AIR COMMAND AND STAFF COLLEGE

AIR UNIVERSITY

SATCOM Supply Versus Demand and the Impact on Remotely Piloted Aircraft ISR

by

Lisa A. Baghal, Major, USAF

A Research Report Submitted to the Faculty

In Partial Fulfillment of the Graduation Requirements for the Degree of

MASTER OF OPERATIONAL ARTS AND SCIENCES

Advisor: Mr. Michael Ivanovsky

Maxwell Air Force Base, Alabama

March 2016

DISCLAIMER

The views expressed in this academic research paper are those of the author and do not reflect the official policy or position of the U.S. Air Force, the U.S. government or the Department of Defense. In accordance with Air Force Instruction 51-303, it is not copyrighted, but is the property of the United States government.

ABSTRACT

Changes in Intelligence, Surveillance, and Reconnaissance (ISR) sensor technology have drastically increased the amount of available data, but the primary method of transmitting the data – Satellite Communications (SATCOM) – has not kept pace. Remotely Piloted Aircraft (RPA) such as the MQ-1 Predator and MQ-9 Reaper are a major user of SATCOM for both command and control and data links. Their full motion video (FMV) sensors provide exquisite ISR capability; however, FMV requires significant SATCOM bandwidth. With military SATCOM (MILSATCOM) capacity at a premium, RPA ISR dissemination is executed exclusively via commercial SATCOM (COMSATCOM). While this may seem like a reasonable solution, there are shortfalls and limitations that must be considered. Especially given that COMSATCOM availability is not guaranteed, and that the Department of Defense (DoD) cannot dictate changes to the constellation to accommodate its evolving needs, the solution set to ensure continuing growth in RPA ISR operations must be robust and multifaceted. Therefore, the DoD must approach the problem from all angles: demanding less RPA ISR, providing more SATCOM bandwidth, and being more efficient at using available SATCOM capacity. In that light, this essay intends to evaluate the gap between SATCOM bandwidth supply and demand, associated consequences, and a range of potential solutions.

CONTENTS

INTRODUCTION

Changes in Intelligence, Surveillance, and Reconnaissance (ISR) sensor technology have drastically increased the amount of available data, but the primary method of transmitting the data – Satellite Communications (SATCOM) – has not kept pace. Remotely Piloted Aircraft (RPA) such as the MQ-1 Predator and MQ-9 Reaper are a major user of SATCOM for both command and control and data links. Their full motion video (FMV) sensors provide exquisite ISR capability; however, FMV requires significant SATCOM bandwidth. With military SATCOM (MILSATCOM) capacity at a premium, RPA ISR dissemination is executed exclusively via commercial SATCOM (COMSATCOM). While this may seem like a reasonable solution, there are shortfalls and limitations that must be considered. Especially given that COMSATCOM availability is not guaranteed, and that the Department of Defense (DoD) cannot dictate changes to the constellation to accommodate its evolving needs, the solution set to ensure continuing growth in RPA ISR operations must be robust and multifaceted. Therefore, the DoD must approach the problem from all angles: demanding less RPA ISR, providing more SATCOM bandwidth, and being more efficient at using available SATCOM capacity. In that light, this essay intends to evaluate the gap between SATCOM bandwidth supply and demand, associated consequences, and a range of potential solutions.

BACKGROUND

Supply and Demand

DoD use of SATCOM has skyrocketed since Operation Desert Storm in 1991. MILSATCOM assets do not provide the needed bandwidth capability, so DoD must supplement bandwidth with COMSATCOM assets. To illustrate the increase in demand and lack of MILSATCOM supply, many statistics are available:

- During Operation Iraqi Freedom, SATCOM bandwidth requirements were 30 times that of Desert Storm.[1]
- MILSATCOM did not have the capacity to meet these requirements in either conflict, but the difference is in the ratio: in Desert Storm the DoD used approximately 20% COMSATCOM, whereas in Operation Iraqi Freedom we used approximately 80% COMSATCOM.[2]
- Some accounts from senior military leaders increase this estimate to 96%.[3]
- The use of fixed COMSATCOM in the Middle East and Africa increased more than 180% from 2003 to 2009.[4]
- RPA operations, a major requirement on SATCOM bandwidth, increased 300% between 2007 and 2011.[5]
- RPA data feeds from Iraq and Afghanistan in 2009 amassed 24 years of video footage, with estimates expected to increase thirtyfold by 2011.[6]
- Also of concern, DoD dependence on COMSATCOM rose by over 800% between 2000 and 2011.[7]

It is clear from these statistics the demand for SATCOM is growing, and DoD cannot meet the requirement on its own. Where the commercial sector once provided a gap-filler for DoD satellites, COMSATCOM has become the backbone of national security communications. Unfortunately, even with COMSATCOM augmentation, capacity is still limited and sometimes unavailable in current hot spots – the Middle East and Africa regions.[8]

SATCOM provides many services to US leaders and their forces including voice and video communications, Global Information Grid (GIG) network access, RPA command and control, and transmission of critical Intelligence, Surveillance, and Reconnaissance (ISR) data. While this essay focuses on the impact of RPA ISR dependence on SATCOM (specifically Reaper and Predator), the above statistics show SATCOM is a critical enabler and area of vulnerability in a wide range of military applications, to include command and control. The result is a need to share and prioritize SATCOM assets. However, this is not a straightforward proposition with many complexities. One aim of this essay is to highlight the complexities of planning, prioritizing, and utilizing SATCOM assets for RPA operations. The product of this analysis is a multi-dimensional solution set designed to attack the problem from many angles.

