CSBA
Center for Strategic and Budgetary Assessments

THE FUTURE OF MILSATCOM

Todd Harrison

THE FUTURE OF MILSATCOM

BY TODD HARRISON

2013

About the Center for Strategic and Budgetary Assessments

The Center for Strategic and Budgetary Assessments (CSBA) is an independent, nonpartisan policy research institute established to promote innovative thinking and debate about national security strategy and investment options. CSBA's goal is to enable policymakers to make informed decisions on matters of strategy, security policy, and resource allocation. CSBA provides timely, impartial, and insightful analyses to senior decision makers in the executive and legislative branches, as well as to the media and the broader national security community. CSBA encourages thoughtful participation in the development of national security strategy and policy, and in the allocation of scarce human and capital resources. CSBA's analysis and outreach focus on key questions related to existing and emerging threats to U.S. national security. Meeting these challenges will require transforming the national security establishment, and we are devoted to helping achieve this end.

ABOUT THE AUTHOR

Todd Harrison is the Senior Fellow for Defense Budget Studies at the Center for Strategic and Budgetary Assessments. Mr. Harrison joined CSBA in 2009 from Booz Allen Hamilton, where he supported clients across the Department of Defense, assessing challenges to modernization initiatives and evaluating the performance of acquisition programs. He previously worked in the aerospace industry developing advanced space systems and technologies and served as a captain in the U.S. Air Force Reserves. Since joining CSBA, Mr. Harrison has authored a number of publications on trends in the overall defense budget, modernization initiatives, the defense industrial base, military personnel costs, and the cost of the wars in Iraq and Afghanistan. He frequently contributes to print and broadcast media and is a term member of the Council on Foreign Relations. He is a graduate of the Massachusetts Institute of Technology with both a B.S. and an M.S. in Aeronautics and Astronautics. Mr. Harrison combines his budgetary, programmatic, and engineering experience with a strong background in systems analysis to lead the Budget Studies program for CSBA.

CONTENTS

EXECUTIVE SUMMARY

For much of the Cold War, space was a sanctuary for the U.S. military. U.S. space systems focused primarily on supporting strategic missions, such as missile warning, intelligence, and nuclear command and control, and a strategic détente held between the United States and Soviet Union. Since the end of the Cold War, however, the space domain has become more crowded and contested. More than 40 nations now own or operate satellites, and virtually all nations depend on space-based capabilities for civilian applications, such as weather forecasting and navigation. The 1991 Gulf War also marked a substantial shift in the way the U.S. military uses space systems. This conflict demonstrated the value of fusing space-based capabilities, such as precision navigation and timing and satellite communications, with conventional weapon systems to create what some have termed the "space-enabled reconnaissance strike complex."[1]

Since the end of the Cold War, an implicit assumption in the space domain has been that deterrence would hold and space systems would not be attacked in conventional conflicts. One of the consequences of this assumption is that U.S. space systems, and military satellite communications (MILSATCOM) systems in particular, have critical vulnerabilities in conventional warfare. MILSATCOM systems are vulnerable to physical attack (kinetic and non-kinetic), electronic attack (jamming), and cyber attacks. Potential adversaries are not as reliant on space-based capabilities and do not have symmetric vulnerabilities, making traditional deterrence in space a difficult proposition. Moreover, the U.S. military's critical dependence on space-based capabilities for global power projection means that counter-space capabilities may figure prominently in an adversary's anti-access/area denial (A2/AD) operations. From the perspective of other nations, U.S. military space systems are weapon systems, and space is a domain of warfare that can and will be contested.

While adapting to a more contested environment should be a priority for the next-generation MILSATCOM architecture, affordability must also be a priority. MILSATCOM systems are arguably just as vulnerable to cost overruns, funding instability, and other programmatic factors that can prevent a satellite from ever getting off the ground as they are to physical, electronic, and cyber attacks. MILSATCOM acquisitions are technologically complex with long development and production schedules and relatively small procurement quantities. These factors tend to reinforce one another in what has been called the "vicious cycle of space acquisition:" higher costs lead to smaller

[1] Jeff Kueter, "The War in Space Has Already Begun," The George C. Marshall Institute Policy Outlook, October 2006, p. 1.

constellations and longer production times; smaller constellations require more capabilities to be packed into each satellite; and packing more capabilities into each satellite drives up complexity, leading to even higher costs and longer production times.[2]

Synchronization across programs is also important in MILSATCOM because all three segments (space, terminal, and control) are needed for the system to be operational. The timing of when these segments are fielded relative to one another is important because satellites have a finite life on-orbit—fuel is consumed for station keeping, parts degrade from the harsh environment of space, and technology becomes obsolete with time. When one segment of the overall system is behind schedule due to funding shortfalls or development issues, the other segments may be forced to slip their schedules in response. Further complicating matters, the programs and associated budgets that fund the three segments of MILSATCOM are spread across the Services, making coordinated control of interdependent programs a challenge.

The Department of Defense (DoD) has a number of options in the next-generation MILSATCOM architecture to address the twin challenges of a more contested space environment and a more constrained budget environment. One option is to improve the passive defenses that allow a system to survive and operate through different forms of attack. Nuclear hardening, data encryption, interleaving, frequency hopping spread spectrum (FHSS), and satellite crosslinks are all forms of passive defenses. Active defenses, in contrast, attempt to intercept and disrupt an attack before it can affect communications and are primarily responsive to physical threats. Examples of active defenses include adding a shoot-back capability to satellites, deploying escort satellites, or using terrestrial forces to target the source of an attack on Earth. A shoot-back or escort satellite approach, however, runs the risk of creating orbital debris from a successful intercept, which could prove to be a long-term threat to other space systems.

Both active and passive defenses increase cost and complexity. The costs associated with implementing data encryption and FHSS, for example, are relatively small compared to the overall cost of the system because they can largely be implemented in software or in the payload without a fundamental change in the satellite design. Active defenses, such as a shoot-back capability, would likely add significant costs to MILSATCOM systems because they require some combination of a larger satellite bus or a smaller payload to compensate for the additional size, weight, and power needed for active defenses. For shoot-back and escort satellite defenses in particular, the attacker will have an inherent cost advantage because the cost of building more anti-satellite (ASAT) weapons is likely to be significantly less than the cost of deploying additional shoot-back or escort satellite systems.

Another approach to improve the protection of MILSATCOM systems is to make the systems more difficult to target by disaggregating, dispersing, or proliferating capabilities. In a disaggregated or dispersed architecture, each satellite or payload is smaller, less capable, and (in theory) less expensive, although the overall cost of the constellation may not be less expensive due to higher launch costs and the added cost of additional satellite buses. A proliferated constellation is by definition more expensive because more of the same satellites are procured. All three approaches make the system more resilient to the loss of a single satellite because each satellite represents a smaller fraction of overall capacity. This complicates an adversary's planning by forcing it to target more satellites to achieve the same effect, but it may not prove to be a significant challenge for an

[2] Lt. Gen. Ellen Pawlikowski, Doug Loverro, and Col. Tom Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," *Strategic Studies Quarterly*, Spring 2012, p. 36.

adversary with a deep magazine of ASAT munitions. The attacker will have a cost advantage as the competition scales because ASAT weapons will likely cost much less than the satellites they threaten. However, while the attacker will have a cost advantage in such a scenario, it may not be willing to escalate to a large-scale space attack, given the long-term, global problem of space debris produced by multiple destroyed satellites.

One approach to disperse and/or disaggregate the space segment is to adopt a payload-centric acquisition model that focuses on specifying the capabilities of the payload first and then finding a satellite bus to host the payload. As part of its rebalancing to the Asia/Pacific region, the United States could partner with Japan, South Korea, and Australia to host protected Advanced Extremely High Frequency (AEHF) payloads on one or more of their satellites in exchange for limited use of the global AEHF constellation. From the allies' perspective, this would improve interoperability with the U.S. military and give them access to a global constellation at a much lower cost than fielding an equivalent capability on their own. From an adversary's perspective, this would greatly complicate planning because an attack on the hosted payload (whether physical, electronic, or cyber) would be an attack on all partner nations in the network, creating the risk of horizontal escalation in a crisis.

A third option to address the vulnerabilities of MILSATCOM systems is to make the systems easier to replace after an attack. The military could have extra payloads or satellites ready to replace lost space assets after an attack, and mobile teleports and satellite control facilities could be used to replace damaged or destroyed ground sites rapidly. Making satellites easier to replace may be a viable option to reconstitute capabilities from a small-scale, limited-duration attack, although even with satellites sitting ready in storage it would take weeks to months to integrate them with launch vehicles, launch them, and move them to the desired orbit. In a more protracted conflict where an adversary is able to attack U.S. satellites repeatedly, it would quickly become cost prohibitive to keep replacing them. Once again, the United States could find itself on the wrong side of a cost-imposing strategy if the adversary's marginal cost of each attack is significantly less than the marginal cost of each replacement satellite or payload. Moreover, the stockpile of satellites or payloads ready at the start of the conflict could quickly be exhausted in a protracted conflict. Even with an active production line available, it would likely take months to years to build additional satellites or payloads.

A fourth option for mitigating the vulnerabilities of MILSATCOM is to find alternative means of communicating. Commercial SATCOM leases provide several advantages, including the flexibility to expand or reduce capacity as needed, but these systems offer virtually no protection from physical, electronic, and cyber attack and can be owned or operated by a foreign entity. An aerial communications layer can also be used to provide high-capacity communications to supplement or replace MILSATCOM within a region. If equipped with payloads using some of the passive protection features described above, such as FHSS, on-board processing, interleaving, and encryption, an aerial layer can be resistant to electronic and cyber attacks. The aircraft used to provide an aerial communications layer, however, can only operate in permissive airspace. They are by definition high emitters and can be targeted by air defense systems.

Terrestrial radio frequency (RF) communications (e.g., radio towers) are a viable alternative for users needing to communicate over relatively short distances. While terrestrial communications can employ many of the same protective features to resist jamming and cyber attack, these systems require a relatively permissive ground environment for the military to field and operate them. Users must have physical access to an area and be within line of sight of a ground station or another user. Another alternative to MILSATCOM is to change the way systems operate to reduce their communications needs. Unmanned aircraft, for example, could employ greater on-board capabilities to analyze sensor data autonomously, only transmitting data with a high probability of interest to analysts on the ground. A store-and-forward approach can also be useful in a contested communications environment to store data locally when communications are being jammed or when a platform wants to avoid detection and then transmit the data once communications are restored. A store-and-forward approach, however, is not an attractive alternative for time-sensitive operations. Overall, few viable alternatives to MILSATCOM exist for mobile platforms operating over long distances in an A2/AD environment.

The four options presented here to make MILSATCOM systems less vulnerable to attack and a less appealing target for adversaries, are by no means exhaustive or mutually exclusive. The value and priority placed on each of these options differs among MILSATCOM users, with some options being better or worse for a particular set of users depending on their operational needs. In a resource-constrained environment, the balance of risk among different types of MILSATCOM users may need to be adjusted. Three key user groups to consider for the next-generation MILSATCOM architecture are global surveillance and strike (GSS), special operations forces (SOF), and strategic forces. While these mission areas do not encompass the full range of U.S. military capabilities, they are among the highest priority missions as the military seeks to shift its focus from the past decade of major stabilization operations in Iraq and Afghanistan to the emerging A2/AD threats in the Pacific.

Improving passive defenses on satellites is a good option for all three of these mission areas to protect systems from electronic and cyber attacks. Dispersing, disaggregating, or proliferating the architecture is a good option for the GSS and strategic forces mission areas to protect systems from physical attack, although these approaches may be unaffordable unless the cost per satellite is reduced significantly. Making systems easier to replace is not a viable option for any of the mission areas because the time needed to prepare and launch a replacement system is too long for a short-duration conflict and the stock of replacements could be exhausted in a protracted conflict. Alternatives to MILSATCOM, such as commercial SATCOM, an aerial layer, terrestrial RF, and store-and-forward, are not viable as well because GSS, SOF, and strategic forces need to conduct time-sensitive operations on a global scale in contested environments.

The challenge for the future architecture is to balance costs and risks so that all MILSATCOM users have an adequate level of protection—i.e., no fronts are left undefended. Six specific recommendations are offered to meet the needs of combat forces based on the threats MILSATCOM systems are likely to face, the budget constraints likely to be imposed, and the options available:

1) The primary recommendation of this study is to transition from a two-tier MILSATCOM architecture (protected and unprotected) to a three-tier architecture. In a three-tier architecture, the highest tier of protection would be reserved for strategic users and would be largely unchanged from the current program of record for protected systems. A new middle tier of protection could be created to extend a lower level of protection to more tactical users. It would be funded by drawing resources from unprotected SATCOM programs, potentially using hosted protected payloads to expand capacity at a lower cost. The lowest tier of the architecture would be reserved for all other non-essential communications and could be acquired as a service rather than a system.
2) A second recommendation is to pivot to the Pacific in space by inviting key allies in the region such as Japan, Australia, and South Korea to be part of the middle tier of the architecture. Partner nations could share the cost of additional protected payloads and in return be given a proportionate share of the global constellation. While various political and operational issues would need to be addressed, including Asia/Pacific partners in the middle tier of the architecture would improve interoperability among the United States

and its partners and improve the capabilities of partners to operate independently in a more contested communications environment. Moreover, it would complicate the planning of potential adversaries because an attack against any protected satellites or hosted protected payloads would be an attack against all of the partner nations in the network and thus run the risk of horizontal escalation.

