ARTICLE

Commercial SATCOM

A Risk Mitigation Strategy

Jonathan K. Corrado

The US military's dependency on commercial satellite communications technology makes the force vulnerable when systems cannot meet the required operational characteristics for military use of satellite communications. The article presents Department of Defense satellite communication requirements and addresses areas of concern relating to military use of commercial satellite communications systems. Specifically, it analyzes concerns related to protection, control, reliability, interoperability, and access; recognizes the need for commercial satellite communications capacity; and gives a risk analysis with possible solutions to mitigate any potential vulnerabilities due to military use of commercial SATCOMs.

Unpredictability has characterized recent global events. From dynamic, geographically dispersed threats to nontrivial natural disasters, a wide spectrum of incidents occurs rapidly and, in most cases, abruptly, anywhere around Earth. Today's incident-guided reality stimulates a persistent necessity that military and US government users must be poised to deploy anytime, anywhere. To maintain this ready posture, the Department of Defense must have access to hardy, cost-effective, highly agile, and secure satellite communications (SATCOM) in short notice across the full spectrum of engagement.

The US military uses commercial and military SATCOM systems to meet its global communications needs. When a heavy allocation of military satellites is required, DOD leases available commercial SATCOM assets to meet unfilled requests and user needs. The Department also continues to provide beyond-line-of-sight communication capability to the military with commercial-band-only equipment.

Until recently, military satellite capabilities outperformed commercial satellite capabilities.[1] But in the current aggressive and globalized market, commercial satellite capabilities have matured and can now meet many DOD satellite service requirements. The commercial satellite market is rapidly growing to meet increased global demands for services, including fulfilling 40 percent of the Department's SATCOM needs.[2]

According to Northern Sky Research, a telecom industry research firm, The US military's SATCOM requirements will grow by 68 percent in the next decade.[3] This demand surge is due to the reallocation of US forces toward the Asia-Pacific theater, increased naval

[1] SES Government Solutions, "MILSATCOM and COMSATCOM—Why They're Better Together," The Government Satellite Report (blog), August 30, 2019, https://ses-gs.com/.

[2] Defense Business Board (DBB), *Report to the Secretary of Defense: Taking Advantage of Opportunities for Commercial Satellite Communications Services*, Report FY13-02 (Washington, DC: DBB, 2013), 1, https://dbb.defense.gov/.

[3] DBB, *Taking Advantage*, 5.

patrols of critical sea lanes, amplified monitoring of world events, and growing involvement in the war on drugs.[4]

The current DOD SATCOM strategy includes an increased reliance on commercial systems and technology to support the needs of the military and national security agencies. But an assessment of the risks and potential vulnerabilities stemming from this practice indicates the Department's reliance on commercial SATCOM may present unacceptable levels of risk. This analysis will argue the US military's surging dependence on commercial SATCOM will become a vulnerability deriving from the availability, security, and command and control (C2) of commercial SATCOM systems.

This article will outline DOD requirements for commercial SATCOM contracts before addressing potential protection, control, legal, and issues with military use of commercial SATCOM. It will address access, interoperability, and the reliability of commercial SATCOM in a military context and analyze the drivers for US military use of commercial SATCOM, recognizing that military SATCOM systems do not provide the necessary capacity to complete all DOD missions effectively. The article will conclude with a risk assessment and possible mitigations.

Communication Requirements and Commercial SATCOM

The US military's decision to rely increasingly on commercial contractors to supply and support its SATCOM requirements begins with an assessment of two key issues. First, the DOD's unique requirements for the satellite systems that it contracts and purchases could make identifying a suitable commercial provider challenging. At the same time, the commercial SATCOM sector's growth and development continues to attract government and defense contracts as the field provides options that support the varied demands for technological quality, communication features, and cost-range diversity.[5] Based on this range of features, military planners often view commercial SATCOM options as viable solutions that address military and national security communication requirements.

The Department's specific SATCOM requirements can be divided into three key categories. First, DOD mandates a set of broader-level planning and security-related compliance requirements that it publishes and delivers to private companies that compete for government contracting bids. These policies address the need for satellite systems that adhere to strict design, encryption, and cybersecurity standards.[6] Second, DOD specifications for SATCOM technical and operational features include the mandates that ensure a satellite system's functionality, interoperability within a given network, standardized architecture, and information-sharing capabilities.

[4] DBB, *Taking Advantage*, 5.

[5] US General Services Administration, Complex Commercial SATCOM Solutions (CS3), n.d., accessed February 1, 2022, https://www.gsa.gov/.