SATCOM Capabilities

SATCOM can be grouped into three categories: protected (nuclear hardened, secure, both fixed and mobile ground stations, low-to-moderate data rates), wideband (fixed ground system, high data rates), and narrowband (mobile ground system, low data rates). RPAs utilize wideband SATCOM due to its high data rate characteristics in the Ku (12-18 GHz) and Ka (26-40 GHz) frequency bands. The military operates the Wideband Global SATCOM system, and two of the primary COMSATCOM service providers for RPA operations are Intelsat and Eultelsat.

The legacy wideband MILSATCOM system is the Defense Satellite Communications System (DSCS). However, first launched in 1982, only seven are still operational. With the life of the DSCS satellites coming to an end, Wideband Global SATCOM System (WGS) is taking its place. With the same mission, "to provide worldwide flexible, high data rate and long haul communications for Soldiers, Sailors, Airmen, Marines, the White House Communication Agency, the U.S. State Department, international partners, and other special users," the WGS system provides an extraordinary increase in capability.[9] According to the Air Force Space Command (AFSPC) factsheet, "Just one WGS satellite provides more SATCOM capacity than the entire Defense Satellite Communications System constellation."[10] Furthermore, the WGS satellites can operate in both the X- and Ka- frequency bands, which is an unprecedented capability. The WGS system employs enhanced encryption algorithms, secure access controls, and limited anti-jam capability. However, there are only seven satellites in this constellation, with three additional satellites planned for launch.[11]

Intelsat provides wideband COMSATCOM for military, commercial and government customers, with a fleet of 50+ satellites. Its global terrestrial network includes both domestic and international teleports and more than 28,000 miles of fiber optic cable.[12] Intelsat has a strong international customer base, and is headquartered in Bermuda.[13] According to, "From remote military outposts, disaster recovery sites and U.S. embassies to health and homeland security agencies, Intelsat General's solutions support the most complex, mission-critical operations anywhere on the globe."[14]

Eultelsat, another COMSATCOM vendor, operates a fleet of 40 satellites over Europe, Africa, the Middle East, and portions of the Asian and American continents. It is a French Corporation with headquarters in Paris, France, employs 1,000 personnel from 37 countries.[15]

Government services only accounts for 14% of Eultelsat's portfolio of activity.[16] While Intelsat and Eultelsat are not exclusive commercial providers for RPA operations, they have a strong presence in the current area of operations.

RPA Requirements

This essay will focus on the MQ-1 Predator and MQ-9 Reaper. Both are multi-mission, medium altitude, long-endurance RPAs, employed as ISR collection assets or against dynamic execution targets. Both platforms employ various imagery, targeting, and full motion video systems.

The RPAs are employed using a concept of operations called "remote split operations." This requires launch and recovery sites within theater, but allows Ground Control Stations (GCS) in the continental US. According to the systems' factsheets, "Remote split operations result in a smaller number of personnel deployed to a forward location, consolidate control of the different flights in one location, and as such, simplify command and control functions as well as the logistical supply challenges for the weapons system."[17,18] However, this results in the requirement for beyond-line-of-sight SATCOM links, relay sites, and ground terminals. MQ-1 utilizes Ku-band, limiting it to COMSATCOM only. There are plans to upgrade the MQ-9 to operate in both Ku- and Ka-band, which would allow use of both COMSATCOM and MILSATCOM.[19]

The number of Combat Air Patrols (CAPs) has grown significantly, increasing demand on SATCOM systems for both command and control and ISR downlink. A 2010 Air Combat Command (ACC) report showed a plan for CAP growth from 45 to 65 CAPs per day by FY13, where each CAP requires two aircraft in flight during transit periods. This means planners must account for 98 CAPS per day worth of SATCOM time/bandwidth. This same report assessed the bandwidth requirement associated with the increase in CAPs is almost 300% higher, and data rate requirement is 600% higher, due in large part to increase in sensor capability. Examples of increased sensor capability includes multi-sensor suites, high definition video and wide area surveillance. Wide area surveillance ("city-sized") is accomplished through a system called "Gorgon Stare," which provides both day- and night-time full motion video ISR capability.[20] DoD confirmed an enhancement of the Gorgon Stare system, Increment II, to be operational in late 2015. This new increment is said to provide a four-fold increase in area coverage and a two-fold improvement in resolution.[21] While exact specifications are not available, this increase in capability certainly increases the requirement for SATCOM bandwidth.

ANALYSIS

Availability

The ACC report from 2010 describes an increase in number of CAPs and in sensor capability, resulting in a significant increase in SATCOM bandwidth requirements. A report to USSTRATCOM in 2009 predicted that Ku-band COMSATCOM, the primary means of MQ-1 and MQ-9 operations, would not be sufficient to meet RPA demand by 2018.[22] It is difficult to predict future COMSATCOM capacity because the commercial sector growth/decline is largely governed by factors other than government needs; however, given this analysis and trends in ISR capability and requirements, it would be shortsighted to rely on the COMSATCOM alone. The planned retrofit of the MQ-9 to include Ka-band MILSATCOM capability helps mitigate this concern, but given a limited, seven-satellite Ka-band constellation with competing priorities, availability emerges as a limiting factor for RPA operations and advancements.

