Fifth Generation Wireless Development in Great Power Competition

Department of Defense Implications and Policy Recommendations

Brigadier General Darrin Leleux
Captain Robert Woodruff
Colonel Kristy Perry
Commander David Bergesen

ABSTRACT

The advent of fifth generation (5G) wireless technology represents new global opportunities and risks that must be considered in the context of reemerging long-term strategic competition with China and Russia, which are intent on shaping a world consistent with their authoritarian models.[1] To deal with this challenge, several bodies – notably the Defense Science Board (DSB), the Defense Innovation Board (DIB), and the European Commission (EC) – have recently offered recommendations on how leaders of large organizations, including nation-states in the case of the EC recommendations, should adopt and field this new communications technology. This article evaluates these recommendations to synthesize a possible way ahead for the Department of Defense (DoD); however, DoD cannot do this alone. A whole-of-nation approach is required for the United States to lead global change and gain the "first-mover" advantage.[2]

INTRODUCTION

The development of fifth generation (5G) wireless technology security is critical for United States (US) national defense and economic security. 5G technology represents a leap forward in the speed and volume of data transmission, as well as a drastic reduction in communication latency, which enables new technologies and operational methodologies. It also has the potential to improve security by interlinking intelligence, surveillance, reconnaissance, and command and control systems by delivering information in real time.[3] The Department of Defense (DoD) must have a strong voice in the development and implementation of 5G technology and associated security measures in order to prevent its adversaries from conducting intellectual property theft, interfering with DoD operations, and compromising the security of DoD personnel, information, equipment, and operational

Brigadier General Darrin Leleux, U.S. Air Force, is currently serving as Deputy Director of the Electromagnetic Spectrum Operations Cross-Functional Team. He was commissioned through the Reserve Officer Training Corps (ROTC) and earned a Bachelor of Science in Electrical Engineering degree from the University of Southwestern Louisiana in 1989, a Master of Science in Computer Engineering from the University of Houston at Clear Lake in 1998, and a Doctor of Philosophy in Electrical Engineering from Rice University in 2002. Prior to his current assignment, General Leleux served as Deputy Director of Strategy, Defense and Capabilities in the Office of the Secretary of Defense for Cyber Policy.

capabilities that will rely on 5G. Since this is a whole-of-nation issue, the U.S. Government (USG) must deliberately incorporate 5G security into conversations with foreign partners, industry, and DoD to evaluate carefully the role of 5G technology in its own, as well as its coalition partners,' communication architectures and operational capabilities.

It is critical that partner governments and domestic/international industries understand the potential risks of using 5G hardware and software from companies such as Huawei and ZTE – both Chinese-owned companies. Beyond the price of initial network investment, leaders should also consider the costs incurred through security compromises and remediation efforts – such as loss of capital, intellectual property, or markets – if strong security is not built into 5G systems and network segments from the beginning. The USG should lead a national effort and continue to be engaged in the establishment of 5G standards which will require the extensive and persistent presence in standard-setting organizations and bodies such as the 3rd Generation Partnership Project (3GPP) and the Institute of Electrical and Electronics Engineers (IEEE). Furthermore, since part of the electromagnetic spectrum that will be utilized for 5G overlaps with DoD and USG public safety frequencies, creative and viable new approaches should be developed with industry to operate dynamically within these specific cooperation segments of the wireless spectrum. Finally, it is critical for global scale 5G systems to be built to the highest security standards to safeguard intellectual property, intelligence, information, and equipment not only in DoD but throughout the US.

In this article, we review and analyze the 5G recommendations made by different organizations to identify commonalities and differences that may be useful in synthesizing a way forward for DoD. We evaluated recommendations by the Defense Innovation Board (DIB), the Defense Science Board (DSB),

Captain Robert Woodruff, U.S. Navy, is currently serving as Information Operations Branch Head at NATO Maritime Command (Headquarters Allied Maritime). He was commissioned through ROTC at Texas A&M University at Galveston in 1999. He earned a Bachelor of Science degree in Maritime Systems Engineering degree from Texas A&M University at Galveston and a Master of Arts in National Security and Strategic Studies from the U.S. Naval War College in 2011. Prior to his current assignment, Captain Woodruff served as Executive Officer at Navy Cyber Warfare Development Group and Deputy Commander of Task Force 1090.

and the European Commission (EC). These organizations offered recommendations in 2019 for large organizations such as DoD and the European Union (EU) to consider when adopting and fielding this new communications technology. We evaluate each of their recommendations in turn with an emphasis on those offered by the DIB, and then synthesize a possible way ahead for DoD.

ANALYSIS OF DEFENSE INNOVATION BOARD RECOMMENDATIONS

The DIB was created in 2016 to bring the technological innovation and "best practices" of Silicon Valley to the US military.[4] They completed a study on "The 5G Ecosystem: Risks & Opportunities for DoD" and published their recommendations in April 2019.[5] The study offered three unclassified recommendations for DoD related to spectrum management, preparing for a "post-Western" wireless ecosystem, and developing trade and supply chain mitigations. In the next few paragraphs, we analyze the first two recommendations and offer ideas to advance the thinking on these topics. The third recommendation, while extremely important, is not included in our analysis as this has been covered extensively in other articles and the news media.