[6] Department of Defense (DOD), *DoD Satellite Communications*, DoD Instruction 8420.02 (Washington, DC: DOD, November 25, 2020), 3, https://www.esd.whs.mil/.

Finally, contracted systems need to adhere to the agency's specific policies for SATCOM operations. According to a report provided by the Joint Chiefs of Staff, this broader category includes two specific requirements. (1) These completed systems require the capacity for being effectively managed through a set of operational and accessible ground controls. (2) The systems should also feature a set of resilient communications infrastructure that can respond to and overcome potential technological challenges or enemy control or disruption attempts.[7] A related requirement in this same context includes a need to efficiently deliver information to selected users to secure the transmission and ensure the timeliness of the messaging.

The Department often seeks to meet these demands by relying on SATCOM systems provided through private commercial contractors. Military reliance on commercial satellite technologies derives from two key motivations. First, the complex and diversified nature of the commercial SATCOM sector enables contracting military agencies to develop highly selective requirements and accept bids from a range of potential providers. Market research related to the field indicates this sector comprises a complex set of competitors, including major firms such as Lockheed Martin and smaller-scale firms that focus on specialized service areas.[8]

By selecting from this group, DOD-affiliated agencies can ensure they can contract with suppliers who will comply with their stated requirements and specifications. Last, this approach also derives from the belief that by contracting with commercial SATCOM providers, defense and security agencies can avoid the risks and costs associated with developing government-specific SATCOM systems.[9]

While the requirements process is well documented and thorough, the reality is that not all commercial systems will meet every DOD requirement—cost-driven business models in the commercial sector are not always aligned with priorities in the security sector. When faced with an option to procure commercially provided bandwidth that may not meet all DOD requirements or be left without the desired capacity of satellite access, the Department must make choices that could result in vulnerabilities to either mission or information.

Protection, Control, and Legal Issues

Department of Defense-related policies for SATCOM communication also entail considerations related to the variables of protection, C2, and the legality of operating specific systems within a given network. While the Defense Department and nonmilitary intelli-

[7] Chairman of the Joint Chiefs of Staff (CJCS), *Department of Defense Satellite Communications*, CJCS Instruction 6350.01F (Washington, DC: CJCS, February 26, 2019), 5, https://www.jcs.mil/.

[8] Research and Markets, *Global Communication & Military Satellite Communications (SatCom) Market Forecast to 2028* (Dublin: Research and Markets, December 2019), 4, https://www.researchandmarkets.com/.

[9] Rick Lober, "Why the Military Needs Commercial Satellite Technology," Defense One, September 25, 2013, https://www.defenseone.com/.

gence agency affiliates continue to rely on commercial-based SATCOM systems, these actions might potentially create vulnerabilities across these same domains. Based on these assessments, increased agency reliance on commercial SATCOM systems can be viewed as a questionable and counterproductive strategy.

The concept of protection in the context of satellite operations typically includes two primary points of consideration. Fundamentally, military planners address the need to protect their SATCOM systems from any potential physical disruption that can negatively impact performance. According to a report provided by the US Army, the branch's leadership and personnel rely on SATCOM to provide imaging beyond the line of sight that can contribute to planning at the operational, strategic, or tactical levels.[10]

Accordingly, the primary need to protect functional satellites at the physical level would include methodologies to ensure operational integrity. Still, given the unique nature of satellite systems, these risks often represent minimal-level threat variables. In contrast, the risk factors related to an enemy's ability to hack, control, and falsely command these systems coupled with the potential for antagonists within an operational environment to disrupt a SATCOM's potential for seamless communication would represent likely and potentially serious threats.[11]

Since commercial SATCOM companies often rely on more widely used technical designs, enemy forces might possess the knowledge and skillsets needed to hack into the commercial SATCOM systems utilized by US military forces and intelligence agencies.[12] These same trends would thus compound the risks derived from an applied system's physical dimensions and capacities.

The concepts for optimized command and control in the context of applied DOD SATCOM systems include the following variables. First, users and stakeholders must have continuous and uninterrupted access to these systems. System users scattered across vast geographic distances need to have access to the same type of information that they can then apply toward their specific and unique operational goals.[13]

Second, SATCOM systems should feature accessible and resilient terminals that can ensure an authenticated user's ability to manage and communicate with it from their position. A third mandate assumes military leaders and personnel will have access to resilient networks to provide the coverage needed to link a unit to a specific SATCOM system. Fourth, these requirements additionally ensure satellite transmissions can be se-

[10] US Army, *Army Field Experiments to Incorporate Commercial Satellite Constellations*, Combat Capabilities Development Command, Command, Control, Communications, Computers, Cyber, Intelligence, Surveillance, and Reconnaissance (CCDC C5ISR) Public Affairs, June 4, 2020, https://www.army.mil/.