Furthermore, the 2009 COMSATCOM capacity study does not account for the inherent risks and issues associated with relying on outside sources as a critical enabler to DoD missions. Because DoD does not own the assets, the capability is not on-demand. COMSATCOM services must be procured and scheduled through the Defense Information Security Agency (DISA), a process that can take months. According to a 2003 Government Accountability Office (GAO) report, DoD users did not find the DISA process, which averaged 79 days, timely or flexible enough to meet their needs.[23] The report stated that often times, services were procured outside the DISA process to meet operational needs. In the intervening years, this issue has not been resolved – a 2015 GAO report found that 32% of fixed COMSATCOM services were still being procured outside DISA channels.[24] While DISA currently advertises anywhere from 4 hours to 90 days for service awards, a 2011 GAO report states that operational requirements in the Middle East are still not being met.[25,26]

There is also no guarantee that commercial vendors will provide supply even if they have the capacity. The DISA COMSATCOM ordering guide explicitly calls out this risk:

> "SATCOM planners cannot assume availability on any given satellite to be available when needed. Availability of COMSATCOM resources is continuously in flux. When there is a known requirement, planners must act quickly to assure access to a particular transponder, coverage, and bandwidth. There is no way to know if bandwidth is available until a user attempts to lease it."[27]

Mergers and acquisitions of satellite vendors, resulting in less capacity and higher cost, exacerbate this risk.[28]

Finally, COMSATCOM systems do not provide protection against jamming, increasing risk against availability. Jamming is one of the lowest-cost, easiest ways to degrade military operations. In 2006, an analysis provided to the House Armed Services committee showed that in a 16-month period during Operation Iraqi Freedom, there were 50 documented cases of interference on DoD-utilized SATCOM.[29] The problem continues still – in early 2015, the US Strategic Command Commander, Admiral Cecil Haney said, "US national security space systems are facing a serious growing threat…For example, multiple countries have developed and are frequently using military jamming capabilities designed to interfere with satellite communications and global positioning systems."[30]

Mission Impact. Lack of SATCOM availability degrades the number of CAPs that can be flown, but can also inhibit the effectiveness or value of executed CAPs. Even if a CAP is completed, lack of bandwidth could limit its operational area or amount of ISR that can be downlinked. As previously stated, ACC anticipates a 600% increase in data rate with its increase in CAPs from 45 to 65 (45% increase) – clearly due in large part to increased sensor capability. Therefore, if SATCOM capacity is not increased, even a successful CAP could be "dropping" valuable ISR due to inability to downlink. Furthermore, as data rates increase, operational area decreases unless satellite power is addressed.[31] This issue can only be addressed with improved satellite constellations. Anti-jam capability is also something that is best accomplished on the space segment, requiring new satellites on orbit. Given that the government sector does not control or even command a majority of the business revenue for COMSATCOM systems, it may be difficult to resolve some of the technical limitations of current satellite architectures. This is compounded by the inefficient planning and scheduling process, without guarantee for bandwidth when required. Any solution set to mitigate DoD's dependence on COMSATCOM should seek to resolve the ambiguity in service availability.

Security

What MILSATCOM lacks in availability it makes up for in data confidentiality and integrity. MILSATCOM systems provide strong encryption techniques that are virtually unbreakable. While COMSATCOM may have more capacity – though not unlimited – its use presents security issues due to lack of strong encryption algorithms and physical protection techniques. Commercial SATCOM systems are not required to employ the same access controls as military systems. Without regulation and protection of the ground system, to include command and control sites, fiber optic networks and data repositories, data security is at risk. This is especially concerning when utilizing non-US based companies providing RPA service in the CENTCOM and PACOM areas of responsibility.

Encryption on COMSATCOM systems is a concern as they are not exquisite and are vulnerable to cracking. A bigger issue, though, is that data is routinely transmitted unencrypted due to the large amount of bandwidth and satellite power that encryption algorithms require. If unencrypted, or encrypted using standard commercial algorithms, adversaries within the footprint of the downlink could intercept and interpret the data. This was proven when hackers in Iraq and Afghanistan used SkyGrabber, downloadable from the internet for $26, to intercept unencrypted video feeds from the Predator through SATCOM links. [32] The decision to send data without encryption was because it slowed down the real-time link.[33]

Mission Impact. Eavesdropping could provide an adversary invaluable insight into US national security sources, methods, and plans. Knowing what our capabilities are – what we can see/hear and what we cannot – can give a dramatic advantage to the adversary in their ability to conduct counter operations. First, it allows them to develop evasion tactics. Second, it allows them to develop and execute effective deception tactics. Both of these counter operations could be detrimental to the RPA ISR mission, especially given its persistent nature. Long-term surveillance, coupled with the knowledge of our ISR capability, could allow the adversary time to slowly adapt and evolve patterns of behavior that limit ISR effectiveness. More secure encryption algorithms would mitigate these concerns but come with added cost – both monetarily and in bandwidth. Because these satellites are not under DoD control, it is imperative to search for solutions that can enhance security utilizing existing constellations.

RECOMMENDATIONS

Less ISR

It is clear from the preceding discussion there is a gap in SATCOM supply and demand for RPA operations, with both availability and security implications. The solution space includes: (1) demand less RPA ISR, (2) supply more SATCOM, or (3) provide a more efficient method of delivery. From trends in RPA Combat Air Patrols (CAPs), language from the USAF leadership, and USAF investments, it seems demanding less RPA ISR is not a viable option. For example, Lt. Gen. Bob Otto, U.S. Air Force deputy chief of staff for intelligence, surveillance and reconnaissance (ISR) has said, "Crisis has become the steady state," and that "the unconstrained demand for ISR" can never be met. In a speech at an Air Force Association meeting, Lt Gen Otto said that when there were 11 full-motion video (FMV) combat air patrols (CAPs) over Iraq in 2005-2007, CENTCOM commanders reported they were meeting only a third of their requirement, but "now we have 65 CAPs, yet CENTCOM says they are still only meeting 21 percent of the requirement."[34] However, even if crisis has become the steady state, DoD must find a way to manage ISR expectations to a manageable level.