> Recommendation #1
>
> DoD needs a plan for sharing sub-6 GHz spectrum to shape the future 5G ecosystem, including an assessment of how much and which bandwidths need to be shared, within what time frame, and how that sharing will impact DoD systems.

Spectrum sharing and shaping the 5G ecosystem is much larger than just a DoD problem. Collaboration between the USG and the commercial sector is critical to effectively innovate and develop a national plan. The Trump administration recognized 5G as a next-generation technology in its 2017 National Security Strategy, highlighting the criticality of the US becoming a first mover and global leader. The administration designated

Colonel Kristy Perry, U.S. Army, is currently serving in United States Cyber Command (USCYBERCOM). She was commissioned through ROTC at Southwest Missouri State University in Springfield in 2000. She earned a Bachelor of Science in Business degree from Southwest Missouri State University and a Master of Science in International Relations from North Carolina State University in 2009. Prior to her current assignment, Colonel Perry served as an Army War College Fellow at the National Security Agency.

the US private sector to lead national efforts in 5G developments.[6] In October 2018, President Trump issued a presidential memorandum to create a National Spectrum Strategy.[7] In April 2018, the National Telecommunications and Information Administration (NTIA) announced plans to develop a collaborative strategy, including spectrum sharing, selling, and development of mid- and high-frequency bands.[8] The National Spectrum Strategy team is comprised of federal and non-federal stakeholders, in addition to public-private partnerships, relying on a flexible spectrum management regulatory model and research establishing a comprehensive set of immediate and long-term requirements[9]. As then NTIA Administrator and leader of the strategy development, David J. Redl stated, "While commercial needs are extensive, we must balance that against government's expanding needs for national defense, public safety, aerospace, and other vital missions."[10] As technology evolves, the spectrum strategy must focus on being agile, collaborative, inclusive, and well-researched and tested. The DoD Spectrum Policy Office under the DoD Chief Information Office (CIO) released a spectrum strategy in 2014; however, the strategy is exclusive to DoD, and, like Redl, recognized the need for collaboration, greater efficiency, flexibility, and spectrum sharing at the national level.[11] More recently, the Secretary of Defense released a new Electromagnetic Spectrum Superiority Strategy in 2020 calling for DoD to lead the way in the development of dynamic spectrum sharing technologies and techniques. Furthermore, DoD awarded a five-year $2.5 billion Spectrum Forward contract designed to accelerate the development and eventual deployment of new technologies including dynamic spectrum sharing for 5G systems.

DoD Sharing of the Sub-6 Gigahertz (GHz) Spectrum (Sub-6)

The sub-6 was designated as the international standard for wireless spectrum usage at the International Telecommunications Union's World Radiocommunication

Commander David Bergesen, U.S. Navy, is currently serving as the Department Head for Navy Intelligence Policy, Requirements, and Wholeness at U.S. Fleet Forces Command. He was commissioned through ROTC at the University of Arizona in 1998. He earned a Bachelor of Arts in Spanish Language and Linguistics degree from the University of Arizona, and a Master of Science in Cyber Systems and Operations from the Naval Postgraduate School in 2014. Prior to his current assignment, Commander Bergesen served as the Ship's Intelligence Officer onboard the USS *John C. Stennis* (CVN-74).

Conference in 2015. However, in the US, sub-6 is primarily managed and utilized by DoD and federal government agencies, leaving limited options for industry development in that range. The DIB recommended that DoD establish a spectrum-sharing plan. US spectrum segmentation and utilization require a holistic approach with national collaboration. Presently, however, there is insufficient collaboration across the private sector and federal agencies to clearly understand the operational risks, costs, required policy changes, and timelines associated with such spectrum sharing. As stated by the Cellular Telecommunications and Internet Association (CTIA) representing the wireless communications industry in the US, "DoD must prepare itself for that future operating environment by focusing on co-existing, if not explicitly sharing, with civil 5G operations in those bands of spectrum."[12] Spectrum usage varies substantially by frequency bands, spread across a diverse set of organizations and functions, further highlighting the need for collaboration.