3) The United States should also be careful to avoid strategic cost traps in the next-generation architecture. For example, if the United States pursues a shoot-back or escort satellite capability, an adversary can impose costs by simply building more ASAT weapons and driving the U.S. military to spend disproportionately more on shoot-back capabilities. Likewise, if the United States procures additional satellites for rapid replacement in the event of an attack, an adversary could build more ASAT weapons and force the military to buy even more replacement satellites. DoD can avoid falling into a strategic cost trap by steering the competition in a more favorable direction. Instead of developing shoot-back capabilities or replacement systems, DoD could improve its capability to attack the source of ASAT threats on Earth. The United States could also raise the consequences of an attack on space systems by bringing more partners into military space programs and hosting payloads on satellites belonging to partner nations.
4) One of the lessons from the demise of the Transformational Satellite Communications System (TSAT) program is the inherent risks involved in new programs. Rather than attempting to start new programs to fill the gap left by TSAT, the Air Force should leverage current programs, namely AEHF, to build and evolve new capabilities. The temptation will be strong to reopen requirements documents and begin specifying new capabilities with each new contract award. To reduce this temptation, the staffs of existing program offices should be reduced to limit the number of people thinking of ways to change requirements. A staff reduction would also allow the contractors building the systems to reduce their overhead costs since they would not need as many people assigned to interface with program office personnel.
5) Another important way to reduce costs and risks is to use competition more appropriately. In MILSATCOM, competition can be an effective tool to drive down costs, improve performance, and incentivize innovation for products where new development is not required and more than one contractor already produces the products DoD needs, such as launch vehicles and satellite buses. For products where only one contractor currently supports DoD, however, a sole source award—while not ideal—may cost the government less overall than an artificial competition that pays a second contractor to perform redundant development work or operate a redundant production line. Ultimately, competition that is not self-sustaining by natural market forces is not healthy for industry or cost-effective for the government.
6) A final recommendation is to consolidate MILSATCOM programs, budgets, and operations under one Service. The Air Force would be the most likely candidate to assume this responsibility, since it already manages the largest share of the MILSATCOM enterprise. The other Services could transfer MILSATCOM programs, operational units, and their associated budgets to the Air Force. Consolidation would create better alignment of authorities and budgets for MILSATCOM, reduce redundancy and overhead costs across the Services, and enable the Air Force to better control the synchronization of MILSATCOM programs.

If the U.S. military is committed to a strategy of assured access in the face of A2/AD capabilities, as the 2012 Defense Strategic Guidance states, then the Department must adapt its space systems to operate in a more contested environment.[3] A day without space could quickly become a decade without space if next-generation space systems are designed for the wrong threats or acquisition programs fail due to cost overruns and delays. MILSATCOM systems provide core infrastructure services upon which other weapon systems depend, and as the space and communications domains become increasingly contested, too many tactical users continue to rely on systems with little or no protection. In a constrained budget, however, it is cost prohibitive to increase protected MILSATCOM capacity by starting new programs or continuing to conduct business as usual. For the Department to bridge the gap between the capabilities needed and the funding available, it must fundamentally rethink the next-generation MILSATCOM architecture and be willing to make some difficult trades.

[3] Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: DoD, January 2012).

INTRODUCTION

Space is no longer a sanctuary for the U.S. military. In the 1960s and 1970s, the United States and Soviet Union dominated the use of space, and a strategic détente emerged between the two space powers.[4] This détente held throughout the remainder of the Cold War, even as other nations began space programs of their own and the commercial use of space began to blossom. Since the end of the Cold War, however, the space domain has become more crowded. Today, more than 40 nations own or operate satellites, and virtually all nations depend on space-based capabilities for civilian applications, such as weather forecasting and precision navigation.[5] U.S. Space Command tracks more than 1,000 active satellites and 21,000 other man-made objects in Earth orbit, mainly debris.[6] Roughly 60 percent of active satellites are used for communications, and most of these belong to commercial operators.[7]

As the number of space-faring nations and private corporations has grown, the space domain has also become more contested. Other nations have taken note of the distinct advantages space systems provide the U.S. military and have developed capabilities to challenge the United States in space. In a highly visible demonstration of this, China successfully tested an anti-satellite (ASAT) weapon in 2007, destroying a malfunctioning weather satellite in low earth orbit (LEO).[8] Moreover, electronic attacks, cyber attacks, and attacks against the ground infrastructure used by space systems are becoming more of a concern because the technological barrier to entry is lower, attacks are less attributable, and the technology itself is more easily proliferated.

The Evolving Role of Space-Based Capabilities

As the space domain has become more crowded and contested, the way the U.S. military uses space has also evolved. During much of the Cold War, space systems focused primarily on supporting strategic missions, such as missile warning, intelligence, and nuclear command and control. Support

[4] Lt. Gen. Ellen Pawlikowski, Doug Loverro, and Col. Tom Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," *Strategic Studies Quarterly*, Spring 2012, p. 30.

[5] Union of Concerned Scientists, *Satellite Database*, available at (http://www.ucsusa.org/nuclear_weapons_and_global_security/space_weapons/technical_issues/ucs-satellite-database.html), accessed on November 20, 2012.

[6] U.S.-China Economic and Security Review Commission, *2011 Report to Congress* (Washington, D.C: Government Printing Office, November 2011), p. 218.

[7] Union of Concerned Scientists, *Satellite Database.*

[8] Shirley Kan, *China's Anti-Satellite Weapon Test* (Washington, DC: Congressional Research Service, April 23, 2007), p. 1.

for tactical missions was secondary, if not an afterthought.[9] The 1991 Gulf War, however, marked a substantial shift in the use of space-based capabilities to support forces in conventional operations. The Gulf War highlighted the fusion of space-based capabilities, such as precision navigation and timing and communications, into other weapon systems. This fusion formed a new set of capabilities some have termed the "space-enabled reconnaissance strike complex."[10]

The U.S. military now relies on space-based systems for a number of core enabling capabilities. Space systems collect images and intercept electronic signals to provide persistent intelligence, surveillance, and reconnaissance (ISR) on a global scale. The Global Positioning System (GPS) provides precision navigation and timing services for a wide range of military and civilian users. Satellites are also used for missile launch warning and weather forecasting. As Robert Butterworth, a former senior official at Air Force Space Command, has noted, "Technology has extended space progressively deeper into warfare, while potential adversaries are developing capabilities that could extend warfare into space."[11] As the military has become more dependent on space-based capabilities and the space domain has become more crowded and contested, military space systems have not evolved to keep pace with these changes.[12]

From the perspective of other nations, U.S. military space systems are weapon systems, and space is a domain of warfare that can and will be contested.

Part of the reason the United States has been slow to recognize and address the vulnerability of military space systems is the lingering debate over the militarization and weaponization of space. Because space systems, including communications satellites, are an integral part of U.S. global power projection capabilities, space is already militarized—that is, the military recognizes the value of and benefits from the use of space assets.[13] Moreover, these capabilities and the effects they produce create such a powerful advantage for the United States that military space systems are effectively weapon systems as well, even if they are not literally armed. Arguing that military space systems are not weapons is like arguing that an M-16 rifle is not a weapon but merely an enabling capability for the ammunition. Such arguments obscure the military utility of space and the attractive set of targets it presents for potential adversaries. From the perspective of other nations, U.S. military space systems are weapon systems, and space is a domain of warfare that can and will be contested.

Space systems, however, are unlike many other weapons systems because they cannot be easily matched to comparable adversary systems to determine which nation has the advantage. For example, more tanks or better tanks may create an advantage in the ground domain. But this logic does not necessarily hold true in the space domain. Military space systems are part of a global infrastructure that enables core combat capabilities, such as precision attack and global power projection. The United States can have a greater number of satellites or more capable satellites than an adversary, but that does not mean the United States has sufficient space capabilities to enable its combat forces. The value of military space systems is ultimately a function of how they contribute to fighting and winning the nation's wars. The United States does not need space capabilities greater than its potential adversaries. Rather, the nation needs reliable, resilient space capabilities that enable other weapon systems to be superior to those of an adversary. As Butterworth has noted, "what the space force needs to do is determined by how the U.S. military plans to fight the war, not by what other

[9] Pawlikowski, Loverro, and Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," p. 32.

[10] Jeff Kueter, "The War in Space Has Already Begun," *The George C. Marshall Institute Policy Outlook*, October 2006, p. 1.

[11] Robert L. Butterworth, "Space and the Joint Fight," *Strategic Forum*, National Defense University, p. 1.

[12] SATCOM refers to the use of satellite communications generally, to include military and commercial systems. MILSATCOM refers to the use of military systems in particular.

[13] Joan Johnson-Freese, *Space as a Strategic Asset* (New York: Columbia University Press, 2007), p. 2.

countries might build and launch."[14] A direct comparison of the numbers and types of satellites is therefore not a useful metric for the military competition in space. What matters are the capabilities these satellites enable for combat forces in other domains and the threats these systems face.

While the challenges of a more crowded and contested space domain are an issue for all military space systems, this study focuses on military satellite communications (MILSATCOM) to highlight how the changing threat environment affects the capabilities needed in the next-generation architecture. Like other military space systems, MILSATCOM provides core infrastructure services upon which other weapon systems depend. Combat forces at all levels are dependent on MILSATCOM for reliable, global communications in the air, sea, and land domains. Moreover, the military's use of MILSATCOM is growing exponentially. In the 1991 Gulf War, for example, the peak demand for MILSATCOM was roughly 100 megabits per second (Mbps) for a force of some 500,000 deployed troops. Eight years later in Joint Task Force Noble Anvil, the U.S. component of NATO's Operation Allied Force in Serbia, U.S. forces consumed some 250 Mbps of satellite bandwidth. By the start of Operation Iraqi Freedom in 2003, MILSATCOM demand grew to 2,400 Mbps for a deployed force less than half the size of the force deployed in the first Gulf War.[15]

The United States does not need space capabilities greater than its potential adversaries. Rather, the nation needs reliable, resilient space capabilities that enable other weapon systems to be superior to those of an adversary.

The Current MILSATCOM Architecture

The current MILSATCOM architecture consists of three types of systems operated by the military: wideband, narrowband, and protected. Wideband systems provide high data rate communications links (up to and beyond 274 Mbps) for data and video.[16] The military currently operates two primary constellations of wideband satellites: the legacy Defense Satellite Communications System (DSCS) operating in X-band and the newer Wideband Global SATCOM (WGS) system operating in both X-band and Ka-band. The military also leases transponders on commercial wideband satellites, such as Intelsat, for additional wideband capacity beyond what DSCS and WGS provide. By some estimates, up to 80 percent of DoD's SATCOM needs have been met using commercial systems.[17]

Narrowband systems provide voice and low data rate (up to 384 Kbps) communications for mobile users in the Ultra High Frequency (UHF) band.[18] The primary military system currently used for narrowband communications is the legacy UHF Follow-On (UFO) constellation. The first satellite of the next generation narrowband constellation, the Mobile User Objective System (MUOS), was launched in 2012. An additional four MUOS satellites are planned, including one on-orbit spare. The military also leases commercial narrowband services from companies such as Iridium.

Protected MILSATCOM systems provide assured, survivable communications that are difficult to detect, intercept, and jam and that can overcome some of the atmospheric effects generated by a nuclear blast. Protected systems provide strategic forces with the ability to communicate in the event of a catastrophic attack and give tactical users a highly reliable and secure means of communication. The military currently operates two protected constellations in the Extremely High Frequency (EHF) band. The legacy Milstar constellation provides data rates up to 1.5 Mbps, and the recently launched

[14] Butterworth, "Space and the Joint Fight," p. 2.

[15] Patrick Rayermann, "Exploiting Commercial SATCOM: A Better Way," *Parameters*, Winter 2003-2004, pp. 54-66.

[16] Jose Torres, *The HDR-RF Test Waveform: An Innovative Risk Reduction Product for FPGA-Based SATCOM Modems* (Bedford, MA: IEEE, 2008), pp. 1-6.

[17] Barry Rosenberg, "DOD's reliance on commercial satellites hits new zenith," *Defense Systems*, February 25, 2010, available at (http://www.defensesystems.com/Articles/2010/03/11/Cover-story-The-Satcom-Challenge.aspx), accessed on July 19, 2013.

[18] John Oetting and Tao Jen, "The Mobile User Objective System," *Johns Hopkins APL Technical Digest*, Vol. 30, No. 2, 2011, p. 103.