The statistics Lt Gen Otto highlighted may indicate RPA CAPs are not meeting requirements effectively. This is consistent with a House Permanent Select Committee on Intelligence (HPSCI) audit, which highlights DoD's need to better define and prioritize ISR requirements and improve future planning in acquisitions of ISR systems and forces.[35] The report calls DoD "ineffective at defining and prioritizing its ISR requirements in light of insatiable demand for ISR."[36] The HPSCI indicates a flaw in the metrics used to define requirements (time on station) and demand (total unmet requests) and suggests a construct linked more to mission effectiveness would be better. For example, the current system does not report number of met/unmet requirements by priority, rather as a percent of all requirements. This does not adequately illuminate effectiveness of the ISR apparatus. Similarly, the report admonishes the CAP metric for measuring time rather than effect, potentially resulting in extraneous ISR that adds little value. [37] Again, this metric does not illuminate effectiveness of an RPA CAP – only that it was in the air for 24 hours. With a system similar to the Army's Integrated Sensor Coverage Area (ISCA) requirements process, ISR demand could be decreased to missions with distinct value. ISCA is platform-agnostic, and could maximize effectiveness across the entire ISR asset portfolio. A change in how the Air Force defines and prioritizes ISR requirements, specifically the metrics that define CAP effectiveness, would take a necessary first step in understanding the real problem and apportioning SATCOM bandwidth to requirements that produce the most effect. This is one necessary way to decrease the gap between supply and demand.

More SATCOM

While an expensive and time-consuming process to produce and launch MILSATCOM assets, the USAF could consider this option. However, given the lengthy development process, DoD must rely on the commercial sector to increase SATCOM capacity in the near-term. Intelsat is launching a new system, Intelsat Epic, which will utilize the C-, Ku-, and Ka-frequency bands and enable "four to six times the bandwidth equivalent of conventional commercial satellites and two-to-three times that of WGS satellites."[38] Epic will use spot beam and frequency-reuse technology to increase efficiency and decrease cost per bit. The first two of these enhanced-capability satellites are planned for launch in 2016 with five more to follow on an undisclosed schedule.[39]

Even with commercial sector upgrades to increase capacity, it is unclear that COMSATCOM will remain the more economical option in the future. First, the industrial base is shrinking due to mergers and acquisitions, leading to increased cost per bit. Second, the procurement mechanisms are inefficient and not cost effective. The current one-year leasing process has been identified in multiple sources as being highly inefficient and costly. Notably, the 2014 National Defense Authorization Act (NDAA) calls single year leases "often the most expensive and least strategic method," and calls for updating DoD's regulations to enable multi-year leases. [40] In addition to multi-year leases, the DoD should consider anchor tenancy agreements, and Indefeasible Right of Use agreements, which provide more assurances in the availability of COMSATCOM for DoD use.[41] Unguaranteed use is one of the major concerns with dependence on the commercial sector, but greater investment into the company would gain some buying power for DoD.

Inefficiencies in the DISA COMSATCOM procurement and scheduling process were identified in a 2003 GAO report and were reiterated in a follow-up 2015 GAO report.[42] Failure of the process is highlighted by the 2016 NDAA recommendation for AFSPC to take control from DISA within three years.[43] Consolidating all SATCOM (both military and commercial) development and procurement activities under one entity would provide more flexibility in which asset could fill a user's requirement, may decrease costs, and will close the feedback loop with future system development. Both 2015 and 2016 NDAAs continue to direct DoD to increase efficiency in the COMSATCOM procurement process.[44,45] It is clear that to respond to the growing need in SATCOM for enhanced RPA use, DoD must resolve deficiencies the planning and procurement process.

Even with enhanced capacity and a more efficient, cost effective process, COMSATCOM currently still presents security concerns due to lack of strong encryption and foreign ownership. While it has not gained much traction in DoD, the Operationally Responsive Space Office (ORS) might be the right DoD organization to build and deploy a dedicated MILSATCOM constellation with military-grade encryption and anti-jam techniques. The problem will be with navigating the DoD acquisition regulations that make major procurements lengthy and complex. One of ORS's goal business models is to build multiple like-kind small satellites, which has been proven cost effective in the commercial sector.[46] If accomplished, owning a dedicated MILSATCOM constellation, even if less capable than WGS or some of the next-generation COMSATCOM, would lessen the burden of unguaranteed scheduling and increase data security. This could be an ideal solution and deserves more investigation and attention, but does not appear viable in the near-term.

Increase Efficiency

Given that demanding significantly less RPA ISR is not a likely option and acquiring more COMSATCOM capacity is limited due to lack of control over the commercial sector, DoD must better utilize the bandwidth currently available. Fortunately, there are potential technical solutions that can pack more information into the same data stream to mitigate lack of availability. In some cases, these solutions can also increase security of the data stream.

Terminal Interoperability. One way to increase utility of available SATCOM assets is to increase terminal interoperability. If all ground and air assets are equipped to receive/transmit in both Ku- and Ka- band, it will enable use of both MILSATCOM and COMSATCOM, whereas RPAs are currently using COMSATCOM exclusively. In addition to higher data rates and additional capacity, the ability to utilize MILSATCOM assets provides some needed flexibility and control into the scheduling process. As of 2010, there were no Ka-capable RPA ground sites, with plan to add/upgrade to allow an almost equal distribution of Ku- and Ka-CAPs.[47] The 2010 plan predicts the ability to start utilizing WGS Ka-band SATCOM in FY15. While this is an important step, it is recommended that all RPA and ground terminals be upgraded to utilize both Ku- and Ka- frequency bands. Use of X-band could also be considered as WGS is X-band capable as well.