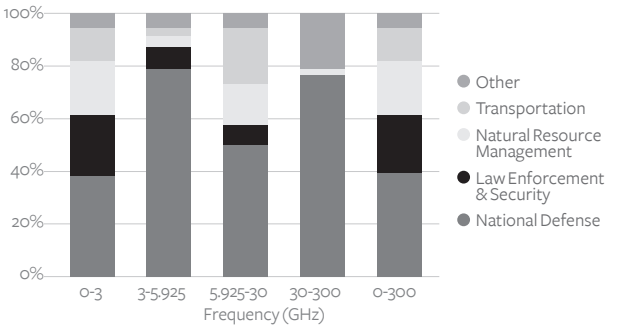

Figure. Federal Government Spectrum Usage[13]

Sub-6 vs. Millimeter Wave (mmWave)

Defense systems, public safety, aerospace and maritime agencies, and private industry operate across various segments of the electromagnetic spectrum; therefore, understanding the capabilities and limitations of the various spectrum bands is essential. 5G wireless systems are designed to operate within two distinct frequency regions: sub-6 and mmWave. The sub-6 band

operates at lower frequencies with corresponding longer wavelengths, while the mmWave operates at higher frequencies with significantly shorter wavelengths. Lower-frequency transmissions such as with sub-6 technologies do not attenuate as readily as higher-frequency ones used by mmWave technology and can achieve greater ranges. However, higher frequencies do offer increased transmission capacity (including more bandwidth available for security overhead), decreased latency, and considerably higher speeds. 5G wireless technology operating in the mmWave segment has been shown to transmit data up to 20 times faster than fourth generation (4G) wireless technology operating in the sub-6 band.[14] Quite significantly, though, the shorter wavelengths of signals in the mmWave bands are more susceptible not only to attenuation but to atmospheric (including moisture and airborne particulates) and physical obstructions (such as concrete, steel, or even trees). Practically, this means degraded signal penetration and possible signal interruption in congested urban environments. 5G systems operating in the sub-6 band would require fewer cell towers or base stations, making sub-6 implementation more cost-effective for telecommunications providers and, therefore, customers.

The international designation of sub-6 as the global standard has led international telecommunications manufacturers (including Chinese firms Huawei and ZTE) to develop hardware that operates primarily within the sub-6 range. As a result, many nations seeking to upgrade to 5G will opt for sub-6, as doing so will require fewer component upgrades while offering increased compatibility within existing 4G infrastructures. This, in turn, will enable more efficient transitions to 5G technology with a lower initial overhead, despite lower speed and bandwidth than mmWave technology.

While the physical characteristics of signals over a continuous range of frequencies change in a continuous manner, it is helpful to consider the advantages and disadvantages of signals within both the sub-6 and mmWave bands. The National Spectrum Strategy must develop an approach to benefit from each. To compete in the international development of 5G technology, the US must direct immediate attention to innovation in sub-6 and work on longer-term mmWave solutions for global markets. The near-term approach for sub-6 should include not only sharing and spectrum lease options but also auctioning of sub-6 spectrum where feasible. Due to the propagation issues with shorter wavelength signals, additional research and development time is required to make mmWave 5G globally viable. Lack of innovation in the sub-6 band would put the US behind 5G innovations by peer competitors that have deliberately focused on sub-6.

Spectrum Auctioning

In December 2018, the Federal Communications Commission (FCC) hosted the largest spectrum auction to date.[15] FCC efforts were focused on selling sub-6 to non-federal entities prioritizing 5G innovations. Although auctioning spectrum is not a new practice, the selling of the sub-6 spectrum was extremely limited in the past. While the FCC shifted to auction portions of the sub-6 spectrum, the time required to transition awarded bands fully is between five and

ten years. With the anticipation of China delivering 5G capabilities soon, the current transition timelines require an immediate upgrade. The Facilitate America's Superiority in 5G Technology (5G FAST) plan is the FCC's comprehensive strategy to make the 5G spectrum open to industry more rapidly, though it may not be fast enough.[16] Sub-6 is the immediate priority, but the 5G FAST plan is inclusive of all bands, recognizing the benefits of leveraging commercial innovation and hybrid solutions within the National Spectrum Strategy.[17] Reallocation of spectrum is both costly and time-consuming. A March 2012 NTIA study indicated that the cost to incumbent users in the federal government for reallocation of just one band of interest (1755-1850 MHz) was estimated to be $18 billion. This reallocation would also require ten years to relocate most of the systems and new federal access to two spectrum bands to accommodate relocated systems.[18] To remain competitive with China, sharing and lease options provide a more immediate solution.

Spectrum Sharing/Leasing

"Sustainable spectrum use is not a one-size-fits-all proposition but a blend of methods for a variety of needs," explained Dr. Matthew Clark, an engineering specialist at The Aerospace Corporation, "and the goal of spectrum sharing systems isn't simply to avoid interference by accounting for every possible sharing scenario but to provide practical services." Spectrum sharing enables multiple systems to use the same RF spectrum. DoD risks inherent to spectrum sharing are serious as they include the potential loss of operational security (OPSEC), loss of effective cybersecurity in reducing malicious activity, difficulty in safeguarding intellectual property, and the potential for RF interference.[20] Spectrum is the "maneuver space behind nearly all operations and spectrum innovation is an important part of how we (DoD) fight," former DoD Deputy CIO, Maj Gen Sandra Finan, stated.[21]