Advanced EHF (AEHF) satellites provide data rates up to 8.2 Mbps.[19] These constellations are supplemented by the Interim Polar System (IPS), a two-satellite constellation in polar orbit that provides continuous coverage above 65 degrees latitude north.[20] To lessen their reliance on ground stations, which can be vulnerable to attack, the Milstar and AEHF constellations use inter-satellite links to pass data directly from one satellite to another without going through a ground station.

The MILSATCOM architecture also includes the control and terminal segments. The control segment consists of ground stations and the supporting infrastructure that control the operation of both the satellite bus (i.e., maintaining the proper orbit) and the payload (i.e., coordinating and allocating satellite resources to different users). The terminal segment includes the end user devices (i.e., radios) used to communicate over the satellites. Terminals can be mobile or fixed and can be integrated into other weapon systems. Terminals, while less expensive per unit, are procured in much larger quantities, making them a substantial component of the overall system cost. The UFO system, for example, has more than 67,000 terminals (and more than 50 different types of terminals) currently in use.[21]

A Strategic Choice in Space

MILSATCOM is now at a fork in the road. The Transformation Satellite Communications System (TSAT) was intended to be the future architecture for both wideband and protected systems. Following the TSAT program’s termination in 2009, no new MILSATCOM space programs have been initiated. The current plan is to continue buying additional WGS, AEHF, and MUOS satellites as needed to keep the existing constellations viable while the military reexamines its plans for the future. While the military considers its options, the demand for SATCOM continues to grow and the vulnerabilities of the current architecture remain exposed. Because of the long lead times in developing and fielding MILSATCOM systems, the decisions the military makes in the next few years—whether to continue buying existing systems or to evolve the architecture in a new direction—will define the capabilities available to combat forces for decades to come.

After terminating the TSAT program, then Secretary of Defense Robert Gates urged the military to “shift away from the 99-percent exquisite service-centric platforms,” and instead pursue “the 80-percent solution, the multi-service solution that can be produced on time, on budget and in significant numbers.”[22] While the threats to space systems are increasing, the next-generation MILSATCOM architecture cannot afford to be the “99-percent” exquisite solution that TSAT aimed to be. The “80-percent” solution, however, should not be interpreted as meaning 80 percent of the reliability or capacity current systems provide. Rather, the “80-percent” solution should be one that makes reasonable and informed trades among cost, schedule, and performance to deliver the best value for combat forces.

The U.S. military faces an important strategic choice in space: should it prioritize the capabilities required to counter the threats MILSATCOM systems face in a more contested space environment? In a constrained budget, this will necessarily require sacrifices in other areas, such as overall

[19] U.S. Air Force, “Advanced Extremely High Frequency Factsheet,” available at http://www.losangeles.af.mil/library/factsheets/factsheet_print.asp?fsID=5319&page=1, accessed on July 9, 2013.

[20] Satellites operating in geostationary orbit cannot provide coverage beyond roughly 65 degrees latitude north and south because the look angle from the ground to the satellite becomes too shallow.

[21] U.S. Navy Space and Naval Warfare Systems Command, “Mobile User Objective System (MUOS) Fact Sheet,” December 2011, available at http://spaceflightnow.com/atlas/av030/muos_factsheet.pdf, accessed on November 20, 2012.

[22] Robert M. Gates, “Remarks at the Army War College,” Carlisle, PA, April 16, 2009.

MILSATCOM capacity. This report explores the challenges and opportunities facing DoD if it chooses to design the next-generation MILSATCOM architecture for a more contested space environment. The first chapter examines the physical, electronic, and cyber threats MILSATCOM systems face. The second chapter explores the programmatic threats these systems face in a more constrained funding environment. The third chapter identifies options (technical, programmatic, and operational) to address the twin challenges of a more contested space domain and more constrained funding environment. The fourth chapter evaluates these options using three example mission areas: global surveillance and strike, special operations, and strategic forces. The paper concludes by making recommendations for the future MILSATCOM architecture in light of the strategic choices facing the U.S. military and how it prepares to operate in the future.

CHAPTER 1: THREATS TO SPACE SYSTEMS

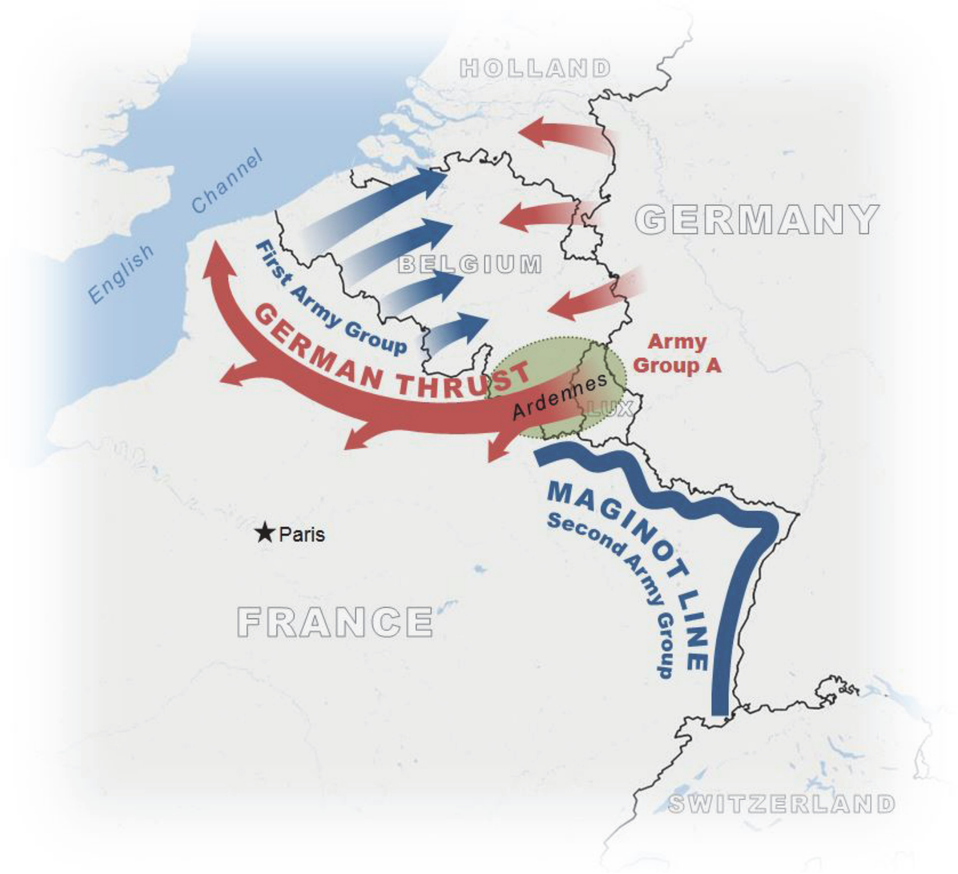
A Maginot Line in Space

In January 1930, French Minister of War André Maginot rose to speak before the Chamber of Deputies. “Whatever form a new war may take, whatever part is taken in it by aviation, by gas, by the different destructive processes of modern warfare, there is one imperious necessity, and that is to prevent the violation of our territory by enemy armies.”[23] Maginot convinced his compatriots to embark on an ambitious venture to build a network of fortifications along the French-German border to prevent a future invasion. The wall of fortifications he conceived—what became known as the Maginot Line—was a remarkable engineering feat for its time. The main units of fortification, *ouvrages*, were buried some 100 feet below hills and ridgelines, were connected by an underground trolley system for transporting troops and supplies, and were designed to be self-sufficient for up to three months. Fearful of the chemical weapons used in World War I, the French even designed the *ouvrages* with an air filtration system and a slight overpressure to protect troops from gas attacks.[24]

The Maginot line was a source of pride and technological accomplishment, and the line did what it was designed to do—repel a direct German invasion through the Alsace and Lorraine regions. Nevertheless, German forces rolled into Paris in 1940 with relative ease. The German military, recognizing that the French line of fortifications along its border would be difficult to penetrate, sidestepped the Maginot Line by invading through Belgium and Luxembourg. As Rudolph Chelminski noted, the Maginot Line’s “shortcomings derived not from failures of execution but from the inability of its proponents to anticipate how much warfare would change in a mere two decades.”[25] The Maginot Line serves as a lasting example of how a military can be incredibly prepared for one type of threat only to find itself vulnerable to a range of other threats.

[23] Rudolph Chelminski, “The Maginot Line,” *Smithsonian*, June 1997, p. 90.
[24] Ibid., p. 91.
[25] Ibid., p. 90.

FIGURE 1: THE MAGINOT LINE AND THE GERMAN INVASION OF FRANCE IN WORLD WAR II



The United States is now at risk of building its own Maginot Line in space. For much of the Cold War, space systems were primarily designed for strategic conflict. The extension of war into the space domain was viewed as unlikely or, at worst, a prelude to a full-scale nuclear war between the United States and Soviet Union. From this perspective, the key type of protection needed for space systems—and MILSATCOM systems in particular—was nuclear survivability.[26] Moreover, not all MILSATCOM systems needed to be nuclear survivable—only those used for nuclear command and control.

The United States is now at risk of building its own Maginot Line in space.

An implicit assumption was that in conventional conflicts, deterrence would hold and space systems would not be attacked. One of the consequences of this assumption in the post-Cold War era is that U.S. space systems, and MILSATCOM systems in particular, have critical vulnerabilities in conventional conflicts. Potential adversaries do not have symmetric vulnerabilities, since no other nation's military is as dependent on space as the U.S. military. This asymmetry makes traditional deterrence in space a difficult proposition. Just as the Germans violated international norms by attacking France through Belgium and Luxembourg, future adversaries could exploit U.S. vulnerabilities by violating international norms and launching an attack in the space domain.

[26] Pawlikowski, Loverro, and Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," pp. 30-31.

Because of the U.S. military's dependence on space-based capabilities for global power projection, counter-space operations may figure prominently in an adversary's efforts to deny the U.S. military freedom of access to areas of strategic importance. Anti-access, area denial (A2/AD) operations are designed to restrict the ability of U.S. forces to project power in a region. The Defense Department noted in a 2013 report to Congress on military and security developments in China that the People's Liberation Army (PLA) is believed to be developing counter-space capabilities that "would serve a key role in enabling A2/AD operations." The report goes on to assert (without identifying specific sources) that:

> PLA writings emphasize the necessity of "destroying, damaging, and interfering with the enemy's reconnaissance...and communications satellites," suggesting that such systems, as well as navigation and early warning satellites, could be among the targets of attacks designed to "blind and deafen the enemy." The same PLA analysis of U.S. and coalition military operations also states that "destroying or capturing satellites and other sensors…will deprive an opponent of initiative on the battlefield and [make it difficult] for them to bring their precision guided weapons into full play."[27]

During the Cold War, it made sense to concentrate MILSATCOM capabilities in a relatively small number of systems due to the high cost of launch and the limited threats to satellites short of a nuclear conflict. This legacy, however, carries through to the constellations currently being launched and does not account for the increasing importance of counter-space operations in an A2/AD environment. This chapter explores the vulnerabilities of MILSATCOM systems, grouping them into three categories of threats: physical attack, electronic attack, and cyber attack.

Physical Attack

MILSATCOM satellites are vulnerable to several different forms of physical attack. Kinetic attacks can take the form of anti-satellite weapons designed to destroy a target satellite by striking it or detonating a warhead in its vicinity. In 2007, China conducted a successful test of a direct-ascent anti-satellite weapon against one of its own satellites in LEO.[28] The United States followed suit in 2008 by launching an SM-3 missile to intercept and destroy (at a much lower altitude) a disabled U.S. military satellite that was projected to re-enter the atmosphere within days.[29] Nuclear weapons can also be used as kinetic weapons against satellites by detonating them in space or at a high altitude to physically destroy a satellite or damage its electronics. Satellites are also vulnerable to co-orbital threats whereby a satellite already in orbit can be deliberately maneuvered into another satellite. In addition to the United States, India, Russia, China, and Japan all have the requisite technology to build and launch small satellites for this purpose and other nations could join their ranks.[30] Space

[27] Office of the Secretary of Defense, *Annual Report to Congress: Military and Security Developments Involving the People's Republic of China 2013* (Washington, DC: Department of Defense, 2013), p. 33.
[28] Kan, *China's Anti-Satellite Weapon Test*, p. 1.
[29] Department of Defense, "DoD News Briefing with Gen. Cartwright from the Pentagon," News Transcript, February 21, 2008.
[30] Brian Garino and Jane Gibson, "Space System Threats," *AU-18 Space Primer* (Maxwell Air Force Base, Alabama: Air University Press, September 2009), p. 277.

mines can also be used to quietly trail a target satellite and detonate a small charge when commanded.[31]

Kinetic attacks tend to have catastrophic effects on the systems they target by totally and permanently disabling them. Moreover, kinetic attacks create space debris that can affect satellites belonging to nations or companies not directly involved in the conflict. The Chinese anti-satellite weapon test in 2007, for example, produced 14 percent of the 22,000 manmade objects currently being tracked by U.S. Space Command—roughly 3,000 pieces of space debris large enough to be tracked.[32] A nuclear attack in space would have broad effects beyond just the satellite (or satellites) being targeted due to the tremendous amount of radiation released.[33] Overall, kinetic weapons tend to be attributable, their effects are irreversible, and the risk of collateral damage is high. Therefore, using these weapons in space would likely be viewed as a significant escalation in a conflict.