Protected Tactical Waveform. Lack of strong encryption and anti-jam capability on COMSATCOM systems is a risk to confidentiality, integrity and availability. The Protected Tactical Waveform (PTW) offers a technical solution projected to improve encryption and anti-jam capability through a change in the ground terminals rather than satellites. This will allow enhanced security on communications without changing the requirements on commercial satellites. The PTW is an architecture-agnostic ground modem that will provide source-based cryptography to increase data confidentiality and integrity, and frequency hopping capability to increase availability through resistance to jamming.[48] This solution will enable the continued use of the expansive commercial SATCOM constellations while decreasing security risk at minimal relative cost.

Compression. Compression technology can dramatically reduce bandwidth requirements, but does degrade image quality to a degree. The RAND Corporation conducted a study for the Army on how to "use bandwidth better" as a solution to stresses on their communication requirements. The report identifies several methods of compression with varying degrees of quality reduction. With respect to FMV, the MPEG method of compression is considered standard practice in the entertainment industry, but has a low compression ratio to maintain image quality. Various methods can result in much higher compression ratios, but the amount of compression that can be achieved depends on the amount of motion in the video. According to David Strong, a senior official at FLIR Government Systems which produces multiple ISR systems for the DoD, compression is necessary and economical without unacceptable image degradation. He says, "You can't cost effectively downlink using uncompressed video, so we use MPEG-4…MPEG-4 gives operators 95 percent of the image quality when they're viewing a 10Mbps stream versus 1.5Gbps for an uncompressed stream."[49] The RAND report cautions that, "The quality factor is hard to analyze without empirical testing. If the decoded images are to be viewed by humans, then humans should be the judges of quality."[50] ISR's value is in the eye of the analyst, so compression can only go so far before it becomes inactionable. Therefore, compression is likely a long-term partial solution, but with increasing sensor capabilities, it will not solve overall problem of insatiable ISR demand with limited SATCOM bandwidth. In other words, compression is necessary but not sufficient.

Laser Data Links. Using laser for data transmission is not a new idea, but has only recently been proven feasible. The Air Force started a laser SATCOM program, called Transformational Satellite Communications System (TSAT), in 2004 with projected launch in 2011. However, cost and schedule overruns – partly due to technological difficulties with the laser transceiver design – resulted in the program being cancelled in 2010.[51] Fortunately, NASA, the European Space Agency (ESA) and commercial SATCOM vendors have continued to develop the technology with success. In 2014, NASA's Jet Propulsion Laboratory produced a laser transmitter called OPALS, which successfully transmitted both text and video from the International Space Station to a ground control station. In one test, a video which took 12 hours to upload via traditional radio frequency was downloaded in a mere seven seconds using OPALS.[52] ESA and Airbus Defense and Space Company have also produced a laser transmitter, the European Data Relay System (EDRS), which was launched aboard a Eultelsat satellite in January 2016.[53] The system is not yet operational.

For comparison, current Ku-band satellites can provide 12.8Mbps, the enhanced Ku-band IntelsatEpic satellites to be launched in 2016 will provide 200Mbps downlink data rate, while OPALS and EDRS provide 1.8Gbps downlink data rate – a tenfold increase in download speed.[54, 55] This may sound like an obvious solution for the RPA bandwidth problem; however, there are drawbacks to consider. First, this technology has not been tested on space-to-air platforms. The movement on both ends of the link is considerably more difficult than a space-to-ground link, where one end is stationary. While Airbus Defense and Space plan to test this capability, specifically for the purposes of potential RPA use, it is unclear that it is feasible in the near-term. Second, laser links are very susceptible to atmospheric and environmental interference, which could degrade availability significantly.[56] Third, implementing a laser SATCOM solution would require an overhaul of the ground and airborne terminals to accommodate the new technology. Because of these reasons, laser data links may be a long-term solution, but will not resolve bandwidth issues in the near-term.

CONCLUSION

The statistics on SATCOM and RPA use clearly indicate a gap between SATCOM supply and RPA demand, which is on a growing trajectory given increasing RPA capability. To fill the gap, DoD procures a significant portion of its SATCOM bandwidth from commercial vendors, but this presents problems of its own. COMSATCOM is not as prevalent as some may think, due to competing business markets outside the US government, lack of jamming protection, and the inefficiency of DoD's COMSATCOM procurement process. Relying on COMSATCOM also increases security risk due to lack of strong encryption. For only $26, hackers were able to intercept and watch Predator feed in Iraq and Afghanistan, giving them valuable insight into US operations.

Because this problem is complex and multifaceted, the solution set must also cover a range of options. All of the solutions presented are necessary, but none are sufficient in isolation. First, DoD must implement a system to better understand, prioritize, and track ISR requirements, such that we can more effectively and efficiently task RPAs. This process may prove invaluable in many ways, only one of which would be to lessen the gap between RPA demand and SATCOM supply. Second, DoD must re-evaluate its reliance on COMSATCOM and the procurement processes. While a dedicated MILSATCOM constellation may be unattainable in the near term, it should not be discounted given the availability and security concerns with dependence on the commercial sector. In the interim, DoD should change the process for scheduling time on commercial constellations to allow more flexibility and assured access.