Although risk is inherent in 5G development, DoD also stands to benefit from industry innovations by gaining spectrum modeling and simulation tools, leveraging artificial intelligence, and allowing DoD traffic to "hide in plain sight."[22] DoD understands the need to collaborate and is currently participating in multiple collaboration and research efforts to support the sharing of spectrum, with a "trust but verify" approach.[23] The National Spectrum Consortium and the National Advanced Spectrum and Communications Test Network (NASCTN) is a multi-agency chartered partnership providing testing, modeling, and analysis to develop spectrum-sharing technologies and inform policy.[24] NASCTN was created in 2015 and comprises the National Institute of Standards and Technology (NIST), the NTIA, the DoD, the National Aeronautics and Space Administration (NASA), the National Science Foundation (NSF), and the National Oceanic and Atmospheric Administration (NOAA).[25]

The FCC and the NTIA both have responsibility and authority to allocate and license use of the spectrum; though each organization performs unique roles, they do coordinate spectrum issues. The Interdepartment Radio Advisory Committee (IRAC) – an entity within the NTIA – is responsible for coordinating and adjudicating spectrum issues on behalf of all government

agencies, including the DoD. The FCC, while not a voting member of the IRAC, is chartered to coordinate all non-federal spectrum-related actions with the IRAC (and vice versa). It is therefore important to recognize that DoD must coordinate all its spectrum needs through the IRAC. Additionally, the Department of State, in coordination with the FCC and NTIA, is responsible for US participation in the ITU-sponsored World Radio Conferences, where worldwide allocations are considered.

It is notable that the NTIA developed a Spectrum Sharing Innovation Test-Bed pilot program focused on the feasibility of spectrum sharing across federal and non-federal agencies. The test bed is comprised of academia, industry, and government agencies and targets sensing, geo-tagging, and location on mobile radio systems.[26] The focus of the test bed is to evaluate equipment characterizations and capabilities followed by a field operational evaluation.[27] This aligns with the "test but verify" concept to find ways to collaborate while mitigating risk.

As recommended by the DIB, DoD must plan for sharing the sub-6 spectrum and assessing bandwidths to be shared, while understanding the impact to DoD systems; however, DoD cannot do it alone. Executing a national spectrum strategy that protects both national and lower-level security concerns will take a collaborative effort. The 5G ecosystem is going to revolutionize global communications; DoD operations, networks, and command and control systems will also benefit from the innovation. It is essential that flexibility, agility, and security are implemented within the collaborative design phase.[28]

> Recommendation #2
>
> DoD must prepare to operate in a "post-Western" wireless ecosystem. This plan should include R&D investments toward system security and resilience on an engineering and strategic level.[29]

Recommendation #2 suggests that China will have a great advantage if it is the first to deliver 5G infrastructure and devices globally, gaining first-mover advantage. The DIB reports that "first-mover advantage is particularly pronounced in wireless generation transitions because the leader can set the foundational infrastructure and specifications for all future products."[30] Many countries will already be beholden to Chinese products when establishing 5G wireless technology networks due to component price and availability of components, as well as compatibility with proprietary interfaces of their current 4G infrastructures or network devices sourced from China.[31]

Chinese companies such as Huawei and ZTE Corporation present critical security risks as they are state-owned enterprises linked to the government. This has the potential to create a global information technology (IT) infrastructure susceptible to Chinese predatory practices, such as intellectual property theft and Chinese-mandated technology transfers creating many security vulnerabilities.[32] China's government has usurped physical and intellectual property, creating an advantage in the information space by exploiting data through creating back door

vulnerabilities within hardware and/or software. In 2019, many Chinese IT companies were implicated in nefarious cyber activities and directly linked to China's government.[33] This linkage can arguably be considered part of the culture as Chinese Law Articles 14 and 17 (National Intelligence Law, enacted June 27, 2017) indicate that Chinese companies have an active role in supplying information and/or access to the state.[34] This culture has provided state-sponsored leverage to make China a peer competitor and adversary of the US, at large, not just DoD.

Security

Security standards provide the basic parameters to create a secure environment across 5G wireless networks and are vital to maintain the confidentiality, integrity, and availability of US data as it traverses through information networks. To protect US data and systems, several improvements to current systems need to be pursued, including policy changes to ensure only secure equipment is used in USG systems, the development of quantum-resistant cryptography, improvement of software-defined networking technologies, and tighter controls over supply chain management. All these changes must be carefully orchestrated to work in concert with each other across all government agencies and industry partners.

Policy and implementation of cryptographic standards are required for global security. US policy protections restrict companies that are non-compliant with current IT security standards from providing equipment for the 5G infrastructure; however, the same standards do not apply to allied countries.[35] These cryptographic standards are being developed by NIST under the U.S. Department of Commerce for use by non-national security federal information systems. Though these systems are for non-national security systems, they could be reviewed or adjusted for applicability to national security systems or critical infrastructure, as well.[36] Smart design of the 5G infrastructure to use these new cryptographic standards would ensure that over the next decade, as the US experience with 5G wireless technology increases and its security is improved, the risk of information theft and unintended decryption remains low. A primary issue is finding a standard that will not impose excessive latency, thereby reducing the benefit of using the new 5G wireless technology. Regardless of the security approaches taken, the US should ensure persistent research and development efforts in security and resilience for the network while operating both in the US and internationally.