[11] National Security Telecommunications Advisory Committee (NSTAC), *Report to the President on Commercial Satellite Communications* (Washington, DC: NSTAC, November 2009), ES-2, https://www.cisa.gov/.

[12] Tim Brauner, "Four RF Technology Trends You Need to Know for Satellite Communication Device Design," Aerospace & Defense Technology, October 1, 2020, https://www.aerodefensetech.com/.

[13] US Space Force (USSF), *Vision for Satellite Communications (SATCOM)* (Washington, DC: USSF, January 23, 2020), 3, https://www.spaceforce.mil/.

cured and safely delivered from and to operational environments that feature varying levels of risk and potential threats.

A final C2-related consideration posits that commanders should have instantaneous and uninterrupted access to requisite data as they develop and revise their plans within an operational setting. The military's continued reliance on commercial-based systems includes the tendency to provide limited forms of bandwidth that can restrict the scope and reliability of SATCOM intelligence.[14]

The primary legal issues deriving from defense- and military-sector reliance on commercial SATCOM technology are related to the jurisdictional channels that govern satellite communications. In brief, military planners seek to ensure their satellites operate within discrete networks that are both segmented from and protected against the data transmitted by competing systems.

This assurance cannot be provided when leasing commercial satellite real estate. The complexity is compounded by the Department's tendency to rely on wide area and local area networks to control US military forces scattered across various geographical sites.[15] Continued reliance on commercial-based systems can create vulnerabilities related to the potential for civilian and enemy-controlled networks to interfere with dedicated US defense and military channels.

This broad look at the potential vulnerabilities associated with protection, command and control, and legal issues with the military use of commercial SATCOM clearly shows the need to accept some risk to mission in DOD contracting of commercial SATCOM systems. The next item of concern is the inability of commercial SATCOM systems to ensure the required capabilities of access, reliability, and interoperability when contracted for US military use.

Access, Interoperability, and Reliability

An additional set of issues related to the Department's SATCOM policies include system access, interoperability, and reliability. The term access refers to the ability of a network's authenticated users to retrieve, apply, and contribute to the network's stored data. Access in this context aligns with the concept as defined by the confidentiality, integrity, availability triad model for information security.[16] In DOD-related settings, access represents a significant concern for the personnel who operate within theaters that are geographically distant from the United States and who may also be distant from any alternative forms of communication or reliable and secure communications infrastructure.

[14] US Army, *Army Field Experiments*.

[15] Randall Bland, "Latency: The Other Enemy on the Battlefield," Government Satellite Report (blog), March 11, 2015, https://ses-gs.com/.

[16] Debbie Walkowski, "What Is the CIA Triad?," F5 Labs, July 9, 2019, https://www.f5.com/.

For users in these operational environments, a combination of weather, geography, and enemy actor threats could sever operational links between military units and the SATCOM systems that transmit requisite data to their positions. The US military's reliance on commercial constellations exacerbates these risks as many of these systems provide limited types of bandwidth.[17] Data processing latency, or the tendency for satellite systems to lag when delivering data to their users, also represents a risk that can limit access.[18]

Mitigation for access concerns is provided if coverage from a separate, equivalent system is also available to an operator, but this requires different systems to communicate. Interoperability, between various commercial providers and between military satellites and commercial satellites, has been a constant challenge for DOD SATCOM. The Air Force Research Laboratory has recently taken steps to address interoperability concerns between commercial and military satellites by contracting with ViaSat, a satellite communications company, to integrate commercial and government-owned systems into a seamless network.[19]

Looking at commercial SATCOM interoperability specifically, the Department developed a flexible modem interface (FMI) to enable communications between different commercial satellite systems, and it demonstrated the FMI device in 2019 onboard the International Space Station.[20] Having the FMI as a translator between different commercial services enables multiple providers to offer seamless services while protecting their proprietary technology.

With the commercial satellite sector continuing to grow with demand and the Department of Defense espousing a vision of networked commercial and military SATCOM, the interoperability of various commercial systems is the biggest hurdle to clear in enabling commercial SATCOM to meet DOD needs.

Satellite communications reliability can be defined as a system's ability to operate across diverse environments despite the challenges that might impact its operations. Reliability derives from access as it can be impacted by a combination of geographic, weather, enemy, and technological variables.