Improving ISR requirement and SATCOM scheduling processes will likely not solve the problem alone, given the rate at which RPA capability is increasing while SATCOM enhancements lag behind. Therefore, it is imperative to investigate and implement a combination of solutions that allow a more efficient use of the available bandwidth. Terminals should be upgraded to transmit and receive in multiple frequency bands to add flexibility as to which SATCOM constellations can be utilized. A very important first step is upgrading both RPA and associated ground terminals to accept Ka-band signals, allowing the use of WGS. Also, more efficient and secure waveforms, such as the Protected Tactical Waveform, should be pursued to enhance availability and security on existing infrastructure. Compression is already in use, and future advanced algorithms should continue to be investigated as this will remain critical to packing as much information into a data stream as possible. However, because compression degrades image quality, it can only provide a partial solution. Finally, laser data links may seem like science fiction, but have recently been proven on a NASA space-to-ground experiment with astounding increases in data rates. Unfortunately, this technology has not yet been proven for space-to-air applications and is therefore not viable in the near-term. Due to the initial success, though, it should not be discounted and should remain a research and development priority for DoD. The recommendations provided herein combine near- and long-term solutions that must remain a focus given that "crisis is now the steady state" and SATCOM upgrades are not keeping pace with RPA enhancements.

---

[1] Eberhart, Bryan, Kenneth Kemmerly, Paul Konyha, "Satellite Communications," Air University Space Primer, Chapter 14, 183.

[2] Forest, Benjamin, "An Analysis of Military Use of Commercial Satellite Communications," Naval Postgraduate School, September 2008, 10.

[3] Werner, Debra, "Cover Story: Hacking Cases Draw Attention To Satcom Vulnerabilities," Defense News, 23 January 2012, http://archive.defensenews.com/article/20120123/C4ISR02/301230010/Cover-Story-Hacking-Cases-Draw-Attention-Satcom-Vulnerabilities (accessed 9 Dec 2015).

[4] Government Accountability Office, Report to Congress, "Telecommunications: Competition, Capacity, and Costs in the Fixed Satellite Services Industry," Report GAO-11-777, September 2011, 2.

[5] Ibid., 12-13.

[6] Johnson, Kimberly, "Full-motion video proves boon to intel gathering," Defense Systems, 7 October 2011, https://defensesystems.com/articles/2011/10/10/c4isr-2-unmanned-aircraft-systems-video.aspx.

[7] Government Accountability Office, Report to the Committee on Armed Services, “Defense Satellite Communications, DoD Needs Additional Information to Improve Procurements,” Report GAO-15-459, July 2015, 9.
[8] Ibid.
[9] Air Force Space Command, WGS Factsheet, http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5333 (accessed 9 Dec 2015).
[10] Ibid.
[11] Ibid.
[12] Intelsat General, Informational Pamphlet, “Far More than Satellite Bandwidth,” http://www.intelsatgeneral.com/ (accessed 9 Dec 2015).
[13] Forest, Benjamin, “An Analysis of Military Use of Commercial Satellite Communications,” Naval Postgraduate School, September 2008, 35.
[14] Intelsat Government Services, http://www.intelsat.com/services/government-services/ (accessed 9 Dec 2015).
[15] Eultelsat, “Our Business,” http://www.eutelsat.com/en/group/our-business/where-we-operate.html
[16] Eultelsat, “Facts and Figures” Brochure, http://www.eutelsat.com/en/group/our-business/what-we-do.html
[17] Air Combat Command, Reaper Factsheet, 23 Sep 2015, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104470/mq-9-reaper.aspx.
[18] Air Combat Command, Predator Factsheet, 23 Sep 2015, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104469/mq-1b-predator.aspx.
[19] Air Combat Command Headquarters, ACC/A8QC, “SATCOM Plan for 65 CAPs,” 12 Apr 10.
[20] Sierra Nevada Corporation, “Gorgon Stare” factsheet, http://www.sncorp.com/Pdfs/BusinessAreas/Gorgon-Stare_Sierra-Nevada-Corp-ISR_20140630.pdf.
[21] Jennings, Gareth, HIS Jane’s Defense Weekly, “DoD confirms Gorgon Stare to be operational in Afghanistan,” London, 16 December 2015, http://www.janes.com/article/56720/dod-confirms-gorgon-stare-to-be-operational-in-afghanistan.
[22] Air Combat Command Headquarters, ACC/A8QC, “SATCOM Plan for 65 CAPs,” 12 Apr 10.
[23] Government Accountability Office, Report to Congress, “Satellite Communications, Strategic Approach Needed for DoD’s Procurement of Commercial Satellite Bandwidth,” Report GAO-04-206, December 2003, 13.
[24] Government Accountability Office, Report to the Committee on Armed Services, “Defense Satellite Communications, DoD Needs Additional Information to Improve Procurements,” Report GAO-15-459, July 2015, 8.
[25] COMSATCOM Center, “Commercial Satellite Communications Ordering Guide,” Defense Information Support Agency, Version 2.2, May 2014, 15.
[26] Government Accountability Office, Report to Congress, “Telecommunications: Competition, Capacity, and Costs in the Fixed Satellite Services Industry,” Report GAO-11-777, September 2011, 12.
[27] COMSATCOM Center, “Commercial Satellite Communications Ordering Guide,” Defense Information Support Agency, Version 2.2, May 2014, 6.
[28] Government Accountability Office, Report to Congress, “Telecommunications: Competition, Capacity, and Costs in the Fixed Satellite Services Industry,” Report GAO-11-777, September 2011, 17-22.
[29] InfoSec Institute, “Hacking Satellites … Look Up to the Sky,” http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/, September 18, 2013 (accessed 9 Dec 2015).
[30] Garamone, Jim, “Stratcom Chief: U.S. Must Maintain Space Dominance,” DoD News, Washington, 6 February 2015, http://www.defense.gov/News-Article-View/Article/604064 (accessed 9 Dec 2015).
[31] Air Combat Command Headquarters, ACC/A8QC, “SATCOM Plan for 65 CAPs,” 12 Apr 10.
[32] InfoSec Institute, “Hacking Satellites … Look Up to the Sky,” http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/, September 18, 2013 (accessed 9 Dec 2015).
[33] Mount, Mike and Elaine Quijano, “Iraqi insurgents hacked Predator drone feeds, U.S. official indicates,” CNN, 17 December 2009, http://www.cnn.com/2009/US/12/17/drone.video.hacked/index.html (accessed 9 Dec 2015).
[34] Pocock, Chris, AIN Online, “The Revolutionary but Thorny U.S. Predator-Reaper Program,” 13 June 2015, http://www.ainonline.com/aviation-news/defense/2015-06-13/revolutionary-thorny-us-predator-reaper-program.
[35] House Permanent Select Committee on Intelligence, “Performance Audit on Department of Defense Intelligence, Surveillance, and Reconnaissance,” April 2012.
[36] Ibid, 1.
[37] Ibid, 5.
[38] Intelsat, “Introducing Intelsat Epic,” http://www.intelsat.com/infrastructure/intelsat-epicng/ (accessed 11 Feb 2016).