Resilience

Deliberate USG planning and action must be taken to ensure resilience when using 5G wireless systems. Two required actions to ensure a cyber-resilient methodology for US 5G wireless systems are: (1) develop better capabilities to observe anomalies or attacks in real time, and (2) improve the ability for cyber defenders to act at the speed of relevance.

USG systems must be able to determine that an attack, malicious event, or exploitation is in progress to take timely actions to ensure system resilience. To identify early warning of an anomaly or attack, US entities must understand their standard day-to-day environment,

sense that something is out of the ordinary, and determine what is happening across the digital domain.[37] Additionally, as DoD implements equipment that can leverage the 5G wireless infrastructure, military communications operators need to be trained and have the right tools to detect outside influence. Once an attack is identified, the more difficult task is attributing the activity to a malicious actor and then identifying the attack vector. To accomplish this, DoD should improve training programs for its cyber warriors and develop tools that can detect anomalies and potentially take the first steps in countering cyber-attacks. To help identify attack vectors and determine where an attack came from, new authorities or adjustment to current authorities may be required, especially if autonomous actions are incorporated into these systems.

Once a malicious act is identified, military operators must take timely action to stop the event. Finding or identifying the attack vector and stopping the inflow or outflow of data through system manipulation are key. To ensure resilience, military operators should be able to switch between 5G wireless and other secure wireless standards as seamlessly as possible.[38] Regardless of the standards, the key to resilience is having the ability to continue combat operations with or without an available network, albeit with reduced functionality. DoD should continue practicing and exercising scenarios either to maneuver or determine alternate means to remain combat-effective in contested, degraded, or denied electromagnetic spectrum environments. These competitive environments in which the cyber domain is contested are where victory in the next war will most likely be determined.

ANALYSIS OF DEFENSE SCIENCE BOARD RECOMMENDATIONS

Established in 1956, the DSB is a committee of civilian experts appointed to advise DoD on scientific and technical matters. The DSB completed a recent six-month Quick Task Force on "Defense Applications of 5G Network Technology."[39] The Task Force's stated objective was "to define a path for potential DoD 5G adoption that mitigates supply chain risk, establishes spectrum co-existence procedures and revamps existing communication infrastructure." The Task Force published its findings and recommendations in June 2019. The report offered the following ten recommendations:

1. Adopt 5G for military use in lightly contested environments.
2. Develop a secure 5G system for contested environments and critical applications.
3. Create test beds for exploring innovative use cases.
4. Stand up a telecommunications security program.
5. Develop a DoD 5G supply chain management strategy.
6. Create a program for "vulnerability analysis."
7. Develop and execute a three-year 5G+ Science and Technology Roadmap.

8. Develop a 5G+ Standards Engagement Plan.
9. Establish a new bi-directional spectrum-sharing paradigm.
10. Accelerate mmWave technology development and transition.

The DIB and DSB recommendations disagree on which portion of the spectrum to focus development (i.e., sub-6 or mmWave). The DIB report acknowledged that "the rest of the world is focused on building out sub-6 infrastructure, with China in the lead." Since DoD will have to operate overseas, it will "ultimately have to learn to operate on that sub-6 infrastructure, regardless of how the US chooses to implement 5G domestically." While the DSB recommendation acknowledges that DoD must be prepared to operate in a contested environment, recommendation #10 clearly focuses on accelerating mmWave technology "as the first priority" over sub-6 bands. Additionally, the DSB recommends that the Defense Advanced Research Projects Agency (DARPA) refine propagation models and investigate the feasibility of adapting 5G fixed mmWave technology to mobile, airborne, and satellite links. It also recommends that DARPA continue to track the development of 5G mmWave technology and create new opportunities for advancement. As stated previously, DoD in partnership with other USG agencies and industry must develop across the spectrum, while prioritizing efforts to sub-6. It also recommends building out mmWave technologies to provide both agility and flexibility of use throughout all environments. Finally, the DSB recommendations agree that a frequency sharing program must be implemented.

The difference in focus between the DIB and DSB recommendations for development of the sub-6 vs. mmWave bands highlights one of the fundamental considerations in 5G policy development, i.e., how much focus should be given to the sub-6 bands which have lower overall potential from a technical perspective. Given its early development by the international community, it has the potential to be ubiquitous soon, particularly among US allies and partners. Due to advantages and disadvantages previously discussed in this article, DoD must take a two-pronged approach ensuring relevance and interoperability in the near term by innovating in the sub-6 space as well as spectrum dominance in the future by innovating in the mmWave space. DoD should not focus solely on one band over the other but should take a balanced approach considering all advantages and disadvantages of these two bands within the spectrum. As of this writing, the US has made and is making allocations for 5G in distinct bands that fall into the sub mmWave bands as well as above, in fact some considerably higher. The 5G FAST Plan of the FCC details the specific bands.

