Approved by Secretary of Defense
2 MAY 2020

Department of Defense (DoD) 5G Strategy (U)

Introduction

Fifth-generation wireless communications technologies (5G) currently in development promise orders of magnitude improvements in multiple areas, including speed, connectivity, and reduced latency. The deployment of 5G capabilities will also be far more disruptive than those of prior generations, with transformative effects that extend beyond telecommunications. 5G networks will enable vastly more smart devices to connect to the internet, thereby accelerating the digital transformation that is already underway in manufacturing, transportation, healthcare, and government. Consumer devices from vehicles to medical implants will become more capable via 5G connections to new edge computing and cloud services, algorithms, and applications. In summary, 5G deployment will enable a new generation of the knowledge economy; increasing productivity, growing new businesses, and spurring innovation.

Ubiquitous high-speed connectivity will also transform the way militaries operate. Tomorrow's warfighters will use local and expeditionary 5G networks to move massive amounts of data to connect distant sensors and weapons into a dense, resilient battlefield network. This data-rich environment will fuel powerful algorithms that will allow commanders to better understand, shape, and adapt to complex and contested physical and information environments. Low-latency communications will enable new generations of unmanned and autonomous weapons systems across all domains. The warfighter will be empowered with far richer access to data at the tactical edge, so that even small units can achieve strategic effects. The U.S. military must learn to utilize the connectivity provided by 5G to operate with the speed, precision, and efficiency necessary to remain effective and survivable in the future.

5G is a critical strategic technology: those nations that master advanced communications technologies and ubiquitous connectivity will have a long-term economic and military advantage. This strategy provides the DoD approach to implementing the *National Strategy to Secure 5G* and aligns with the National Defense Authorization Act for Fiscal Year 2020 (FY2020), Section 254. The overall strategy is also consistent with National Defense Strategy guidance to lead in key areas of great power competition and lethality to ensure 5G's "impact on the battle network of the future."

Challenge

The ongoing migration to 5G technologies creates multifaceted opportunities and risks. The central challenge for DoD is to accelerate the development and deployment of 5G-enabled capabilities, while ensuring those systems — as well as those of our allies and partners — are robust, protected, resilient, and reliable.

Accelerating the transition to 5G is challenged by key standards, security principles, and spectrum policies that are still in development. Historically, DoD has not engaged with the governance bodies that set mobile wireless industry standards. The international allocation of spectrum for 5G use and the best policies for sharing spectrum among multiple users also continues to be debated. Numerous reviews regarding 5G exports, foreign investment, and technology control measures are still underway. Related factors impacting the cost and speed of 5G deployment include industrial policy, fair market access, and government incentives.

Ensuring that DoD can operate in a global 5G environment is challenging because potential U.S. adversaries seek to dominate the 5G market in key partner nations, which could allow such competitors to gain unauthorized network and data access via exploited components in the supply chain, malicious software, and/or insider threats. Given the complexity of 5G infrastructure, even inadvertent vulnerabilities may be very difficult to detect and prevent. Finally, adversaries could leverage control of the 5G market to advance security and foreign policy goals that ultimately undermine U.S. interests.

Because 5G networks will transport massive amounts of sensitive personal, corporate, and government information, they are particularly attractive targets for potential U.S. adversaries. With persistent access to an ally's 5G network, an adversary could potentially engage in widespread espionage, threaten the privacy and rights of citizens globally, prepare the operational environment to provide an advantage in armed conflict, conduct information operations, and/or disrupt critical infrastructure. For these reasons, 5G networks must incorporate suitable protections. The U.S. Government also encourages allies and partners to prioritize security considerations by avoiding untrusted and unreliable suppliers for their 5G networks, even as DoD seeks to be prepared to operate in all network environments.

Only a robust, in-depth approach to 5G security can address the full range of hardware, software, and human-factor risks, while posturing the DoD to fully leverage 5G-enabled capabilities.

5G Objectives

DoD requires access to resilient, and protected 5G capabilities and spectrum. Therefore, the DoD will support national efforts to:

1. (U) Advance U.S. and partner 5G capabilities,
2. (U) Promote awareness of 5G risks to national security,
3. (U) Develop approaches to protect 5G infrastructure and technologies.

(U) Given the breadth of these challenges, the DoD must collaborate closely with other U.S. Departments and Agencies, industry, academia, Congress, allies, and partners to ensure success.