[39] Intelsat, "Intelsat Epic Frequently Asked Questions," http://www.intelsat.com/infrastructure/intelsat-epicng/frequently-asked-questions/ (accessed 11 Feb 2016).
[40] *National Defense Authorization Act for Fiscal Year 2014,* Public Law 113–66, 113TH Congress, *1st Sess*. December 2013, 157
[41] Defense Business Board, "Taking Advantage of Opportunities for Commercial Satellite Communications Services," 24 January 2013, 15.
[42] Government Accountability Office, Report to the Committee on Armed Services, "Defense Satellite Communications, DoD Needs Additional Information to Improve Procurements," Report GAO-15-459, July 2015, 19.
[43] Senate Armed Services Committee, *National Defense Authorization Act for Fiscal Year 2016 Report to Accompany S. 1376*, 114th Congress, 1st sess., Report 114-49, 9 May 2015, 263.
[44] *National Defense Authorization Act for Fiscal Year 2015*, Public Law 113–291, 113TH Congress, *2d Sess*. December 2014, 339-340.
[45] Senate Armed Services Committee, *National Defense Authorization Act for Fiscal Year 2016 Report to Accompany S. 1376*, 114th Congress, 1st sess., Report 114-49, 9 May 2015, 264.
[46] Baghal, Lisa, "Assembly, Integration and Test Methods for Operationally Responsive Space Satellites," Air Force Institute of Technology, Wright Patterson AFB, OH, March 2010.
[47] Air Combat Command Headquarters, ACC/A8QC, "SATCOM Plan for 65 CAPs," 12 Apr 10.
[48] Chuang, Jo-Chieh, Joseph Han, and Bomey Yang, "2025 and Beyond: The Next Generation of Protected Tactical Communications," Crosslink Magazine, Aerospace Corporation, 1 September 2014, http://www.aerospace.org/crosslinkmag/fall-2014/2025-and-beyond-the-next-generation-of-protected-tactical-communications/ (accessed 9 Dec 2015).
[49] Defense Systems, "Military Pushes for more capable sensor inputs for UAVs," 19 Dec 2011.
[50] Pane, John F., and Leland Joe, "Making Better Use of Bandwidth," The RAND Corporation, 2005, 29-30.
[51] Government Accountability Office, Report to Congressional Committees, "DOD Needs Additional Knowledge as it Embarks on a New Approach for Transformational Satellite Communications System," Report GAO-06-537, May 2006.
[52] Photonics.com, "Tests of Space Station's Laser Downlink Successful," Pasadena, CA, 15 December 2014, http://www.photonics.com/Article.aspx?AID=56998
[53] Clark, Steven, "Laser-equipped satellite to inaugurate European data relay system," Space Flight Now, 28 January 2016, http://spaceflightnow.com/2016/01/28/laser-equipped-satellite-to-inaugurate-european-data-relay-system/.
[54] Air Combat Command Headquarters, ACC/A8QC, "SATCOM Plan for 65 CAPs," 12 Apr 10.
[55] Clark, Steven, "Laser-equipped satellite to inaugurate European data relay system," Space Flight Now, 28 January 2016, http://spaceflightnow.com/2016/01/28/laser-equipped-satellite-to-inaugurate-european-data-relay-system/.
[56] Clark, Steven, "Laser-equipped satellite to inaugurate European data relay system," Space Flight Now, 28 January 2016, http://spaceflightnow.com/2016/01/28/laser-equipped-satellite-to-inaugurate-european-data-relay-system/.

BIBLIOGRAPHY

Air Combat Command, ACC/A8QC, "SATCOM Plan for 65 CAPs," 12 Apr 10.

Air Combat Command, Predator Factsheet, 23 Sep 2015, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104469/mq-1b-predator.aspx.

Air Combat Command, Reaper Factsheet, 23 Sep 2015, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104470/mq-9-reaper.aspx.

Air Force Space Command, WGS Factsheet, http://www.losangeles.af.mil/library/factsheets/factsheet.asp?id=5333.

Baghal, Lisa, "Assembly, Integration and Test Methods for Operationally Responsive Space Satellites," Air Force Institute of Technology, Wright Patterson AFB, OH, March 2010.