ANALYSIS OF EUROPEAN COMMISSION RECOMMENDATIONS

The third set of recommendations examined were proposed by the EC in March 2019, offering a common EU approach to 5G. The recommendations were published in the article "European Commission recommends common EU approach to the security of 5G networks."[40] The recommendations leverage a December 2018 EU Cybersecurity Act that was agreed to by the European

Parliament, the European Council, and the European Commission. Unlike the DIB and DSB recommendations, the EC recommendations focus on the process of developing 5G standards, strategies, and security controls rather than considerations of the specific technologies. In synthesizing a way forward for DoD, consideration should be given both to the processes associated with developing 5G policies and to the technology's advantages and disadvantages.

The EC recommendations provide a concrete path forward for EU member countries and the EU writ large. Many of the recommendations of the Commission potentially may be applied to DoD. Adapting these recommendations to DoD focuses on developing a central coordination and information-sharing network that requires DoD components to develop component-level 5G risk assessments and update existing cybersecurity requirements and contracting mechanisms to consider 5G technology. Additionally, these recommendations would standardize mitigating 5G security controls including, but not limited to, certification requirements, tests, security controls, and the identification of products or suppliers that are considered potentially non-secure. These recommendations would also develop and mandate DoD 5G cybersecurity certification frameworks for all DoD 5G digital products, processes, and services.

SUMMARY OF DOD RECOMMENDATIONS

After reviewing and analyzing the recommendations made by the organizations discussed in this article, we offer the following eight recommendations, which include consideration for both process and technology as a way forward for DoD:

1. **Create a DoD 5G Coordination Group** – Establish a senior DoD-wide 5G coordination group with representation from across the Department to implement the recommendations listed below.
2. **Create a 5G Cybersecurity Information Sharing Network** – Develop a DoD-wide 5G cybersecurity information-sharing network.
3. **Develop a 5G Cybersecurity Threat Assessment** – Immediately complete a 5G cybersecurity threat landscape assessment that will support DoD agencies in completing their DoD component-specific risk assessments.
4. **Develop DoD Component-Level 5G Risk Assessments** – Using NIST Special Publication 800-37 (Guide for Applying the Risk Management Framework) as a guide, mandate that each DoD component conduct a component-level risk assessment of 5G network infrastructures in the near term including, but not limited to, identifying threats, vulnerabilities, and mitigating security controls.
    a. Include technical risks linked to the behavior of suppliers or operators, including those from China, Russia, North Korea, and Iran.
    b. DoD agencies would then submit threat assessments to the DoD-wide 5G coordination group to identify common threats.

5. **Update Existing Cybersecurity Requirements for 5G** – Mandate that each DoD component update existing cybersecurity requirements to include 5G network providers and include conditions for ensuring the security of DoD networks especially, when granting rights of use for RF in 5G bands. Updated cybersecurity requirements should include the following:
    a. Reinforced contract obligations on suppliers and operators to ensure the security of their 5G networks, and
    b. The right of DoD components to exclude companies from their 5G suppliers and operators for national security reasons if they do not comply with DoD 5G standards.
6. **Develop a Coordinated DoD 5G Risk Assessment** – DoD component-level 5G risk assessments will be a central element in building a coordinated DoD 5G risk assessment. The DoD-wide 5G coordination group should implement the following:
    a. Assess the effects of both DoD-wide and component-level recommendations to determine whether there is a need for further action,
    b. Develop standardized 5G security controls which should include, but are not limited to, certification requirements, tests, security controls, and the identification of products or suppliers that are considered potentially non-secure, and
    c. Develop and mandate DoD 5G cybersecurity certification frameworks for all 5G digital products, processes, and services.
7. **Develop DoD 5G Contract Requirements** – Develop specific DoD security requirements for contracts related to 5G networks, including mandatory requirements to implement 5G cybersecurity certification frameworks. Additionally, DoD should consider segmenting off, or deliberately routing around, networks or network segments that do not follow DoD 5G cybersecurity certification standards.
8. **Develop DoD 5G Policy** – Develop a DoD policy that requires operators take technical and organizational measures to manage appropriately the risks posed by security of 5G networks and services.

RECENT PROGRESS

Since the original writing of this article in the summer of 2019, significant progress has been made in advancing US 5G policy.

First, Congress passed the "Secure 5G and Beyond Act of 2020" on March 23, 2020. It requires development of a national strategy, to be known as the National Strategy to Secure 5G and Next Generation Wireless Communications, which shall ensure the security of 5G wireless communications systems and infrastructure within the US; assist mutual defense treaty allies, strategic partners, and other countries in maximizing the security of 5G systems and infrastructure;

and protect the competitiveness of US companies, privacy of US consumers, and integrity of standards-setting bodies.

