared, and existing bands.



Source: https://www.everythingrf.com/community/5g-frequency-bands

Figure 6: Global 5G Spectrum.

4.5 ELECTROMAGNETIC INTERFERENCE

4.5.1 Aviation Safety

The U.S. Federal Aviation Administration has given its two cents on electromagnetic interference and aviation [24]:

> …(FAA) has warned that radar altimeters on aircraft, which operate between 4.2 and 4.4 GHz, might be affected by 5G operations between 3.7 and 3.98 GHz [24]. This is particularly an issue with older altimeters using RF filters which lack protection from neighboring bands.

Radio altimeters generate very accurate data regarding an aircraft's altitude. The information from radio altimeters corresponds with other safety technologies on the plane, including navigation tools, geographic awareness, and crash-avoidance systems. Therefore, the FAA must impose regulations on flight's using specific kinds of radio altimeter technologies that neighbor antennas in 5G networks.

These safety regulations could affect flight schedules and operations. Consequently [25]:

> The FAA rushed to test and certify radar altimeters for interference so that planes could be allowed to perform instrument landings (e.g., at night and in low visibility) at affected airports. By January 16, it had certified equipment on 45% of the U.S. fleet and 78% by January 20, 2022.

4.5.2 Weather Forecasting

The spectrum used by various 5G proposals, especially the n258 band centered at 26 GHz, will be near that of passive remote sensing, such as by weather and Earth observation satellites, particularly for water-vapor monitoring at 23.8 GHz [26]. Water-vapor data is pumped into an arsenal of weather models and is a foundation of improved accuracy in the genesis of storms and areas downwind that are most likely to take the worst hits.

"Acting NOAA director Neil Jacobs testified before the House Committee in May 2019 that 5G out-of-band emissions could produce a 30% reduction in weather forecast accuracy [27]." In March 2019, the U.S. Navy wrote a memorandum warning of deterioration and made technical suggestions to control band bleed-over limits for testing and fielding and for coordination of the wireless industry and regulators with weather forecasting organizations [27].

At the 2019 quadrennial World Radiocommunication Conference, scientists recommended a solid buffer of -55 dBW, while U.S. regulators only recommended a restriction of -20 dBW [28]. The International Telecommunication Union (ITU) agreed on a median -33 dBW until September 1st, 2027, and thereafter a regulation of -39 dBW. However, this so-called higher standard is still much weaker than that advocated for by scientists, initializing deterrents from

the World Meteorological Organization that the ITU standard, at 10× less strict than its suggestion, produces the "potential to significantly degrade the accuracy of data collected" [29].

5.0 CONCLUSION

In this report, CSIAC provides an overview of 5G technology to include its hardware, software, and RF components. 5G is an enabling technology that is quickly becoming ubiquitous. Readers are supplied with a snapshot of the status of 5G deployments throughout the world. Spectrum will play a key role in the operation, development, and rollout of 5G. The unique impact of 5G within the DoD is identified through policy, use cases, and ongoing efforts. 5G technology can enhance DoD decision-making and capabilities all the way down to the tactical edge of the battlefield. The speed of 5G will expand DoD's ability to link multiple systems into tactical and enterprise networks, while sharing information in real time. The improved connectivity provided by 5G will enable many new technologies and new missions. Lastly, some of the challenges and difficulties of 5G implementation such as cost and cybersecurity are discussed.

REFERENCES

[1] Thales Group. "5G Technology and Networks (Speed, Use Cases, Rollout)." https://www.thalesgroup.com/en/markets/digital-identity-and-security/mobile/inspired/5G, accessed 14 June 2022.

[2] Federal Communications Commission. "FCC Announces Winning Bidders of 3.7 GHz Service Auction." https://www.fcc.gov/document/fcc-announces-winning-bidders-37-ghz-service-auction, accessed 14 June 2022.

[3] Ericsson. "Ericsson Mobility Report." https://www.ericsson.com/en/reports-and-papers/mobility-report, accessed 14 June 2022.

[4] Kavanagh, S. "What Is 5G New Radio (5G NR)." https://5g.co.uk/guides/what-is-5g-new-radio/, accessed 14 June 2022.

[5] StartUs Insights. "5G Technology: The Current State & Development." https://www.startus-insights.com/innovators-guide/what-you-need-to-know-about-the-current-state-of-5g-technology/, accessed 14 June 2022.

[6] GSA. "LTE and 5G Market Statistics – 8 April 2019." https://gsacom.com/paper/lte-5g-market-statistics-8-april-2019/, accessed 14 June 2022.