1. Advance U.S. and partner 5G capabilities:

The United States and its global partners are able to provide the most advanced and highest quality 5G products in the world. DoD must develop and employ new concepts of operation that use the ubiquitous connectivity that 5G capabilities offer to increase the effectiveness, resilience, speed, and lethality of our Forces. DoD will leverage the vitality of the U.S. information technology and microelectronics industries to accelerate the design, development, production, acquisition and fielding of these capabilities - capabilities that offer significant performance enhancements in speed, connectivity, and latency over older generation capabilities and systems. DoD can spur development by prioritizing 5G investment, fostering industry experimentation and integration on DoD sites, promoting dynamic and bidirectional sharing of spectrum, and investing in both sub-6 GHz and millimeter-wave advanced technologies.

2. Promote awareness of 5G risks to national security:

DoD, along with other U.S. Departments and Agencies, must ensure that allies and partners are aware of national security risks that derive from reliance upon vendors that lack good security practices and/or are vulnerable to influence by state or non-state actors. The decisions that allies and partners make regarding 5G investments and deployment should not only consider capital costs, but also long-term impacts to their national security, information sharing, critical infrastructure, and economic competitiveness. DoD must similarly combat coercive tactics by our strategic competitors, while providing partners with clear, accurate information that helps them assess 5G risks and opportunities.

3. Develop approaches to protect 5G infrastructure and technologies:

In accordance with the *National Strategy to Secure 5G*, DoD must assess 5G vulnerabilities and develop security principles for equipment, architectures, and operations. To address strategic risks such as coercive leverage or state direction to vendors, DoD must adopt measures to minimize risks to the supply chain for critical components. These measures include avoidance of untrusted and unreliable sources as well as recognition that no network is ever completely secure. In-depth protection also requires adoption of compliance standards for 5G design, cybersecurity for 5G infrastructure, and implementation of a “zero-trust” security model. These measures will collectively ensure that DoD can operate within untrusted networks effectively. DoD will also leverage the extensive technical expertise resident within the United States to provide robust national and international standards for 5G design.

This strategy will result in key outcomes that include:

- 5G-enhanced DoD mission capabilities,
- Protected and resilient DoD capabilities that leverage ubiquitous connectivity,
- Assured global spectrum access even within congested and contested environments,
- Robust, resilient microelectronic components and supply chains, and

- Closer collaboration with international partners on 5G development and protection.

5G Lines of Effort

The following are necessary lines of effort to achieve the key outcomes:

1. Promote technology development,
2. Assess, mitigate, and operate through 5G vulnerabilities,
3. Influence 5G standards and policies,
4. Engage partners.

1. Promote Technology Development:

DoD will facilitate the advancement and adoption of 5G technology and identify new uses for 5G systems, subsystems, and components by promoting science, technology, research, development, testing and evaluation efforts via unique access to testing sites, spectrum licenses, technical expertise, and resources. DoD will also work with industry and academia to support the development of critical technologies, integrate those technologies within a protected architecture, and demonstrate "transformative 5G and beyond" applications.

- Hosting 5G Demonstrations

  DoD will select military facilities that will serve as hosts for a series of 5G industry demonstrations beginning in FY 2020. These demonstrations will develop and test military and dual-use 5G technologies, concepts, and applications. Selected testbeds will benefit industry partners by providing large, complex environments that are suitable for testing the integration of 5G features (e.g., smart ports, supply chain management, and depot operations). Successfully demonstrated and proven products will be rapidly deployed, with follow-on acquisitions, operations, and sustainment through the appropriate organizations across DoD.

- Millimeter Wave Technology

  DoD recognizes that truly transformational uses for "5G and beyond" capabilities will require operations across all 5G spectrum bands, including the contiguous spectrum available at high frequencies above 24 GHz in the millimeter-wave bands. The U.S. microelectronics industry excels in millimeter-wave technology, and DoD can leverage this expertise for the development, acquisition, and fielding of millimeter-wave equipment. DoD will also support policies that foster shared co-primary Federal access, and will promote national and international standards related to millimeter-wave technologies.

- Dynamic Spectrum Sharing

  Ubiquitous 5G coverage will require access to a variety of radio frequencies (RF) including those falling within the mid-band (1 GHz to 6 GHz) range. Because this spectrum is both heavily utilized by DoD and is highly sought after by the 5G industry, technologies and frameworks will be needed to share this spectrum amongst disparate users. DoD will support research, development, testing, acquisition, and fielding of systems incorporating new technologies that permit greater spectrum access while preventing harmful interference to legacy systems. DoD will develop the technologies and capabilities needed for near-real-time sharing, in order to enable military operations in congested spectrum environments.