The Chinese anti-satellite weapon test in 2007 produced 14 percent of the 22,000 manmade objects currently being tracked by U.S. Space Command.

Non-kinetic forms of physical attack, however, can temporarily or partially degrade a satellite with less risk of debris. Directed energy weapons, such as lasers and high-powered microwave systems, can target space systems more quickly (within seconds) and create effects that may not be immediately evident. A high-powered laser, for example, can be used to damage critical satellite components, such as solar arrays and sensors. But this requires a megawatt-class laser with high beam quality and advanced stability and pointing—technology that is costly and not widely available.[34] In September 2006, however, it was reported that China illuminated U.S. satellites using ground-based lasers in an apparent attempt to "blind" the satellites, an indication that this technology, while advanced, is not out of reach.[35]

Satellites are not the only segment of the MILSATCOM architecture at risk of physical attack. Rather than attacking the satellites on-orbit, an adversary could achieve similar effects by attacking the ground stations that support them. The ground segment is perhaps more vulnerable to attack because it is often highly visible, located in a foreign country, and a relatively soft target. For example, teleport sites (shown in Figure 2) serve as critical data relays for MILSATCOM users. For wideband systems like WGS, data from a forward-deployed user is often sent via satellite to a teleport where it is relayed through another satellite or through fiber to users around the world. Users of the narrowband MUOS system are even more dependent on ground stations because all communications must pass through the ground control center, even if both users are under the footprint of the same satellite.[36] Protected MILSATCOM systems like Milstar and AEHF are less dependent on ground stations because they have inter-satellite links. These links enable them to transmit data between satellites from one theater to another without passing through an intermediary ground station.

[31] U.S. Congress, Office of Technology Assessment, *Anti-Satellite Weapons, Countermeasures, and Arms Control* (Washington, D.C.: Government Printing Office, September 1985), p. 7.

[32] U.S.-China Economic and Security Review Commission, *2011 Report to Congress*, p. 218.

[33] In 1962, the United States conducted a test of a 1.4 megaton nuclear warhead at an altitude of 248 miles. The burst of radiation from this experiment inadvertently (and permanently) damaged at least three U.S. and British satellites. See Steven James Lambakis, *On the Edge of Earth: The Future of American Space Power* (Lexington, KY: University Press of Kentucky, 2001), p. 123.

[34] Garino and Gibson, "Space System Threats," p. 277.

[35] Vago Muradian, "China Tried to Blind U.S. Sats with Laser," *Defense News*, September 25, 2006.

[36] This method of connecting users, known as an "M-hop" on MUOS, simplifies the design of the satellite payload because the switching is done on the ground. It also doubles the time delay users experience. Since each roundtrip to geostationary orbit takes roughly ¼ second, the time delay for MUOS users is ½ second.

FIGURE 2: THE WAHIAWA TELEPORT SITE IN HAWAII

Ground stations are vulnerable to direct physical attack by a number of means. Guided rockets, artillery, mortars, and missiles (G-RAMM) could be used to attack ground stations from beyond visible range, while rocket-propelled grenades and small arms fire could be used to disable antennas at close range. Ground stations can also be disrupted by attacking the electrical power grid, water lines, and the high-capacity communications lines that support them. While attacks against ground stations could have large implications if the communications links that pass through them are severed, the effects would not be permanent. Unlike satellites, which require years to build and cannot be repaired once they are launched, ground stations can be repaired in a matter of days, weeks, or months depending on the level of damage incurred.

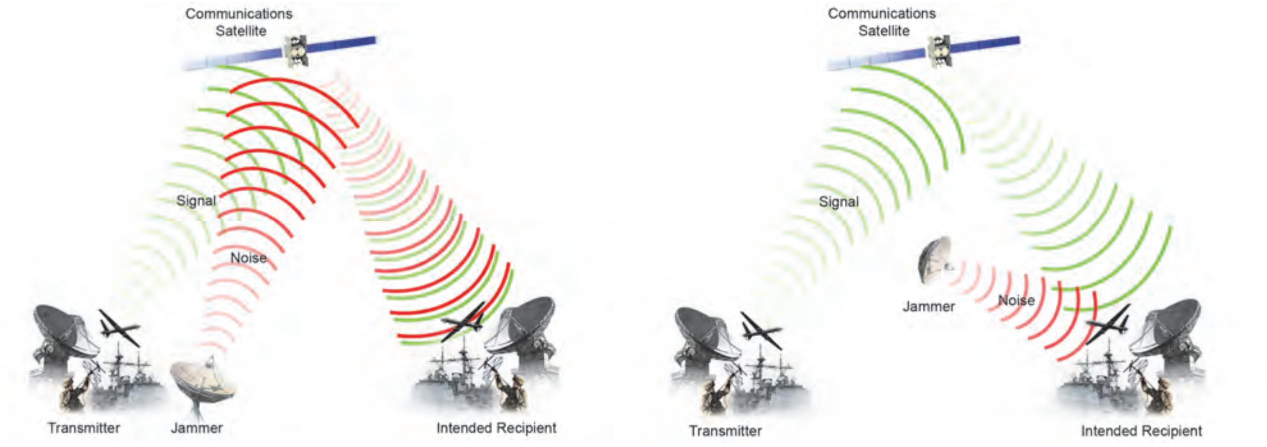
Electronic Attack

Electronic attack is the use of electromagnetic energy to interfere with communications, a process commonly known as jamming. A jammer must operate in the same frequency band and within the field of view of the antenna it is targeting. Unlike physical attacks, jamming is reversible—once the jammer is disengaged, communications can be restored. An uplink jammer is used to jam signals being received by a satellite by creating enough noise that the satellite cannot distinguish between the intended signal and the noise. Uplink jamming of the control link can prevent a satellite from receiving commands from operators on the ground. Uplink jamming can also target user data being transmitted over the satellite by interfering with the uplink of data to the satellite, which corrupts the data for all recipients in the downlink. An uplink jammer must be roughly as powerful as the signal it is attempting to jam, and it must be within the footprint of the satellite antenna it is targeting.[37] Neither of these factors is particularly challenging, especially considering that the footprint of a satellite antenna typically ranges from a few hundred miles to more than 1,000 miles in diameter.

[37] Garino and Gibson, “Space System Threats,” pp. 274-275.

While an uplink jammer can have broad effects across many users of a satellite, a downlink jammer has more localized effects. Downlink jammers target ground users of a satellite by creating noise in the same frequency as the downlink signal from the satellite. A downlink jammer only needs to be as powerful as the signal being received on the ground, but it must also be within the field of view of the receiving terminal's antenna, which limits the number of terminals that can be affected by a single jammer. Since many ground terminals use directional antennas pointed at the sky, a downlink jammer will be more effective if it is located higher than the terminal it is attempting to jam. This limitation can be overcome by employing a downlink jammer on an airborne platform, which positions the jammer between the terminal and the satellite and allows the jammer to cover more terminals over a wider area.[38] Ground terminals with smaller antennas (disadvantaged terminals) or omnidirectional antennas have a wider field of view and thus are more susceptible to downlink jamming.

FIGURE 3: EXAMPLES OF UPLINK AND DOWNLINK JAMMING



Uplink Jamming

Downlink Jamming

In 2006 testimony before the House Armed Services Committee Strategic Forces Subcommittee, Lieutenant General Robert Kehler, then Deputy Commander of U.S. Strategic Command, noted that the U.S. military has already experienced jamming on commercial systems it leases.[39] For example, analysis of commercial SATCOM links over a 16-month period during Operation Iraqi Freedom found 50 documented instances of interference with military communications over commercial SATCOM. Of these 50 instances, 29 were determined to be unintentional "self-jamming," such as a terminal operating on the wrong frequency or an improperly configured terminal. Of the 21 instances in which the cause could not be determined, five stand out as potential instances of hostile jamming. All five suspected cases of jamming occurred in the uplink signal, originated in the Southwest Asia region, and involved a transmitter using a continuous wave carrier signal. The use of a continuous wave carrier signal is particularly suspicious because it is unlikely to be an accidental transmission by a friendly user. Moreover, the continuous wave carrier signals used in these instances varied their

[38] Ibid., p. 275.

[39] Lt. Gen. Robert Kehler, "Statement before the House Strategic Forces Subcommittee, Committee on Armed Services," June 21, 2006.

center frequency within a band—what is known as a "sweeper" signal in jamming because it creates intermittent outages across a wider piece of the spectrum.[40]

As this example demonstrates, jamming can be difficult to detect and distinguish from accidental interference. It can also be difficult to attribute a particular instance of jamming to a particular source. Even when attribution is possible, neutralizing the source of jamming can present a host of challenges. For example, in 2003 Voice of America television broadcasts into Iran were reportedly jammed by a source emanating from within Cuba. Cuba is within the antenna footprint of the Loral Skynet satellite used for these broadcasts and, thus, is an ideal location for an uplink jammer. The source of jamming was determined to be near Havana.[41] While the jamming could have been conducted by the Cuban government, it is also possible Cuba was not aware of the jamming from within its own borders. Regardless of what the Cuban government knew, they had few incentives to cooperate with the United States to eliminate the source of the jamming.

Cyber Attack

MILSATCOM systems are also vulnerable to cyber attacks, which can be used to intercept data, corrupt data, or take control of systems for malicious purposes. Unlike electronic attacks, which interfere with the transmission of data in the electromagnetic spectrum, cyber attacks target the data itself and the systems that use this data. Any data interface in the system is a potential intrusion point, including the antennas on both the satellites and terminals and the landlines connecting ground stations to terrestrial networks. Cyber attacks can target satellites, ground control stations, and terminals. A successful attack in any one of these segments could be used to launch additional attacks on the other segments. The effects of a cyber attack on MILSATCOM systems could range from local disruptions (i.e., causing a single terminal to go offline) to widespread disruptions and potentially the permanent loss of a satellite. Attribution for a cyber attack can be difficult, if not impossible, because attackers can use a variety of methods to conceal their identity, such as using a hijacked computer to launch an attack.

A cyber attack could be used for many purposes, including: detection and monitoring of communications; interception and exploitation of data; data corruption and spoofing; and seizing command and control of key systems. For example, an adversary could gain access to a system to monitor the flow of data and discern sensitive operational details, such as the location of users and which users are communicating with one another. An attack could also be used to covertly intercept communications and exploit that information for operational advantage. A more sophisticated attack could intentionally corrupt data as it flows through a communications system to fool the end user of that data or cause all users to question the integrity of the system. A more damaging form of cyber attack involves taking control of a system. If an adversary were able to take control of a satellite, for example, it could shut down all communications, move the satellite to a different orbit, or even destroy the satellite by expending its fuel supply or damaging its electronics. Moreover, it may be difficult for controllers to know what caused a satellite to lose control, since accidental malfunctions occur occasionally.

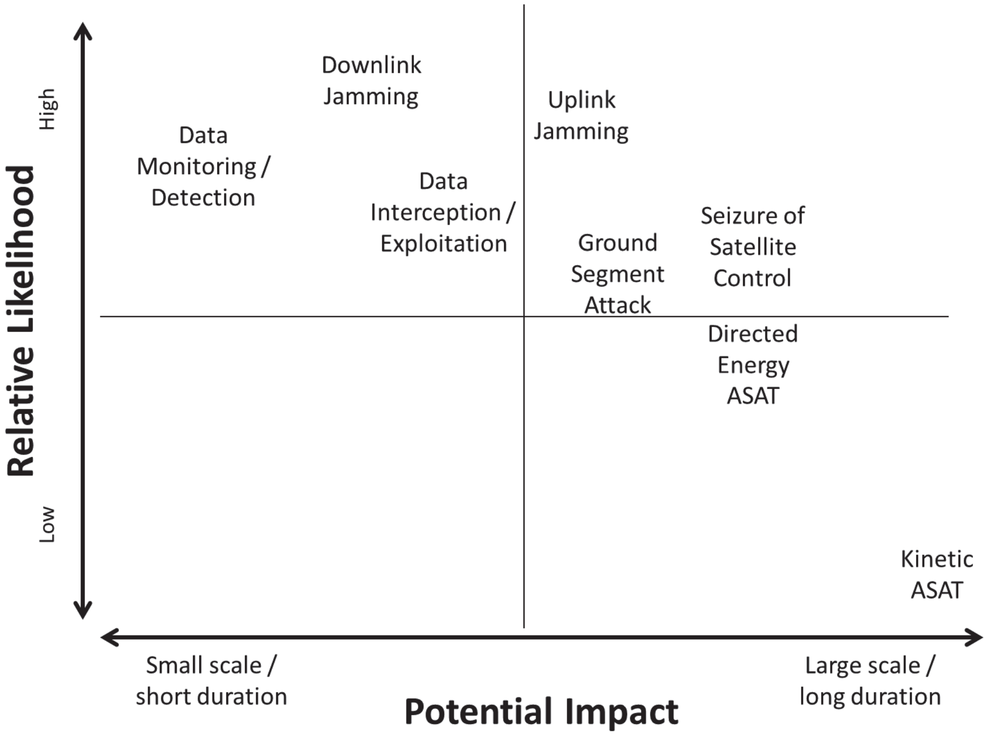
[40] Hank Rausch, "Jamming Commercial Satellite Communications During Wartime: An Empirical Study," *Proceedings of the Fourth IEEE International Workshop on Information Assurance,* April 2006.
[41] "U.S. Accuses Cuba of Jamming Broadcasts To Iran," PBS News Hour Online Report, July 17, 2003, available at http://www.pbs.org/newshour/media/media_watch/july-dec03/jamming_07-17.html, accessed on December 12, 2012.