[7] Berry, I. "Top 10 Global 5G Infrastructure Companies." https://mobile-magazine.com/top10/top-10-global-5g-infrastructure-companies, accessed 14 June 2022.

[8] U.S. Department of Defense. "Department of Defense (DoD) 5G Strategy." Washington, DC, 2 May 2020.

[9] U.S. Department of Defense. "Department of Defense 5G Strategy Implementation Plan." Washington, DC, 15 December 2020.

[10] U.S. Department of Defense. "DoD Announces $600 Million for 5G Experimentation and Testing at Five Installations." https://www.defense.gov/News/Releases/Release/Article/2376743/dod-announces-600-million-for-5g-experimentation-and-testing-at-five-installati/, accessed 14 June 2022.

[11] "STTR 5G++ – Adapting 5G for Tactical mmWave Netwo… – GovAlpha." https://www.govalpha.com/contract/W911NF21C0015/, accessed 14 June 2022.

[12] Lawton, W. "5G Technologies Implementation in an Army Tactical Environment Technical Program Support." DTIC accession no. AD1117815, Distribution B, U.S. Army Program Executive Office for Command, Control, Communications Tactical, Aberdeen Proving Ground, MD, 21 September 2020.

[13] Patel, T. "Open, Programmable, Secure 5G." https://www.darpa.mil/program/open-programmable-secure-5g, accessed 14 June 2022.

[14] GovTribe. "Open Programmable Secure 5G (OPS-5G)." https://govtribe.com/opportunity/federal-contract-opportunity/open-programmable-secure-5g-ops-5g-hr001120s0026, accessed 14 June 2022.

[15] Stephenson, A., and M. Vanderveen. "MITRE FiGHT Ensuring a Secure & Resilient 5G." DTIC Accession no. AD1156242, Distribution A, MITRE Corporation, VA, October 2021.

[16] Doran, J. "5G Roll-Out Will Need $2.7tn Investment in Next Two Years." https://www.prnewswire.com/news-releases/5g-roll-out-will-need-2-7tn-investment-in-next-two-years-300801153.html, accessed 14 June 2022.

[17] U.S. Department of Defense. "Securing Defense-Critical Supply Chains." An action plan developed in response to President Biden's Executive Order 14017, Securing Defense-Critical Supply Chains, accessed 14 June 2022.

[18] Sritapn, V., D. Massey, and B. Talbot. "5G Security Evaluation Process Investigation: Version 1, May 2022." https://www.cisa.gov/sites/default/files/publications/5G_Security_Evaluation_Process_Investigation_508c.pdf, accessed 14 June 2022.

[19] National Institute of Standards and Technology. "Zero Trust Architecture." NIST Special Publication (SP) 800-207, Gaithersburg, MD, August 2020.

[20] 3GPP. https://www.3gpp.org/, accessed 14 June 2022.

[21] Vystrcil, M., K. Rehka, K. Andrews, Y. Hendel, and J. Lopez. "The Prague Proposals, The Chairman Statement on Cyber Security of Emerging and Disruptive Technologies." Prague 5G Security Conference 2021, Prague, CZ, December 2021.

[22] National Telecommunications and Information Administration. "National Strategy to Secure 5G Implementation Plan | National Telecommunications and Information Administration." https://www.ntia.gov/5g-implementation-plan, accessed 14 June 2022.

[23] Turner, A. "5G – The Critical Need for Harmonised Spectrum." *Mobile Europe.* https://www.mobileeurope.co.uk/5g-the-need-for-harmonised-spectrum/, accessed 14 June 2022.

[24] Levin, A. "U.S. FAA Issues Safety Alert on 5G Interference to Aircraft." Bloomberg.com. https://www.bloomberg.com/news/articles/2021-11-02/u-s-faa-issues-safety-alert-on-5g-interference-to-aircraft, accessed 14 June 2022.

[25] Federal Aviation Administration. "5G and Aviation Safety." https://www.faa.gov/5g, accessed 14 June 2022.

[26] GCN. "What's Needed to Keep 5G From Compromising Weather Forecasts." https://gcn.com/emerging-tech/2020/09/whats-needed-to-keep-5g-from-compromising-weather-forecasts/315369/, accessed 14 June 2022.