- Open Architecture and Virtualization

  DoD will contribute to the development of advanced 5G network architectures. The DoD experimentation program will also inform more-secure designs for 5G core and edge systems, including Open Radio Access Networks and network slicing. The resulting open architectures, as well as virtualized networks and services, will make it easier for companies to offer 5G services, thereby spurring innovation, competition, and acquisition options. The approach will also enhance security, by providing a broader community of stakeholders that are dedicated to ensuring the overall integrity of the resulting architectures.

- Workforce Development

  The growth of the U.S. 5G industry requires a broad, well-trained workforce. DoD, in collaboration with academia, industry, and interagency partners, will identify the necessary skills and develop a human capital plan that leverages DoD's STEM programs and long history with university and laboratory partnerships. This approach will also extend to the next generation of talent that will be needed to develop advanced technologies for 6G and beyond.

2. Assess, Mitigate, and Operate Through 5G Vulnerabilities:

Given the military's need to operate within hostile and contested environments, DoD will utilize a risk-based framework to ensure the confidentiality, integrity, and availability of our 5G networks, devices, weapon systems, and applications and encourage its partners and allies to do likewise. DoD will also conduct country-specific assessments to determine how non-secure devices in ally and partner networks may affect DoD operations.

- Threat Intelligence

  DoD must have a clear and comprehensive understanding of 5G threats and vulnerabilities. DoD also has concerns regarding potential adversaries' capabilities and

their intent to leverage 5G technologies against U.S. interests. In addition to monitoring foreign technical developments, DoD must also understand how adversary military and intelligence forces may leverage 5G-enabled capabilities to impact operations. These evaluations must leverage U.S. allies and partner collaborations to the maximum extent possible.

- Minimizing 5G Infrastructure Risks

  Risks to 5G infrastructure supply chains can be reduced and more easily managed by working with allies and partners, to ensure that suppliers adhere to stringent monitoring, inspection, physical security, operational security, and personnel-vetting standards and best practices. In accordance with Executive Order 13873, *Securing the Information and Communications Technology and Services Supply Chain* (May 15, 2019), DoD will not acquire, import, transfer, install, deal-in, or use 5G technologies that are produced by foreign adversaries. Moreover, DoD, in close coordination with allies and partners and industry, must develop and execute a detailed plan for supply chain risk management for this sector. The final result must support the ability of DoD to operate around the world, even within regions with networks that have been compromised.

- Global Operations

  DoD operates globally and will require the ability to securely use private, hybrid, and public 5G networks. DoD will work with industry, academia, standards setting bodies, and government research labs to develop and deploy techniques and technologies across DoD devices and infrastructure that ensure protected and resilient utilization of 5G networks globally, even in denied, degraded, intermittent, and limited environments.

- Security Assessments

  DoD will conduct security assessments to discover, assess, and mitigate 5G vulnerabilities. These actions include identifying vulnerabilities during development, deployment, and sustainment of 5G-enabled networks, platforms, and systems.

- Cybersecurity and Zero-Trust

  The scale, complexity, and decentralized design of 5G architectures make it infeasible to depend upon perimeter security, which assumes that only trusted devices have been allowed inside the network. DoD will instead develop and validate a zero-trust model for 5G. The zero-trust approach will allow DoD to manage risk, while operating within untrusted network environments by utilizing encryption and fine-grained management of authorities and information access.

3. Influence 5G Standards and Policies:

5G represents a global technology; it is being developed, deployed, and regulated by numerous private and governmental organizations. The national and international standards to which 5G systems are designed will necessarily impact which companies and countries are best-positioned to provide those capabilities.

- Standards Setting Bodies

  To promote high-quality, protected, and reliable 5G devices and applications, the U.S. must play a lead role in shaping information and communications technology standards. DoD will fully implement its Standards Engagement Plan and will actively participate in the 3rd Generation Partnership Project (3GPP) organization. It is vital that DoD and its interagency partners, including the Federal Communication Commission (FCC), National Institute of Standards and Technology (NIST), and National Telecommunications and Information Administration (NTIA), have specific and prioritized outcomes for this engagement, including strengthening U.S. influence in key standards setting organizations and promoting high-quality American 5G and beyond technologies.

- Advanced Spectrum Management

  Traditional approaches to spectrum management – allotting slices of frequencies for single-purpose use – do not support the growing demand for spectrum for both civil and military innovation. As the 2018 *Presidential Memorandum on Developing a Sustainable Spectrum Strategy for America's Future* suggests, spectrum regulations and policies must keep pace with technological advances, growing spectrum demands, and operational realities. As the biggest user of Federal spectrum, DoD must continue to work closely with NTIA and the FCC to develop new policies for sharing spectrum, including dynamic spectrum sharing and bidirectional sharing of existing bands. 5G sharing decisions must be informed by technical feasibility and engineering analyses that ensure current and future DoD mission requirements can be satisfied. DoD seeks to demonstrate that this approach will provide both DoD and 5G network operators with greater spectrum access, capacity, and protection from interference. This approach will also pave the way for broader national adoption of spectrum sharing, which will help to spur 5G deployment, provide DoD with access to mission critical spectrum when needed, and improve resilience against coercive, illicit, and exploitative actions in the spectrum.