Second, the President approved, and the White House published on March 23, 2020, a "National Strategy to Secure 5G of the United States of America." This document lays out four lines of effort:

1. Facilitating domestic 5G rollout.
2. Assessing the risks and identifying core security principles for 5G infrastructure.
3. Managing the risks to our economic and national security from the use of 5G infrastructure.
4. Promoting responsible global development and deployment of 5G infrastructure.

Third, the Federal Communications Commission established the 5G FAST Plan to implement the President's policy. This plan entails taking action to make additional spectrum available for 5G services, updating infrastructure policy and encouraging the private sector to invest in 5G networks, and modernizing outdated regulations to promote the wired backbone of 5G networks and digital opportunity for all Americans. The plan addresses each of the low, mid, and high bands as well as the potential bands for unlicensed allocation. It addresses the specific bands that the Commission has already allocated (and in some cases auctioned), or intends to allocate, for 5G services. The plan also addresses FCC policies for updating infrastructure policy, particularly for small cells. Finally, the plan addresses FCC intentions to modernize regulations pertaining to 5G backhaul and digital opportunities for Americans. This includes requirements for supply chain integrity and national security considerations. It emphasizes the importance of backhaul infrastructure as it is crucial for small cell connectivity to the rest of the network. Furthermore, the Commission recognized the import of integration of the radio access network (the basis for 5G) with the backhaul network, which couples with a switching network to form the basis of the overall communications network and architecture.

Fourth, a new initiative of industry and the FCC is worthy of note. The Commission has initiated an "Open Radio Access Network (RAN)" proceeding. An Open RAN, or Open Radio Access Network (O-RAN), is a concept based on interoperability and standardization of RAN elements including a unified interconnection standard for hardware and open-source software elements from different vendors. An O-RAN architecture integrates a modular base station software stack implemented on off-the-shelf hardware which allows baseband and radio unit components from discrete suppliers to operate together seamlessly. The O-RAN will most certainly contain important elements of the security stack as well.

Finally, the DoD has been advancing both doctrine and strategy to transition away from the traditional consideration of electromagnetic warfare (EW) as separable from spectrum management to a unified treatment of these activities as Electromagnetic Spectrum Operations (EMSO). Recent examples of this include the publication of the new Joint Publication 3-85

titled Joint Electromagnetic Spectrum Operations (JEMSO) in May 2020 and the October 2020 release of the new Electromagnetic Spectrum Superiority Strategy aligned with the 2018 National Defense Strategy. In addition to calling for DoD to lead the way in the development of dynamic spectrum sharing technologies and techniques, the Strategy addresses how DoD will "develop superior Electromagnetic Spectrum (EMS) capabilities; evolve to an agile, fully integrated EMS infrastructure; pursue total force EMS readiness; secure enduring partnerships for EMS advantage; and establish effective EMS governance to support strategic and operational objectives."

CONCLUSIONS

The innovation of 5G technologies will make a global impact on wireless communications, creating many opportunities and risks, with the advantage going to the first mover. Three diverse groups made assessments of the impact of 5G, focusing on recommendations to large organizations such as DoD and the EU. In this article, we reviewed and analyzed these recommendations to identify commonalities and differences that may be useful in synthesizing a way forward for DoD. We evaluated each of the recommendations in turn, then synthesized a possible way forward for DoD. Although we agree that DoD is critical to US national security, it cannot operate alone and a whole-of-nation approach is required. DoD, USG agencies, private industry, and US allies must collaborate to innovate at a speed exceeding that of their adversaries, especially China. Although positioning DoD to mitigate vulnerabilities in this new technology is critical, 5G technologies must be leveraged as an opportunity to improve national security by innovating across the entire spectrum with high security standards.

DISCLAIMER

The views expressed in this work are those of the authors and do not reflect the official policy or position of the United States Military Academy, the Department of the Army, or the Department of Defense.