At one level, DOD reliance on commercial SATCOM might be viewed as a strategy that reduces the potential for the systems being interrupted as the systems are commercial products supported by commercial providers. But commercial SATCOM systems are often not built with defenses against intentional disruption by an enemy actor or hardened against potential wartime environment interference as features like these add additional unit cost,

[17] NSTAC, *Report to the President*.

[18] Bland, "Latency."

[19] Sandra Erwin, "Air Force Enlists ViaSat to Help Integrate Commercial and Military Satellite Networks," Space News, March 15, 2021, https://spacenews.com/.

[20] Irene Tzinis, ed., "Demonstrating a Space Communications Universal Translator with NASA," NASA (website), April 1, 2021, https://www.nasa.gov/.

weight, and complexity. These components are not needed for general day-to-day commercial use, which negatively affects its reliability for users on the operational front.

DOD Commercial SATCOM Reliance

Satellite communications are vital to war-fighter support and sustainability, and the military will need additional capacity and system capability as new dynamic missions evolve, operations grow in new geographical regions, new technologies generate new communications requirements, and the distributed C2 system envisioned in the *JCS Capstone Concept for Joint Operations: Joint Force 2030* moves toward reality.[21]

Despite the potential vulnerabilities and risks presented in this article, a well-documented need for increased capacity of SATCOM systems for US military use exists. Government-developed systems, from cradle to grave, are expensive and provide a level of protection that is not necessary for all military SATCOM applications. The ability for commercial systems to maintain a level of communication and command and control between US forces has been proven, and it is a near certainty that this contracting process will continue.

Several arguments have contributed to the US military's reliance on commercial SATCOM technology. Commercial systems provide a flexible, easy-to-procure, cost-effective option for SATCOM use. Contracting SATCOM services relieves the Department of the research and development burden (i.e., cost), with market competition fueling technological advancements in commercial systems. The military can control cost by relying on tendering processes to select commercial SATCOM providers best qualified to fulfill a contract, taking advantage of market competition.

Further, commercial system performance and security are quickly advancing with an increased focus on cybersecurity in the commercial sector, which better aligns with DOD requirements. Finally, contracting out SATCOM services hinges on the belief that commercial contractors represent the most capable agents of delivering quality SATCOM systems while also adhering to scheduling and budgeting requirements. In contrast, government-developed programs have historically faced a cumbersome acquisition and employment process that leads forces to be more reactive than proactive in securing necessary communications paths.[22] All of these factors combined make military use of commercial SATCOM appealing.

These arguments, however, often do not address the challenges and risks that can derive from the Department's overreliance on commercial platforms. Primarily, protecting information transmitted via SATCOM should be of utmost concern. If the US military can contract a commercial SATCOM service, that same service (or system specification) may be available to US adversaries, creating an inherent vulnerability. While not all mili-

[21] DBB, *Taking Advantage*, 1.

[22] Rebecca Cowen-Hirsch, "A Path to an Integrated DoD Satellite Architecture via Commercial SATCOM as a Service," Via Satellite, February 13, 2020, https://www.satellitetoday.com/.

tary data passed via SATCOM needs an increased level of protection (e.g., Armed Forces Network), any SATCOM system's capability for military use should be at the top of any requirements list.

Additionally, reliability and access-related risks are amplified by requiring US military forces to rely on a complex set of competing SATCOM systems. The complexities deriving from these conditions also create C2-related challenges as military commanders and personnel attempt to rely on systems that can be impacted by disruptions generated through interoperability-related concerns. The Department could address these challenges by reducing the number of commercial SATCOM systems contracted for military use. Focusing DOD contract spending on a small number of commercial variants with dedicated security sector platforms is one mitigation of this issue.

Risk Management

Given the potential risks that derive from the military's reliance on commercial SATCOM technologies to address its communication-related needs, the Department should address these risks in its current approach while further mitigating the risks with both policy and technology. An optimal approach would include the military's ability to generate the benefits from commercial SATCOM while protecting its users from the continued risks associated with an overdependency on commercial SATCOM.

In the near term, the Department of Defense could mitigate interoperability concerns and reduce overhead costs by reducing the number of commercial providers selected for tendering contracts. A recent decision by the US Army's executive leadership illustrated how this approach might represent a viable solution.[23] In a first-of-a-kind contract, the branch awarded a single-award blanket purchase to Peraton, a commercial SATCOM provider, to coordinate communications services for DOD operators in the US Africa Command operating region leveraging satellites and technologies across multiple commercial operators. The Army justified this approach by contending it would limit many of the risk factors related to systems access and interoperability.