- 5G-Enabled Concepts of Operations

  The deployment of 5G capabilities will offer a host of opportunities to both reform DoD enterprise services and to create powerful new military advantages. DoD will develop new concepts of operation to ensure its forces will be the first to harness the transformational speed and connectivity of 5G. DoD will explore and develop 5G-enabled capabilities across the full range of its missions and will ensure that it can achieve its mission

objectives in contested and congested spectrum environments. The Military Departments will strengthen military effectiveness by integrating advanced information networks into the way U.S. forces are organized, trained, and equipped.

- Technology Control Measures

DoD must also support whole-of-government efforts to protect 5G-enabling technologies from potential U.S. adversaries. This includes reviewing foreign investments in U.S. companies, updating and reviewing export controls, and other measures – while not compromising DoD's ability to acquire next-generation technologies. The Department must balance protecting sensitive information against the need for U.S. companies to collaborate and access international markets. These measures must be reviewed and updated regularly to match the rapid pace of technology evolution.

4. Engage Partners:

DoD must engage with interagency, international, and industry partners proactively to shape 5G outcomes. This requires positive, prioritized, and coordinated dialogue in support of our shared interests with each of these communities.

- International Allies and Partners

DoD must collaborate closely with the State Department to utilize upcoming bilateral and multilateral dialogues to discuss 5G concerns with international partners. DoD must convey to allies and partners the risks to their national security equities — mobilization, interoperability, information sharing, operations, and resilience against coercion — to quickly address them before mitigations become far costlier. The matter is urgent, as many nations are already auctioning 5G spectrum and making long-term investments in 5G infrastructure. It is important that the United States promotes a shared understanding of the importance of 5G protection and the serious threat posed by unauthorized foreign access. *The Prague Proposals* on 5G security and the *National Strategy to Secure 5G* provide a helpful basis for framing this issue, specifically noting that "the overall risk of influence on a supplier by a third country should be taken into account".

The decisions made by our allies and partners about 5G deployment often involve senior government and industry leaders who may not view telecommunications infrastructure as a national security issue. DoD must ensure that foreign counterparts understand the risk 5G threats and vulnerabilities pose to interoperability and industrial security so they can accurately communicate the message across their governments. This requires DoD to provide a clear national security-based rationale concerning the risk of 5G vendors beholden to foreign governments.

Some states continue to seek to undermine fair and open international competition for 5G equipment and services via diplomatic pressure, misleading reporting, market

manipulations, state-backed financing, and/or other aggressive interventions. The United States is confronting such tactics directly and ensuring that our allies and partners are aware of ties between foreign suppliers and their governments' security organizations. DoD will support these national-level efforts by collaborating with the global community to identify 5G security vulnerabilities and share relevant threat intelligence with DoD counterparts.

In order to influence significant upcoming decisions, DoD must develop clear, prioritized outcomes for international engagement and ensure DoD military, political, and industry outreach is aligned in support of those outcomes. This will include positive messaging about opportunities to collaborate with the United States on 5G research, standards, and deployment.

- Industry Engagement

  DoD will continue to engage in open and transparent dialogue with our global industry partners, including 5G microelectronics manufacturers, telecommunications companies, and application developers. A healthy and robust National Security Innovation Base is vital to providing the United States with access to low-risk sources of components for the defense supply chain. DoD engagement with industry will continue to inform the U.S. approach to 5G standards, research priorities, and international collaboration. Only industry is able to deliver the 5G capabilities needed by DoD.

- Congressional Engagement

  Many aspects of national 5G development and deployment are shaped by legislation. U.S. companies require adequate access to capital to deploy 5G infrastructure, along with fair, competitive access to global markets. DoD will work with interagency partners to identify and recommend specific legislative proposals to strengthen 5G standards and security, incentivize deployment, and offset distortions to the open market.

Conclusion

5G technologies are strategic capabilities that will impact the U.S. economic and national security and those of our allies and partners. If DoD acts with urgency, it can utilize its unique partnerships, expertise, and resources to accelerate 5G innovation and deployment, including leading edge millimeter-wave and spectrum sharing technologies in support of DoD’s enduring missions. This will help ensure that the U.S. military, the American public, and our allies and partners have access to the best 5G systems, services, and applications in the world.