NOTES

1. Jim Mattis, *National Defense Strategy*, May 1, 2018, accessessed July 15, 2019, https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf.
2. Defense Innovation Board, 2019, "The 5G Ecosystem: Risks and Opportunities for DoD," *defense.gov*. April 4, 2019, accessed July 19, 2019.
3. Ibid.
4. Wikipedia, *Defense Innovation Advisory Board*, accessed August 6, 2019, https://en.wikipedia.org/wiki/Defense_Innovation_Advisory_Board.
5. Defense Innovation Board, "The 5G Ecosystem: Risks and Opportunities for DoD."
6. Scott C. Brown, 2019, *Trump and FCC Outline Aggressive 5G Plan, will not Nationalize Networks*, April 12, 2019, accessed July 15, 2019, https://www.androidauthority.com/trump-fcc-5g-plan-975903/.
7. Paul Kirby, *DoD "All In" on Spectrum Sharing, Deputy CIO Tells Industry Group*, November 2, 2016, accessed July 19, 2019. https://blog.npstc.org/2016/11/04/dod-all-in-on-spectrum-sharing-deputy-cio-tells-industry-group/.
8. Tom Leithhauser, "Agencies, Private Sector Endorse Creation of a National Spectrum Strategy" *Telecommunications Report 84* (13): 2018, 25-28.
9. Paul Kirby, *DoD "All In" on Spectrum Sharing, Deputy CIO Tells Industry Group*.
10. Ibid.
11. Ibid.
12. Monica Alleven, "CTIA: DoD Report Fails to Reflect U.S. Standing in Race to 5G," May 3, 2003, accessed July 18, 2019, https://www.fiercewireless.com/wireless/ctia-dod-report-fails-to-reflect-u-s-standing-race-to-5g.
13. National Telecommunications and Information Administration, *How the Spectrum is Used*, https://www.ntia.doc.gov/book-page/how-spectrum-used.
14. Defense Innovation Board, "The 5G Ecosystem: Risks and Opportunities for DoD."
15. Scott C. Brown, *Trump and FCC Outline Aggressive 5G Plan, will not Nationalize Networks.*
16. European Commission, *European Commission recommends common EU approach to the security of 5G networks.* March 26, 2019, accessed August 6, 2019, https://europa.eu/rapid/press-release_IP-19-1832_en.htm.
17. Ibid.
18. Matthew A. Clark, "Aerospace Corporation," *aerospace.org,* November 2018, accessed July 19, 2019, https://aerospace.org/sites/default/files/2018-12/Clark_SpectrumSharing_12042018.pdf.
19. Ibid.
20. Ibid.
21. Paul Kirby, *"All In" on Spectrum Sharing, Deputy CIO Tells Industry Group*.
22. Defense Innovation Board, "The 5G Ecosystem: Risks and Opportunities for DoD."
23. Paul Kirby, *DoD "All In" on Spectrum Sharing, Deputy CIO Tells Industry Group*.
24. National Institute of Standards and Technology,*National Advanced Spectrum and Communications Test Network (NASCTN)*, accessed July 20, 2019, https://www.nist.gov/communications-technology-laboratory/nasctn.
25. Ibid.
26. National Telecommunications and Information Administration, U.S. Department of Commerce, *Specturm Sharing Innovation Test Bed*, accessed July 15, 2019, https://www.ntia.doc.gov/category/spectrum-sharing-innovation-test-bed.
27. Ibid.
28. Defense Innovation Board, "The 5G Ecosystem: Risks and Opportunities for DoD."
29. Ibid.
30. Ibid.
31. Ibid.
32. Mike Rogers, *The 5G Promise an the Huawei Threat; Big Brother is coming to your home via cheap Chinese goods*, January 29, 2019, accessed July 26, 2019. http://search.proquest.com.nduezproxy.idm.oclc.org/docview/2171790881?accountid=12686.

NOTES

33. 115th Congress, "Public Law 115-232 (John S. McCain National Defense Authorization Act For FY 2019), " NDAA 2019, Washington, DC; 116th Congress, "National Defense Authorization Act FY 2020." NDAA FY 2020, Washington, DC, Mike Rogers, *The 5G Promise an the Huawei Threat; Big Brother is coming to your home via cheap Chinese goods*, anuary 29, 2019, accessed July 26, 2019,http://search.proquest.com.nduezproxy.idm.oclc.org/docview/2171790881?accountid=12686; Jerry Hildenbrand, *How does a phone maker 'mistakenly' collect user data and ship it off to a server in China?* March 23, 2019, accessed July 25, 2019, https://www.androidcentral.com/how-does-company-nokia-or-oneplus-mistakenly-collect-user-data-and-ship-it-server-china.
34. Defense Innovation Board, "The 5G Ecosystem: Risks and Opportunities for DoD."
35. 115th Congress, "Public Law 115-232."
36. Lily Chen, Stephen Jordan, Yi-Kai, Moody, Dustin Liu, Rene Peralta, Ray Perlner, and Daniel Smith-Tone, 2016, *Report on Post-Quantum Crpytography*, NISTIR 8105, Washington, DC: National Institute of Standards and Technology (Department of Commerce). Gorjan Alagic, Jacob Alperin-Sheriff, Daniel Apon, David Cooper, Quynh Dang, Yi-Kai Liu, Carl Miller, et al. 2019, *Status Report on the FIrst Round of the NIST Post-Quantum Cryptography Standardization Process*, NISTIR 8240, Washington, DC: National Institute of Standards and Technology (Department of Commerce).
37. William Bryant, "Resiliency in Future Cyber Combat," *Strategic Studies Quarterly* (Winter 2015), 87-107.
38. Department of Homeland Security – Cybersecurity and Infrastructure Security Agency, *Overview of Risks Introduced by 5G Adoption in the United States*, July 31, 2019, accessed July 31, 2019, https://www.dhs.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.
39. Craig Fields and Alfred Grasso, 2019, *Defense Applications of 5G Network Technology*. Report, Defense Science Board, Washington, DC: Defense Science Board Quick Task Force.
40. European Commission, “European Commission recommends common EU approach to the security of 5G networks.”