Like physical and electronic attacks, cyber attacks in the space domain are already occurring. In 2009, it was discovered that insurgents in Iraq and Afghanistan had been intercepting video feeds from U.S. Predator unmanned surveillance aircraft after copies of the videos were found on insurgents' laptops. Because the video feeds were transmitted without any protection or encryption, insurgents were able to use commercially available software to intercept the data.[42] In its 2011 report to Congress, the U.S.-China Economic and Security Review Commission cited four instances in 2007 and 2008 in which cyber attacks were used against two U.S. government satellites in an apparent attempt to target their command and control systems. The most successful of these attacks was against a National Aeronautics and Space Administration (NASA) satellite used for earth observation, known as Terra EOS. In this attack the commission notes that, "The responsible party achieved all steps required to command the satellite but did not issue commands."[43]

Comparison of Threats

While all of the vulnerabilities listed above should be considered when designing the next generation MILSATCOM architecture, they are not necessarily equal in priority. The relative priority of these vulnerabilities should be determined based on their potential impact and likelihood of occurrence, as shown in Figure 4. Vulnerabilities that have both a greater potential impact on military operations and are more likely to be exploited by an adversary (shown in the upper right quadrant of the chart) should be afforded the highest priority.

FIGURE 4: RISK MATRIX FOR MILSATCOM VULNERABILITIES



[42] Siobhan Gorman, Yochi J. Dreazen, and August Cole, "Insurgents Hack U.S. Drones," *The Wall Street Journal*, December 17, 2009.
[43] U.S.-China Economic and Security Review Commission, *2011 Report to Congress*, p. 216.

The key metrics for weighing the relative impact of threats are the scope of the disruption and the duration of disruption. For example, a kinetic anti-satellite weapon would cause widespread and long-lasting disruptions because it would destroy a satellite that takes years to replace and the orbital debris generated from the attack could affect many other space systems for decades to come. Uplink jamming has relatively less impact because it can affect all users of a satellite over a broad area but is temporary and does not permanently harm the system. Downlink jamming is also reversible, and has a more limited impact than uplink jamming because it only affects users within line of sight of the jammer.

The key metrics for understanding the relative likelihood of a particular vulnerability being exploited are the resources required to launch an attack (i.e., how difficult it is) and the likelihood of attribution. Methods of attack that require complex or expensive technology will be available to fewer adversaries and thus are less likely to be used than attacks that use commonly available technology. It is also reasonable to assume that methods of attack that can be launched anonymously with little risk of retaliation are more likely to be used than attacks where the source can be readily identified. Uplink and downlink jamming, for example, are both forms of attack that are relatively more likely than others because they can be undertaken using off-the-shelf technology and, as the examples cited previously demonstrate, detection and attribution of intermittent jamming can be difficult. A kinetic anti-satellite weapon, however, is relatively less likely because it requires more advanced technology and the launch site can be identified by U.S. missile warning satellites, creating the potential for retaliation.

A key limitation of the approach shown in Figure 4 is that the impact and likelihood of threats is fundamentally a subjective assessment and worthy of periodic reconsideration. Nevertheless, some ranking of relative priority among these vulnerabilities is necessary to understand which are the most important to address.

CHAPTER 2: FUNDING CONSTRAINTS

A common maxim in defense planning is “the enemy gets a vote,” meaning an adversary’s decisions can affect your plans. This maxim could be extended to include Congress and the acquisition system itself because MILSATCOM systems are arguably just as vulnerable to cost overruns, funding instability, and other programmatic factors that can prevent a satellite from ever getting off the ground as they are to physical, electronic, and cyber attacks. As the military begins to plan for the next-generation MILSATCOM architecture, affordability is a major concern. This chapter describes the overall budget environment for defense, the key cost drivers for MILSATCOM systems, and the programmatic threats with which these systems must contend.

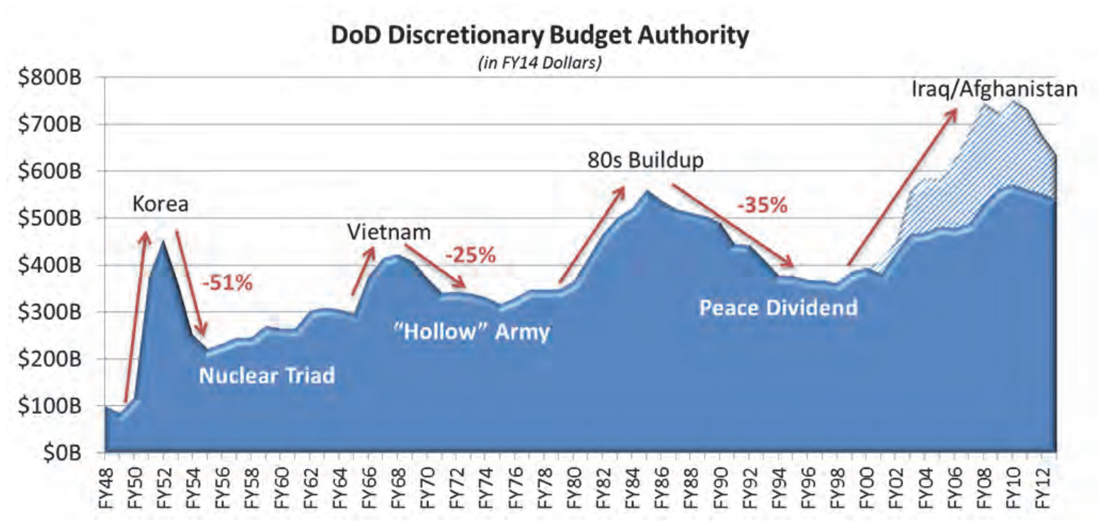
MILSATCOM systems are arguably just as vulnerable to cost overruns, funding instability, and other programmatic factors that can prevent a satellite from ever getting off the ground as they are to physical, electronic, and cyber attacks.

Budget Environment

Throughout American history, the defense budget has risen and fallen in irregular cycles in response to changes in the economic and security environment. The defense budget appears to be entering the downturn phase of one of these cycles, which could extend through the rest of the decade. The overall DoD budget grew 108 percent in real terms from Fiscal Year (FY) 1998 to FY 2010, or 59 percent excluding the cost of the wars in Iraq and Afghanistan. As part of a broader deficit reduction agreement, the Budget Control Act (BCA) of 2011 set budget caps for defense through FY 2021. These caps were automatically reduced in November 2011 when the so-called Super Committee failed to find additional deficit reduction as required under the BCA. Under the revised budget caps, the base DoD budget in FY 2021 will be 13 percent less in real terms than its peak in FY 2010—or 33 percent lower if the anticipated reduction in war funding is included.[44]

[44] This assumes war-related funding will decline to near zero on or before FY 2021.

FIGURE 5: DEFENSE BUDGET CYCLES



This level of decline is roughly in line with previous drawdowns. At the end of the Korean War, defense spending fell by 51 percent in real terms from peak to trough (FY 1952 to FY 1955). Defense spending during the Vietnam War peaked in FY 1968 and fell 25 percent by FY 1975. Likewise, defense spending during the 1980s buildup fell 35 percent from its peak in FY 1985 to its low point in FY 1998. What is notable about the downturn component of previous cycles is that each involved a significant reduction in the size of the military. For example, end strength fell from 3.6 million to 2.5 million following the Korean War, from 3.5 million to 2.0 million at the end of the Vietnam War, and from 2.2 million to 1.4 million following the 1980s buildup.

Rather than getting larger and more expensive during the most recent buildup, the military simply became more expensive.

This downturn, however, is likely to be different because this buildup was unlike previous buildups. The increase in defense spending over the past decade did not involve a significant buildup of military forces—end strength fluctuated between 1.45 million to 1.51 million. The size of the military is essentially the same today as it was when the current buildup began, making it difficult for the Defense Department to reap savings of the order experienced in previous drawdowns simply by reducing the size of the force.

Rather than getting larger and more expensive during the most recent buildup, the military simply became more expensive. For example, from FY 2001 to FY 2012, compensation costs per active duty service member grew 56 percent, adjusting for inflation, or 4.1 percent annually.[45] As a result, the share of the base DoD budget devoted to military personnel-related costs grew from 30 percent in FY 2001 to 34 percent in FY 2012. Even if military personnel costs return to their historical norm of 2.6 percent real annual growth, by FY 2021 they will consume 46 percent of the DoD budget under the funding level currently prescribed in law.[46] The cost of peacetime operations and maintenance per active duty service member also increased, growing 34 percent in real terms from FY 2001, or 2.7

[45] Military personnel-related costs for active duty service members includes all Military Personnel funding not designated as war-related, minus accounts marked for Guard and Reserve personnel, plus the Defense Health Program account from Operations and Maintenance (O&M).
[46] This assumes a $563 billion DoD budget in FY 2021, consistent with the budget caps imposed by the Budget Control Act of 2011. It also assumes active duty end strength remains at 1.4 million.

percent annually.[47] If peacetime operations and maintenance costs return to their historical norm of 2.5 percent real annual growth, by FY 2021 they will consume 40 percent of the DoD budget.[48] Under these scenarios, only 14 percent of the budget would remain for procurement, research, development, test and evaluation, military construction, and family housing. Currently, DoD allocates 36 percent of its budget for these accounts. In such a budget environment, MILSATCOM programs will be forced to compete not only with other programs in a much smaller acquisition budget but also with other priorities outside of acquisitions, such as force structure, readiness, and military compensation.

While adapting to a more contested threat environment should be a priority for the next-generation MILSATCOM architecture, affordability must also be a priority. The challenge is to improve protection against the most likely threats without driving up costs and making MILSATCOM systems unaffordable. An important first step is to understand the key cost drivers for the MILSATCOM space, control, and terminal segments.

Key Cost Drivers

Space Segment

The main cost components of the space segment are the satellites, including the satellite bus and payload, and the launch vehicles used to orbit them. The cost of the satellites varies significantly depending on the type of system. Table 1 shows the current estimate of the average unit cost for AEHF, WGS, and MUOS satellites, including all recurring and non-recurring costs. While the satellites are similar in size, their costs vary by nearly a factor of five. Protected satellites, like AEHF, are more expensive because the satellite bus and payload are more complex and have many unique military requirements. For example, while the AEHF bus is based on Lockheed Martin's commercially available A2100 family of buses, it must be nuclear hardened to meet the requirements of strategic users. In contrast, the WGS satellite uses Boeing's 702HP commercial satellite bus with relatively few modifications, which allows the program to leverage more commercially developed technologies and reduce non-recurring development costs. For all three satellites, the payloads are largely unique to the U.S. military due to the frequency bands in which they operate, the waveforms they employ, and other military-specific requirements.

TABLE 1: COSTS FOR CURRENT GENERATION MILSATCOM SYSTEMS

Constellation	*Satellite Mass*	*Satellite Bus*	*Average Total Cost per Satellite (in billions of FY13 dollars)*[49]
AEHF	6,168 kg	Lockheed A2100M	$2.45
MUOS	6,740 kg	Lockheed A2100M	$1.22
WGS	5,990 kg	Boeing 702HP	$0.51

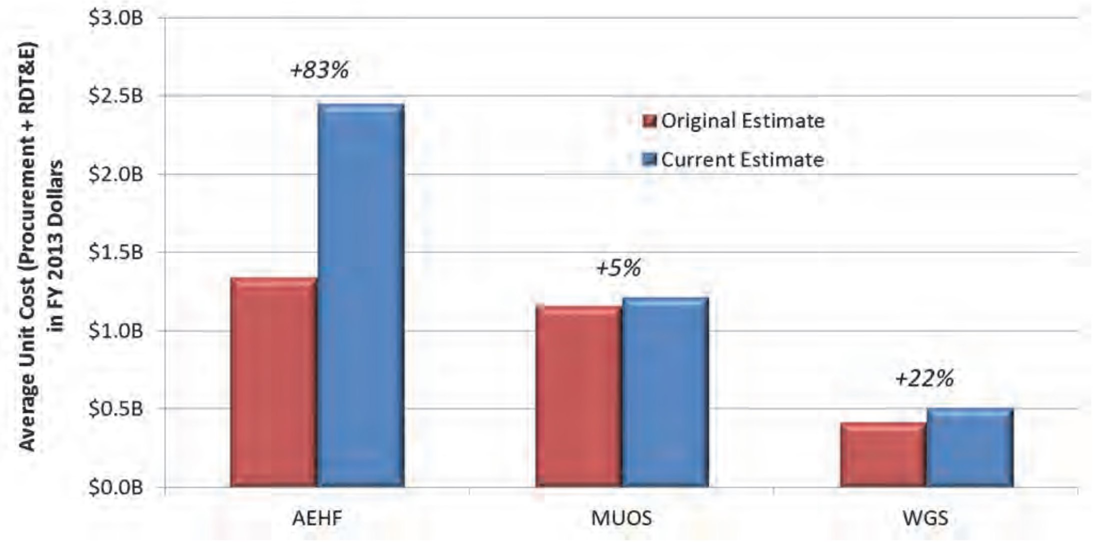
[47] Peacetime operations and maintenance costs include all O&M funding not designated as war-related minus the Defense Health Program.