Chuang, Jo-Chieh, Joseph Han, and Bomey Yang, "2025 and Beyond: The Next Generation of Protected Tactical Communications," Crosslink Magazine, Aerospace Corporation, 1 September 2014, http://www.aerospace.org/crosslinkmag/fall-2014/2025-and-beyond-the-next-generation-of-protected-tactical-communications/.

Clark, Steven, "Laser-equipped satellite to inaugurate European data relay system," Space Flight Now, 28 January 2016, http://spaceflightnow.com/2016/01/28/laser-equipped-satellite-to-inaugurate-european-data-relay-system/.

COMSATCOM Center, "Commercial Satellite Communications Ordering Guide," Defense Information Support Agency, Version 2.2, May 2014.

Defense Business Board, "Taking Advantage of Opportunities for Commercial Satellite Communications Services," 24 January 2013.

Defense Systems, "Military Pushes for more capable sensor inputs for UAVs," 19 Dec 2011, https://defensesystems.com/articles/2011/12/13/c4isr-2-uav-sensors.aspx.

Eberhart, Bryan, Kenneth Kemmerly, Paul Konyha, "Satellite Communications," Air University Space Primer, Chapter 14.

Eultelsat, "Facts and Figures" Brochure, http://www.eutelsat.com/en/group/our-business/what-we-do.html.

Eultelsat, "Our Business," http://www.eutelsat.com/en/group/our-business/where-we-operate.html.

Forest, Benjamin, "An Analysis of Military Use of Commercial Satellite Communications," Naval Postgraduate School, September 2008.

Garamone, Jim, "Stratcom Chief: U.S. Must Maintain Space Dominance," DoD News, Washington, 6 February 2015, http://www.defense.gov/News-Article-View/Article/604064.

Government Accountability Office, Report to Congress, "Satellite Communications, Strategic Approach Needed for DoD's Procurement of Commercial Satellite Bandwidth," Report GAO-04-206, December 2003.

Government Accountability Office, Report to the Committee on Armed Services, "Defense Satellite Communications, DoD Needs Additional Information to Improve Procurements," Report GAO-15-459, July 2015.

Government Accountability Office, Report to Congress, "Telecommunications: Competition, Capacity, and Costs in the Fixed Satellite Services Industry," Report GAO-11-777, September 2011.

Government Accountability Office, Report to Congressional Committees, "DOD Needs Additional Knowledge as it Embarks on a New Approach for Transformational Satellite Communications System," Report GAO-06-537, May 2006.

House Permanent Select Committee on Intelligence, "Performance Audit on Department of Defense Intelligence, Surveillance, and Reconnaissance," April 2012.

InfoSec Institute, "Hacking Satellites … Look Up to the Sky," http://resources.infosecinstitute.com/hacking-satellite-look-up-to-the-sky/, September 18, 2013.

Intelsat General, Informational Pamphlet, "Far More than Satellite Bandwidth," http://www.intelsatgeneral.com/.

Intelsat Government Services, http://www.intelsat.com/services/government-services/.

Intelsat, "Introducing Intelsat Epic," http://www.intelsat.com/infrastructure/intelsat-epicng/.

Intelsat, "Intelsat Epic Frequently Asked Questions," http://www.intelsat.com/infrastructure/intelsat-epicng/frequently-asked-questions/.

Jennings, Gareth, HIS Jane's Defense Weekly, "DoD confirms Gorgon Stare to be operational in Afghanistan," London, 16 December 2015, http://www.janes.com/article/56720/dod-confirms-gorgon-stare-to-be-operational-in-afghanistan.

Johnson, Kimberly, “Full-motion video proves boon to intel gathering,” Defense Systems, 7 October 2011, https://defensesystems.com/articles/2011/10/10/c4isr-2-unmanned-aircraft-systems-video.aspx.

Mount, Mike and Elaine Quijano, “Iraqi insurgents hacked Predator drone feeds, U.S. official indicates,” CNN, 17 December 2009, http://www.cnn.com/2009/US/12/17/drone.video.hacked/index.html.

National Defense Authorization Act for Fiscal Year 2014, Public Law 113–66, 113TH Congress, *1st Sess*. December 2013.

National Defense Authorization Act for Fiscal Year 2015, Public Law 113–291, 113TH Congress, *2d Sess*. December 2014.

Pane, John F., and Leland Joe, “Making Better Use of Bandwidth,” The RAND Corporation, 2005.

Photonics, “Tests of Space Station’s Laser Downlink Successful,” Pasadena, CA, 15 December 2014, http://www.photonics.com/Article.aspx?AID=56998.

Pocock, Chris, AIN Online, “The Revolutionary but Thorny U.S. Predator-Reaper Program,” 13 June 2015, http://www.ainonline.com/aviation-news/defense/2015-06-13/revolutionary-thorny-us-predator-reaper-program.

Sierra Nevada Corporation, “Gorgon Stare” factsheet, http://www.sncorp.com/Pdfs/BusinessAreas/Gorgon-Stare_Sierra-Nevada-Corp-ISR_20140630.pdf.

Senate Armed Services Committee, *National Defense Authorization Act for Fiscal Year 2016 Report to Accompany S. 1376*, 114th Congress, 1st sess., Report 114-49, 9 May 2015.

Werner, Debra, “Cover Story: Hacking Cases Draw Attention To Satcom Vulnerabilities,” Defense News, 23 January 2012, http://archive.defensenews.com/article/20120123/C4ISR02/301230010/Cover-Story-Hacking-Cases-Draw-Attention-Satcom-Vulnerabilities.