[27] Paul, D. "Some Worry 5G May Pose Huge Problems for Weather Forecasting" *Columnists*, https://buffalonews.com/opinion/columnists/some-worry-5g-may-pose-huge-problems-for-weather-forecasting/article_e96085df-6a1f-5212-a040-3d0659bf3e6f.html, accessed 14 June 2022.

[28] Witze, A. "Global 5G Wireless Deal Threatens Weather Forecasts." *Nature*, vol. 575, no. 7784, pp. 577–577, November 2019.

[29] World Meteorological Organization. "WMO Expresses Concern About Radio Frequency Decision." https://public.wmo.int/en/ media/news/wmo-expresses-concern-about-radio-frequency-decision, accessed 14 June 2022.

BIBLIOGRAPHY

Brain, M. "How the Radio Spectrum Works." *HowStuffWorks*, https://electronics.howstuffworks.com/radio-spectrum.htm, accessed 14 June 2022.

Medin, M., and G. Louie. "The 5G Ecosystem: Risks & Opportunities for DoD." Defense Innovation Board, Washington, DC, DTIC accession no. AD1074509, April 2019.

Midatala, S. "Top 7 Challenges Faced During 5G Network Deployment – TelecomLead." https://www.telecomlead.com/5g/top-7-challenges-faced-during-5g-network-deployment-97331, accessed 14 June 2022.

Muro, B. "These COTS SDR System Solutions Focus on 5G | Electronic Design." https://www.electronicdesign.com/technologies/embedded-revolution/article/21808417/these-cots-sdr-system-solutions-focus-on-5g, accessed 14 June 2022.

Rajiv. "What Are the Components of 5G Technology." *RF Page*, https://www.rfpage.com/what-are-the-components-of-5g-technology/, accessed 14 June 2022.

Siegel, E. "The Science of Why 5G is (Almost) Certainly Safe for Humans." *Forbes*, https://www.forbes.com/sites/startswithabang/2019/11/01/the-science-of-why-5g-is-almost-certainly-safe-for-humans, accessed 14 June 2022.

Mobile World Live. "High-Precision 5G Whitebox Solutions Make COTS-Based Open Virtual RAN Viable." https://www.mobileworldlive.com/latest-stories/high-precision-5g-whitebox-solutions-make-cots-based-open-virtual-ran-viable, accessed 14 June 2022.

U.S. Department of Defense. "DoD Establishes 5G and Future Generation Wireless Cross-Functional Team." https://www.defense.gov/News/Releases/Release/Article/2960806/dod-establishes-5g-and-future-generation-wireless-cross-functional-team/, accessed 14 June 2022.

U.S. Department of Defense. "Department of Defense and NTIA Launch 5G Challenge to Accelerate Development of Open 5G Ecosystem." https://www.defense.gov/News/Releases/Release/Article/2990687/department-of-defense-and-ntia-launch-5g-challenge-to-accelerate-development-of/, accessed 14 June 2022.

BIOGRAPHIES

PHILIP PAYNE

Philip Payne is the Cybersecurity & Information Systems Information Analysis Center (CSIAC) Technical Lead for SURVICE Engineering Company. A Certified Information Systems Security Professional (CISSP) and Security+ certified, he comes from a rich background in cybersecurity with the Command, Control, Computers, Communications, Cyber, Intelligence, Surveillance, and Reconnaissance (C5ISR) Center (formerly Communications-Electronics Research, Development, and Engineering Center [CERDEC]), where he led a world-class, cross-domain solution (CDS) lab. He performed lab-based security assessments on U.S. Army CDSs going through the Secret and Below interoperability CDS certification and accreditation approval process. He was a key member of the Information Security (INFOSEC) Branch, which has made a myriad of contributions in cyberspace for the U.S. Department of Defense. In his previous position at SURVICE, he was the Senior Cybersecurity Engineer of the Cyber Research and Development team supporting the Data Analysis Center (formerly the U.S. Army Material Systems Analysis Activity [AMSAA]) on early acquisition cybersecurity assessments for U.S. Army systems. Mr. Payne holds a B.S. and M.S. in computer engineering from Johns Hopkins University and Polytechnic University, respectively.

RYAN FOWLER

Ryan Fowler is a CSIAC Research Analyst for SURVICE Engineering Company, where he works alongside experts in the field to answer technical inquiries and assists in developing technical information for cyberspace. He supports and helps develop dissemination products, such as technical inquiry reports, webinars, and state-of-the-art reports. Mr. Fowler holds a B.S. and M.S. in cybersecurity, with a focus in cyber forensics, from Frostburg State University and Towson University, respectively.