[48] This assumes a $563 billion DoD budget in FY 2021, consistent with the budget caps imposed by the Budget Control Act of 2011. It also assumes active duty end strength remains at 1.4 million.

[49] Data derived from DoD, *Selected Acquisition Report Summary Tables* (Washington, DC: DoD, December 31, 2011), using the current estimate for the total program cost converted to FY 2013 dollars divided by the total number of satellites planned.

Cost overruns have been a significant issue for MILSATCOM satellites over the past decade. All three systems currently in production have exceeded original cost estimates, as shown in Figure 6. AEHF in particular has been plagued by cost overruns—83 percent over its original baseline—due to significant changes in the number of satellites planned. The program originally planned to field five satellites but was reduced to three following the start of the TSAT program. As the TSAT program encountered delays, the AEHF program reverted to five satellites. However, the elapsed time between these decisions created a break in production for the contractor, which drove up the cost of the fourth satellite to more than double that of the third satellite, triggering a Nunn-McCurdy breach.[50] The WGS program also experienced a Nunn-McCurdy breach due to a break in production, with Block II (satellites 4 to 6) costing roughly 50 percent more than Block I (satellites 1 to 3). Moreover, Block IIf (satellites 7 and 8) cost 50 percent more than Block II satellites.[51]

FIGURE 6: COMPARISON OF ORIGINAL VERSUS CURRENT COST ESTIMATES[52]



For the current generation of MILSATCOM systems, the key cost drivers for the satellites appear to be program instability (leading to breaks in production) and unique military requirements on the satellite bus and payload. International partners can, in principle, help improve program stability by broadening the set of stakeholders in a program. In addition to offsetting some of the costs, including international partners has the added advantage of improving interoperability between U.S. and partner forces. Canada, the Netherlands, and the United Kingdom are all partners in AEHF, and collectively they have contributed $270.5 million to the program.[53] Australia joined the WGS program in 2007, providing $927 million for the sixth satellite and associated ground equipment in exchange for

[50] Government Accountability Office, *Space Acquisitions: DOD Faces Substantial Challenges in Developing New Space Systems* (Washington, DC: Government Printing Office, May 20, 2009) p. 6.

[51] Irv Blickstein, et. al, *Root Cause Analysis of Nunn-McCurdy Breaches*, Volume 1 (Arlington, VA: RAND, 2011), p. 74.

[52] Data derived from multiple DoD Selected Acquisition Report Summary Tables, available at http://www.acq.osd.mil/ara/am/sar/, accessed on February 6, 2013.

[53] Department of Defense, *Selected Acquisition Report: AEHF* (Washington, DC: DoD, December 31, 2011), p. 4.

roughly one satellite's worth of bandwidth across the constellation.[54] The inclusion of Australia in the WGS program is notable because it may have prevented a break in production between satellites five and six.

In MILSATCOM, the prime contractor for the satellite is typically the satellite bus manufacturer. The satellite payload (or part of the payload) is often subcontracted to another firm. For wideband and narrowband systems in particular, the satellites can use a commercially available satellite bus with few modifications. The payload, however, typically has more unique military requirements and requires more custom development work, which limits the number of qualified vendors often to just one or two firms. One approach to reduce satellite costs is to separate the procurement of the satellite bus and payload. This could create more opportunities for competition by allowing satellite bus manufacturers to bid for the bus alone, which could open the competition to smaller or more commercially-oriented firms that may not have the requisite capabilities to serve as a prime contractor over the military-specific aspects of the overall program. Another option would be to make the payload contractor the prime, since competition is already limited for these capabilities, and allow competition for the satellite bus to occur at the subcontractor level.

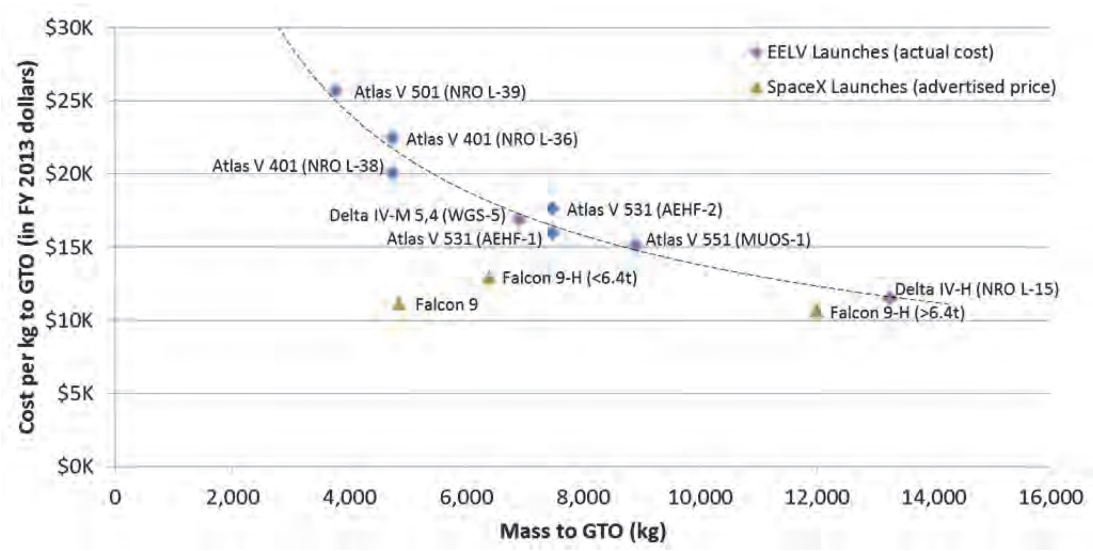
Launch

Launch costs, while less than the cost of the satellites themselves, are also an important consideration for MILSATCOM systems. Current generation MILSATCOM satellites are similar in weight, as shown in Table 1, and are launched into similar geosynchronous orbits. Thus, the launch costs are similar for all three types of satellites, roughly $120 to $130 million per launch in FY 2013 dollars. Launch costs add roughly 5 percent to the cost of AEHF, 10 percent for MUOS, and 25 percent for WGS.

One reason MILSATCOM satellites have tended to be large and highly aggregated is that the launch cost per unit mass tends to decline as the mass of the satellite increases, as shown in Figure 7. For example, it is less expensive to launch one 6,000 kg satellite than two 3,000 kg satellites. A new space launch provider, however, aims to bend the cost curve, making smaller missions more economical. The advertised prices for SpaceX's Falcon 9 and Falcon 9 Heavy launch vehicles, shown in green, are well below comparable Evolved Expendable Launch Vehicle (EELV) costs. The Falcon 9 in particular is roughly half the cost of the comparable Atlas V 401 launch vehicle. If the Air Force is able to realize these projected savings, smaller satellites may become a more attractive option for the future architecture.

[54] Statement of the Hon. Dr. Brendan Nelson, Minister for Defence, "Australia to Join with United States in Defence Global Satellite Communications Capability," October 3, 2007.

FIGURE 7: LAUNCH COSTS TO GEOSYNCHRONOUS TRANSFER ORBIT (GTO)[55]



Control and Terminal Segments

The MILSATCOM control segment includes ground systems that control the satellite bus and payload. The Command and Control System-Consolidated (CCS-C) is used for S-band control of satellite buses for Air Force MILSATCOM systems, including WGS, AEHF, Milstar, and DSCS satellites.[56] The Air Force's AEHF Mission Control Segment (MCS) controls the normal operation of the AEHF payload and satellite bus.[57] The WGS payload is controlled through the Wideband Satellite Operations Centers (WSOCs), which are operated and maintained by the Army. The MUOS constellation, which is developed and managed by the Navy, uses separate systems for command and control, including the Satellite Control Segment for control of the satellite bus and the Network Management Segment for control of the payload.

Development and procurement of the terminal segment is also dispersed across the Services. The Army, Navy, and Air Force each have independent terminal acquisition programs for AEHF and WGS. The development of MUOS-capable terminals was consolidated in the Joint Tactical Radio System (JTRS) program, but the terminals are funded separately by each of the Services. Due to repeated cost overruns and schedule delays, however, the Services are pursuing alternatives to JTRS-developed MUOS terminals.

The total cost of the control and terminal segments is difficult to quantify because the systems are funded through many different sources, some of which overlap with other program costs. The control segment is typically funded in part through the satellite development program and is often not

[55] EELV launch costs are derived from actual contract costs to DoD as reported in daily contract award notices (available at http://www.defense.gov/contracts/archive.aspx) and converted to FY 2013 dollars from the date of award. The maximum payload masses for each launch vehicle are from the Atlas V User's Guide (available at http://www.ulalaunch.com/site/docs/product_cards/guides/AtlasVUsersGuide2010.pdf) pp. 1-8; Delta IV User's Guide (available at http://www.ulalaunch.com/site/docs/product_cards/guides/DeltaIVPayloadPlannersGuide2007.pdf) pp. 2-10; Falcon 9 Overview (available at http://www.spacex.com/falcon9.php); and Falcon Heavy Overview (available at http://www.spacex.com/falcon_heavy.php).

[56] U.S. Air Force Fact Sheet, *Command and Control System Consolidated*, January 4, 2013.

[57] Department of Defense, *Selected Acquisition Report: AEHF*, p. 4.

reported separately. The cost of the terminal segment is more complicated to calculate because the costs are spread across multiple terminal acquisition programs in all three departments of the military. Moreover, the costs of terminal antennas and integration are sometimes funded in whole or in part by the platforms in which these terminals are used. According to one estimate, the terminal segment can cost more than the space and control segments combined.[58]

Cost is a significant factor in preventing the proliferation of protected MILSATCOM terminals to more tactical users. The Navy Multiband Terminal (NMT) and the Air Force's Family of Beyond-line-of-sight Terminal (FAB-T) are two major acquisition programs for AEHF-capable protected terminals. Both programs have experienced significant cost overruns and delays. The total cost per terminal for NMT and FAB-T are now estimated to average $7.0 million and $18.9 million, respectively.[59] Rather than field entirely new terminals, the Army elected to upgrade its existing inventory of Secure Mobile Anti-Jam Reliable Tactical Terminals (SMART-T) to operate over AEHF. The estimated cost of a SMART-T with AEHF capabilities is $2.5 million per terminal.[60]

In order to expand protected MILSATCOM capabilities to more users in the air, sea, and ground domains, DoD must drive down the cost of protected terminals. It is not realistic to expect that terminals can cost more than the platforms on which they are fielded. The military's attempts at reducing terminal costs, however, have often proved ineffective or counterproductive. For example, in June 2003 the Assistant Secretary of Defense for Networks and Information Integration (ASD/NII) issued a memorandum requiring all radio systems above 2 MHz (which included all MILSATCOM terminals) be developed in compliance with the Software Communications Architecture (SCA).[61] This new requirement applied to programs that were already in development, such as NMT and FAB-T. In the years that followed, this decision contributed to additional costs and schedule delays as these programs attempted to modify their designs to ensure compliance with an SCA standard that was not yet fully defined, particularly for high data rate MILSATCOM systems.

The military does not need to develop a new terminal, a new set of standards, or a new waveform in order to reduce costs.

The military, however, does not need to develop a new terminal, a new set of standards, or a new waveform in order to reduce costs. Recognizing the military need and the market opportunity that already exists, industry has begun working on its own to develop low-cost protected terminal alternatives for use with AEHF and Milstar. For example, TeleCommunications Systems, Northrop Grumman, and Lockheed Martin have partnered to develop and offer two low-cost protected terminals: one for protected communications on the move (P-COTM) and one for protected SIPR/NIPR access (P-SNAP). These terminals are being offered for as low as $350,000 each—a fraction of the cost of existing protected terminals.[62] These low-cost terminals do not offer all of the features of NMT, FAB-T, and SMART-T, but they provide a basic level of protection and would allow DoD to expand access to protected communications capabilities for more tactical users—exactly the sort of "80-percent solution" Secretary Gates advocated.

[58] Gregory Evans, "Joint Terminal Engineering Office," briefing presented at the 7th MILSATCOM Symposium of the Armed Forces Communications and Electronics Association, Los Angeles, CA, October 26, 2011, available at http://www.afcea-la.org/filebrowser/download/608, accessed on February 7, 2013.