While a singular network would reduce interoperability challenges, accessibility and reliability concerns remain. Having a dedicated commercial operations center to connect users to resources and address any challenges could ensure the users have relatively uninterrupted communications without tying up DOD satellite operations resources. As this is a new procurement model, potential challenges are unknown, but it appears to be a step in the right direction for reducing the number of commercial SATCOM contracts while continuing to provide access.

As a long-term option to more completely mitigate the risks for critical SATCOM, the Department and other intelligence and national security agencies should continue to field dedicated satellite systems to provide critical and protected communications to

[23] "Peraton Awarded $219M Contract to Provide Satellite Communications to AFRICOM," Peraton News & Insights, March 3, 2020, https://www.peraton.com/.

authorized users. At the same time, they should leverage commercial SATCOM as primarily a surge capacity for noncritical communications such as entertainment and personal communications.

But as the delineation of critical and noncritical traffic versus military or commercial SATCOM use is not always clear, the use of commercial systems as a backup for critical traffic could also be employed to increase the overall probability of mission success. Such a move would provide redundancy, improve access, and increase the complexity of the problem from an adversary's perspective, providing security in depth.

Continuing to field government-owned satellite systems and focusing on channeling critical communications through DOD SATCOM can significantly mitigate the risks associated with commercial systems and reduce commercial satellite platforms' security and reliability requirements. With the new US Space Force acquisition model for future satellite systems, the Department could mitigate risks related to costs by leveraging recent commercial satellite advancements and commercial-off-the-shelf components where appropriate while continuing to draw from DOD in-house developments to keep the system protected by its singularity.[24] This solution would improve the variables of system access, interoperability, reliability, and security by ensuring all DOD-affiliated networks rely on the same satellite systems as they exchange and utilize the same data.

Conclusion

As time goes on, the military's use of commercial SATCOM increasingly plays a more pronounced role in the military SATCOM architecture as the DOD looks to manage its resources more efficiently. With today's fiscally constrained environment of military budgets and decreased spending, defense planners are giving substantial consideration to commercial SATCOM, but risks lay in the balance.

The background and arguments presented in this article show the military's surging dependence on commercial SATCOM presents access, protection, and C2 vulnerabilities in myriad areas for operational US forces. Assured military communications relying heavily on SATCOM systems in a wartime environment will enable US battlefield success. The needed increase in SATCOM capacity has driven the Department to contract satellite usage from commercial providers. While the requirements are well defined, the commercial sector has its drivers (in cost and performance) that may not align with strict DOD requirements.

Historically, the military research and development machine has maintained the US military's technological edge. Reliance on commercial SATCOM systems will shift this responsibility outside of DOD lifelines, although not completely as the Department retains some in-house SATCOM systems. While commercial satellite communications are a viable solution for some high-data-rate transfer of noncritical information, the military

[24] J. R. Wilson, "How Military Harvests Technology from Commercial Industry," *Military & Aerospace Electronics*, October 1, 2016, https://www.militaryaerospace.com/.

must be conscious that this increased SATCOM capacity is vulnerable and could be cut off at any time.

The US military need for SATCOM capacity beyond what military systems can provide is the main driver of its use of commercial satellite communications systems. The near-term cost benefits for almost on-demand satellite access for forces at the tactical and operational levels have greatly increased the communications capacity of the US military.

While the vulnerabilities highlighted in this article are stark and troubling, diligent system assignment and continued focus on protecting both military- and commercially developed satellite communications systems will lead to assured SATCOM use for US military forces. Management of all satellite communications systems within the Department of Defense will help mitigate the risks and vulnerabilities presented by the military use of commercial SATCOM systems.

Specifically, the consolidation of SATCOM management roles and responsibilities to the US Space Force should help spearhead and address these concerns. Continued focus on the management of the space domain can address some of the concerns presented here. Still, it is also clear the satellite communications field will need American ingenuity to maintain a competitive technological edge for assured access and protection.

Jonathan K. Corrado, PhD

Commander Jonathan K. Corrado, USNR, is a qualified surface warfare officer and Seabee combat warfare officer. As a civilian, Dr. Corrado works in the nuclear industry.

Disclaimer and Copyright

The views and opinions in *Air & Space Operations Review* (*ASOR)* are those of the authors and are not officially sanctioned by any agency or department of the US government. This document and trademarks(s) contained herein are protected by law and provided for noncommercial use only. Any reproduction is subject to the Copyright Act of 1976 and applicable treaties of the United States. The authors retain all rights granted under 17 U.S.C. §106. Any reproduction requires author permission and a standard source credit line. Contact the *ASOR* editor for assistance: asor@au.af.edu.