[59] Data derived from DoD, *Selected Acquisition Report Summary Tables*, using the current estimate for the total program costs converted to FY 2013 dollars and divided by the total number of terminals planned for each program.

[60] Department of the Army, *Fiscal Year (FY) 2014 President's Budget Submission, Other Procurement, Army, Communications and Electronics Equipment, Budget Activity 2,* April 2013, p. 75.

[61] Assistant Secretary of Defense for Networks and Information Integration Memorandum, Subject: Radio Frequency (RF) Equipment Acquisition Policy, June 17, 2003.

[62] Sandra Erwin, "Lockheed-Northrop Alliance Looks to Shake Up Military SATCOM Market," *National Defense Magazine Blog,* September 26, 2012.

Programmatic Threats

The Vicious Cycle

MILSATCOM acquisitions are technologically complex with long development and production schedules and relatively small procurement quantities. These factors tend to reinforce one another in what has been called the "vicious cycle of space acquisition:" higher costs lead to smaller constellations and longer production times; smaller constellations require more capabilities to be packed into each satellite; and packing more capabilities into each satellite drives up complexity, leading to even higher costs and longer production times.[63] The vicious cycle of space acquisitions makes MILSATCOM systems arguably as vulnerable to cost overruns and schedule slips as they are to physical, electronic, and cyber attacks.

A high-profile example of the vicious cycle at work is the Transformational Satellite Communications System (TSAT), which was intended to be the follow-on for both WGS and AEHF. TSAT would have aggregated both wideband and protected capabilities into a smaller number of satellites. In its original configuration, the government envisioned that TSAT would operate in X-band, Ka-band, and EHF and would have used lasers for especially high-capacity communications links. When the program was formally initiated in 2004, the Air Force optimistically projected a first launch date of 2011 and a total cost of $15.5 billion for a five-satellite constellation. When some of the required technologies proved less mature than anticipated, the schedule slipped, costs increased, and capabilities were removed or deferred to future versions of the satellite.[64] Congress in turn reduced funding for the program, noting that the schedule was aggressive and the required technologies were not yet mature. The cascading effect of schedule slips, cost increases, funding instability, and capability reductions continued until the program was terminated in 2009. By that time more than $3 billion had been spent on development; many capabilities had been removed from the design; the total projected cost of the program had grown to more than $30 billion; and the first launch was slated for 2019 at the earliest. The Air Force's Space and Missile Systems Center (SMC) later acknowledged that TSAT "represented one more run around the vicious circle" of the acquisition system.[65]

Program Synchronization

Another programmatic vulnerability for MILSATCOM is synchronization across the space, control, and terminal segments. Synchronization is the proper alignment of schedules among interdependent programs to deliver capabilities efficiently and effectively.[66] In 2001, the Commission to Assess United States National Security Space Management and Organization noted in its final report to Congress:

> When satellite programs are funded in one budget and terminals in another, the decentralized arrangement can result in program disconnects and duplication. It can

[63] Pawlikowski, Loverro, and Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," p. 36.

[64] Government Accountability Office, *DOD Needs Additional Knowledge as it Embarks on a New Approach for Transformational Satellite Communications System* (Washington, D.C.: Government Accountability Office, May 2006).

[65] Pawlikowski, Loverro, and Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," p. 43.

[66] For a more extensive discussion of program synchronization, see Todd Harrison, "Measuring and Maintaining Program Synchronization," *Proceedings of Military Communications Conference (MILCOM)*, IEEE, 2008, available at: http://www.researchgate.net/publication/224372611_Measuring_and_maintaining_program_synchronization, accessed on December 18, 2012.

> result in lack of synchronization in the acquisition of satellites and their associated terminals…The current methods of budgeting for national security space programs lack the visibility and accountability essential to developing a coherent program.[67]

Synchronization across programs is important in MILSATCOM because all three segments (space, terminal, and control) are needed for the system to be operational. The timing of when these segments are fielded relative to one another is important because satellites have a finite life on-orbit—fuel is consumed for station-keeping, parts degrade from the harsh environment of space, and technology becomes obsolete with time. When one segment of the overall system is behind schedule due to funding shortfalls or development issues, the other segments may be forced to slip their schedules as well. Further complicating matters, the programs and associated budgets that fund the three segments of MILSATCOM are spread across the Services. In the terminal segment, the Army, Navy, and Air Force each independently fund the development of their own MILSATCOM terminals. If terminal programs are behind schedule in the Army or Navy, for example, it can lead the Air Force to delay the launch of a satellite or risk having a wasting asset on orbit that is not fully utilized. Likewise, a delay in a satellite program can cause a ripple of delays across the terminal programs intended for use on that satellite. Ultimately, this can lead to funding instability and successive schedule slips for the programs involved, which only exacerbates the "vicious cycle" of space acquisition.

MILSATCOM systems are also dependent on other elements of the space enterprise, such as launch vehicles. A delay in the availability of a launch vehicle, whether due to funding or technical issues, can have ripple effects across MILSATCOM acquisition programs. Because MILSATCOM architectures rely on a relatively small number of satellites acquired over long periods, a loss of even one satellite on launch could have severe consequences. A recent example of this critical dependence is the in-flight anomaly experienced on the RL10 upper stage, which is the only upper stage used on the EELV to launch MILSATCOM and other critical space systems. While launching a GPS satellite on October 4, 2012, the RL10 upper stage experienced a fuel leak. Although the satellite still reached its intended orbit, the anomaly prompted an investigation and delayed all other EELV launches. General William Shelton, head of Air Force Space Command, noted that, "We have to find out what happened and why, because there is no Plan B. The cost of launch failure would be staggering."[68]

[67] *Report of the Commission to Assess United States National Security Space Management and Organization,* Washington, DC, January 11, 2001, p. 75.

[68] Amy Butler, "Monopoly? SpaceX bests Orbital, eyes dual with ULA for Air Force contracts," *Aviation Week and Space Technology*, December 10, 2012, p. 34.

CHAPTER 3: OPTIONS FOR THE FUTURE ARCHITECTURE

This chapter explores options to address the twin challenges identified in the previous chapters: a more contested space environment and a more constrained budget environment. Writing in a now declassified memo for the National Reconnaissance Office in 1972, the physicist Amrom Katz suggested several approaches to protect space systems generally.[69] His list, which he acknowledged was not exhaustive, included: 1) making satellites more difficult to attack; 2) making satellites more difficult to detect; 3) making satellites easier to replace; and 4) being prepared to shoot down an adversary's satellites.

Katz's second point—making satellites more difficult to detect—is not a viable approach in MILSATCOM because the satellites are by definition prolific emitters in the electromagnetic spectrum and thus are easy to detect. Katz noted that the fourth point was not a compelling approach either because shooting down someone else's satellite would not bring back a disabled U.S. satellite. Moreover, this form of deterrence is not likely to be effective against adversaries who do not have critical space assets of their own that can be held at risk.

The options for the future architecture presented in this chapter build on the first and third options suggested by Katz. The first two options involve making systems more difficult to attack—Katz's first point—by improving system defenses and disaggregating, dispersing, or proliferating the constellation to make the satellites more difficult to target. The third option explored is to make the systems easier to replace—Katz's third point—so that their capabilities can be reconstituted quickly if they are attacked. A fourth option—one not listed by Katz—involves using alternatives to MILSATCOM that provide similar communications capabilities. Like Katz's list of options, the options explored in this chapter are not intended to be exhaustive or mutually exclusive.

Improve Defenses

Improving the defenses of MILSATCOM systems makes it harder for an adversary to attack these systems and disrupt or degrade the ability to communicate. While the space segment is vulnerable to

[69] Amrom Katz, "Preliminary Thoughts on Crises: More Questions Than Answers," Memorandum dated March 1972, pp. 6-7, available at: http://www.nro.gov/foia/declass/NROStaffRecords/489.PDF, accessed on November 30, 2012.

attack in many ways, the control and terminal segments are also vulnerable and must be considered. Ultimately, the protection of an overall system is only as strong as its weakest link, and the weakest link for a MILSATCOM system may, in some cases, be on the ground.

The current MILSATCOM architecture divides systems into protected and not protected, with many of the requirements for protected MILSATCOM focused on the strategic mission. But dividing the architecture distinctly along these lines is somewhat arbitrary because protection is not all or nothing. There are degrees of protection and different types of protection depending on the threat a system needs protection against. For example, protected systems like Milstar and AEHF employ a number of features designed to make jamming more difficult. Even using all of these features, however, Milstar and AEHF are not completely jam proof. Jamming can still degrade the performance of these systems and even cause some users to lose communications entirely. Likewise, unprotected systems like MUOS and WGS can employ some features, such as antenna notching and spread spectrum waveforms, which can improve their defenses to jamming.

To determine how best to improve MILSATCOM defenses, four fundamental questions need to be answered:

1) What threats does the system need to be defended against;
2) What is the weakest part of the system relative to these threats;
3) What level of protection is sufficient; and
4) What level of protection is affordable?

The first question requires a frank assessment of the impact and likelihood of different types of threats, as summarized in Figure 4 of the first chapter of this report. The priority should be to defend MILSATCOM systems against the most likely threats with the greatest potential impact—the upper right quadrant of the risk matrix. The second question requires a thorough assessment of the overall MILSATCOM architecture, from terminals and ground stations to the satellite bus and payload, to identify the parts of the system most vulnerable to these threats. The third and fourth questions involve a tradeoff between resources and risk. How much risk one is willing to tolerate must be balanced against the resources available to "buy down" that risk.

The answers to all four of these questions are ultimately subjective, but they are nevertheless important questions to ask when evaluating different means for improving the defenses of MILSATCOM systems. Below is a non-exhaustive list of various means to improve these defenses and the threats each option helps address. The list is divided into passive defenses, which allow a system to survive and operate through an attack, and active defenses, which attempt to intercept and disrupt an attack.

Passive Defenses

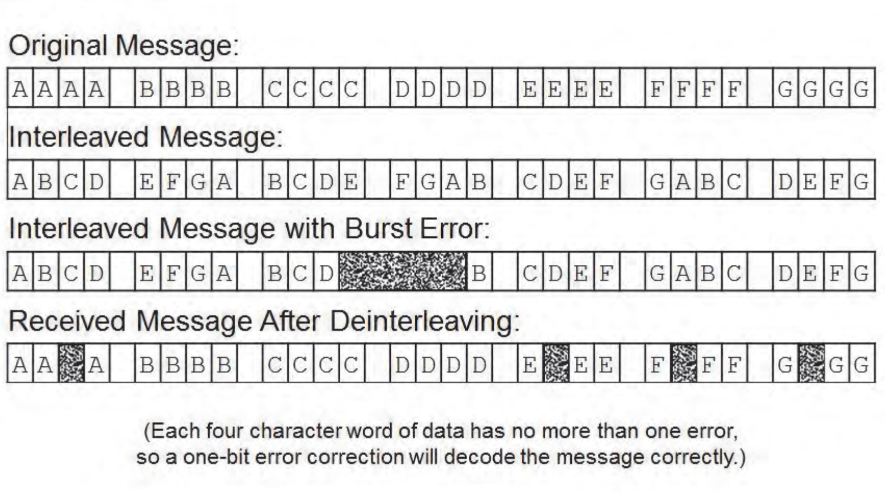
Frequency Hopping Spread Spectrum (FHSS): This method of protection involves rapidly changing the frequency of transmission using a pseudorandom sequence known to both the transmitter and receiver. It protects against uplink and downlink jamming by making it difficult for a narrowband jammer to match the frequency of transmission. By spreading the signal across a larger piece of bandwidth, the power required for transmission is lower, which also makes the signal harder to detect. And without knowing the hopping pattern, the signal is difficult to intercept—the random hopping can be difficult to distinguish from background noise.

Antenna Notching / Nulling: The antennas of MILSATCOM systems can be used to improve their resistance to jamming, particularly in the space segment. Antenna notching blocks all signals in a frequency band from being received, while antenna nulling blocks all signals from a geographical location from being received. A nuller, for example, can be used to block all signals coming from an area where an uplink jammer is suspected. Nulling out the area around a jammer, however, also blocks any authorized users within the footprint of the nuller.

On-board Processing: MILSATCOM systems can also improve their resistance to jamming and other forms of interference by demodulating and decoding the signal on the satellite before retransmitting it to another user. This allows the satellite to detect and correct errors in the data from the uplink so that these errors are not propagated in the downlink.

Interleaving: The process of dividing and mixing the bits of data being transmitted in a non-contiguous manner is known as interleaving. Because radio frequency (RF) interference tends to occur in bursts, errors often occur in multiple bits of data next to each other in a transmission. If more bit errors occur in a data packet than the error correction method can compensate for, the data becomes corrupted. Interleaving reduces this risk by shuffling the order of the data before it is transmitted and then reassembling it after it is received. This minimizes the chance that a burst of interference will create multiple errors within a single data packet. When combined with on-board processing and FHSS, interleaving can greatly improve the resistance to jamming and other forms of interference. Interleaving, however, increases the latency—the time between when data is transmitted and when it is received—because all of the data in an interleaving block must be received and reassembled in the proper order before it can be used.

FIGURE 8: EXAMPLE OF INTERLEAVING



Original Message:

AAAA BBBB CCCC DDDD EEEE FFFF GGGG

Interleaved Message:

ABCD EFGA BCDE FGAB CDEF GABC DEFG

Interleaved Message with Burst Error:

ABCD EFGA BCD▨ ▨▨▨B CDEF GABC DEFG

Received Message After Deinterleaving:

AA▨A BBBB CCCC DDDD E▨EE F▨FF G▨GG

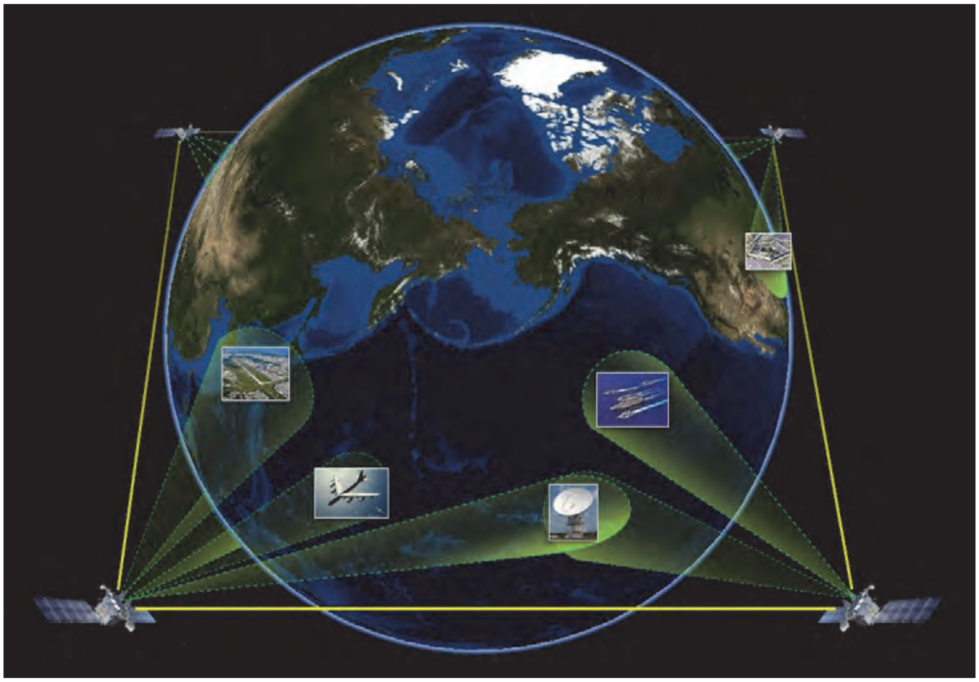
(Each four character word of data has no more than one error, so a one-bit error correction will decode the message correctly.)

Satellite Cross-Links: Satellites can reduce their dependence on ground stations by using inter-satellite links to pass data directly between satellites. Without cross-links, a satellite must route all data it receives to ground stations within its coverage footprint. For communications beyond the footprint of a satellite, this often means the data must be routed back up to another satellite and down to another ground station, delaying transmission time and using more valuable satellite resources. If one of these ground stations experiences an outage, whether due to attack, adverse weather, or other reasons, a satellite may not be able to route data to its intended recipient.

Cross-links allow a satellite to route data directly to other satellites and users beyond its coverage area. They also present fewer entry points for a potential cyber attack and fewer opportunities for detection, interception, and jamming because the antennas used between satellites are not pointed at

Earth. Cross-links also mean that the entire constellation of satellites can be controlled and monitored from a single control station, reducing the need for primary and backup control stations in each satellite's area of coverage.

FIGURE 9: EXAMPLE OF CROSSLINKS IN A FOUR-SATELLITE CONSTELLATION



Hardening for EMP: An electromagnetic pulse (EMP), whether produced by a nuclear detonation or high power microwave weapon, can damage electrical circuits and components on satellites, terminals, and control systems. Systems can be shielded to make them more survivable, but the additional development and testing required to ensure components are adequately protected adds complexity and expense. While hardening cannot protect a satellite from a close-proximity nuclear detonation, it can force an attacker to expend one nuclear warhead per satellite.[70]

Hardening for Conventional Ground Attacks: Ground stations can be hardened against conventional physical attacks by a number of means, such as establishing greater perimeters around facilities, relocating ground stations to less vulnerable areas, building hardened shelters designed to withstand attack, and maintaining robust backup systems for power, water, and other essentials.

Data Encryption: One of the most basic levels of protection against cyber attack is to encrypt all data being transmitted over MILSATCOM systems. While the level of encryption can vary by mission, a minimal level of encryption can be applied to all communications.

Active Defenses

Unlike passive defenses, which allow a system to survive and operate through an attack, active defenses are designed to intercept, disrupt, or otherwise thwart an attack before it can affect communications.

[70] U.S. Congress, Office of Technology Assessment, *Anti-Satellite Weapons, Countermeasures, and Arms Control*, p. 81.

Shoot-Back: One approach to defending satellites from ASAT weapons is to give satellites the capability to shoot-back. If an ASAT weapon is deployed, a satellite could strike the approaching warhead before it detonates using a small kinetic interceptor or a non-kinetic weapon, such as a high-powered laser. A critical challenge with this approach is that a shoot-back capability adds weight, power, and technological complexity to an already expensive satellite. Because satellites are mass and power limited, both kinetic and direct energy shoot-back systems would have a limited number of shots against incoming threats. Much like terrestrial missile defense systems, a shoot-back satellite defense system could put the United States on the wrong side of a cost-imposing strategy because it will likely cost less for an adversary to build more ASAT weapons than it will for the United States to build the systems needed to defend against more ASAT weapons. Moreover, even if a shoot-back system is successful at intercepting a threat, the destroyed warhead may create a long-lasting debris field that endangers the target satellite or other satellites.

A shoot-back satellite defense system could put the U.S. on the wrong side of a cost-imposing strategy because it will likely cost less for an adversary to build more ASAT weapons than it will for the U.S. to build the systems needed to defend against more ASAT weapons.

Escort Satellites: Another approach to defending space systems is to deploy escort satellites on orbit that have a shoot-back capability. A small constellation of escort satellites could, in principle, be deployed between orbital slots to protect a larger number of satellites at a relatively lower cost than including a shoot-back capability on each satellite. This would essentially be a zone defense approach in space. Escort satellites, however, still face many of the same issues as a shoot-back system: they would have a limited number of shots, their costs would scale in a way that favors the attacker, and a successful intercept could create a dangerous debris field.

Maneuver: One option explored during the Cold War was to design satellites with the ability to out-maneuver ASAT weapons. The challenge with this approach is that the satellite must be able to accelerate quickly—roughly as much as the ASAT weapon it is evading—which requires that a greater fraction of the satellite's mass be devoted to fuel rather than payload. A 1985 study by the U.S. Congress Office of Technology Assessment found that the physics tend to favor the attacker, "because an interceptor's payload can be quite small…an interceptor might have acceleration and delta-V [change in velocity] capabilities which would be much more costly to provide to satellites with large mission payloads."[71]

Attack the Source: Perhaps the most promising approach to defending space systems from physical attack is to target the source of an attack using terrestrial-based weapons. For example, the launch facilities of ASAT weapons or the location of a high-powered laser can be attacked on the ground with conventional weapons, such as a cruise missile or GPS-guided bomb. Space-based ASAT weapons, such as co-orbital satellites, could also be attacked from the ground using kinetic or non-kinetic ASAT weapons or other co-orbital satellites. The location of mobile ASAT systems and stealthy co-orbital satellites, however, may not be known prior to an attack.

All of the options presented to improve the defenses of MILSATCOM systems, both active and passive, increase costs and complexity. The costs associated with implementing data encryption, FHSS, and interleaving, for example, are relatively small compared to the overall cost of the system because they can largely be implemented in software or in the payload without a fundamental change in the satellite design. In contrast, active defenses, such as a shoot-back or maneuver capability, would likely add significant costs to MILSATCOM systems and require some combination of a larger satellite bus or a smaller payload to compensate for the additional size, weight, and power needed for active defenses.

[71] U.S. Congress, Office of Technology Assessment, *Anti-Satellite Weapons, Countermeasures, and Arms Control*, p. 81.

It is worth noting that the use of kinetic ASAT weapons and counter ASAT systems, such as the shoot-back and escort satellite capabilities discussed above, could threaten the viability of military, civil, and commercial space systems on a global scale. Every time debris is generated from an ASAT attack or counterattack, the probability of other satellites randomly colliding with debris increases. Each collision—whether debris hitting a satellite or striking other debris—can create thousands of new pieces of debris, thus increasing the probability of future collisions exponentially in a process known as the Kessler Syndrome.[72] At some point, the density of debris could reach "critical mass" and cause an uncontrolled chain reaction of collisions over the course of months or years, indiscriminately wiping out billions of dollars in critical space infrastructure that all nations have come to depend upon.[73] It could create a cloud of debris around Earth that makes future satellite launches too risky to pursue—effectively ruining the space domain for all civilian, commercial, and military users.

Disaggregate, Disperse, or Proliferate

Another approach to improve the protection of MILSATCOM systems is to make the systems more difficult to target by: 1) disaggregating capabilities so that multiple missions are not dependent on the same constellation of satellites; 2) dispersing capabilities by distributing payloads across a larger number of satellites; and 3) proliferating constellations by launching more of the same satellites. In a disaggregated or dispersed architecture, each satellite or payload is smaller, less capable, and (in theory) less expensive; however, the overall cost of the constellation may not be less expensive due to higher launch costs and the added cost of additional satellite buses. A proliferated constellation is by definition more expensive because more of the same satellites are procured, although the unit cost should decline as more satellites of the same type are built.

All three approaches make the system more resilient to the loss of a single satellite because each satellite represents a smaller fraction of overall capacity. This complicates an adversary's planning by forcing it to target more satellites to achieve the same effect.[74] As the Air Force Space and Missile Systems Center (SMC) has noted, "by reducing the operational impact of losing an individual vehicle, increasing constellation size, and distributing capability, we also change the effect of an attack and make it harder for an adversary to attain his intended results."[75] These approaches, however, are not without risks. While disaggregation, dispersion, and proliferation increase the difficulty of an attack, it may not prove to be a significant challenge for an adversary with a deep magazine of ASAT munitions. If an adversary is capable of attacking one satellite, it may also be able to attack multiple satellites. As in the case of a shoot-back or escort satellite capability, the attacker will have a cost advantage as the competition scales because ASAT weapons will likely cost much less than the satellites they threaten. While the defender will be at a disadvantage in such a scenario, the attacker may not be willing to escalate to a full-scale space attack, given the potential for space debris and the long-term, global effects that would result from multiple destroyed satellites.

While disaggregation, dispersion, and proliferation increase the difficulty of an attack, it may not prove to be a significant challenge for an adversary with a deep magazine of ASAT munitions.

[72] See Donald Kessler and Burton Cour-Palais, "Collision Frequency of Artificial Satellites: The Creation of a Debris Belt," *Journal of Geophysical Research*, Vol. 83, No. A6, June 1, 1978.
[73] John Johnson, Jr., "Scientists Cite Growing Peril of Space Junk," *L.A. Times*, April 16, 2008, p. A10.
[74] While an adversary capable of targeting one satellite is, in principle, capable of targeting more than one, forcing an adversary to be successful in multiple attacks to achieve the same effect increases the difficulty and risk of attacking.
[75] Pawlikowski, Loverro, and Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," p. 40.

One approach to disperse and/or disaggregate the space segment is to adopt a payload-centric acquisition model. Rather than designing and building satellites from the top down with a defined set of capabilities, a payload-centric approach would focus on specifying the capabilities of the payload first and then finding a satellite bus to host the payload. Using this approach, the payloads could be designed from the outset to be hosted by a wide range of satellite buses. It would also separate the procurement of satellite buses from satellite payloads and create more possibilities to host DoD payloads on non-DoD satellites.[76] If a commercial satellite, for example, has extra payload capacity available, DoD could pay to have a MILSATCOM payload hosted. Using a payload-centric approach could create system integration challenges due to differences in the interfaces and capabilities of different satellite buses. It could also present operational challenges, such as being forced to share satellite resources with other payloads or to use different control system software for satellites with different buses.

Hosting MILSATCOM payloads on the satellites of other nations—another form of dispersion—could be used to complicate an adversary's calculus. For example, as part of its rebalancing to the Asia/Pacific region, the United States could partner with allies in the region, such as Japan, South Korea, and Australia, to host a protected AEHF payload on one of their satellites. In exchange, these nations could be granted limited use of the global AEHF constellation. While such an arrangement would require overcoming various political and operational challenges, the potential operational and fiscal benefits are worth exploring. From the allies' perspective, this approach would improve interoperability with the U.S. military and give them access to a global constellation at a much lower cost than fielding an equivalent capability on their own. From an adversary's perspective, this would greatly complicate planning because an attack on the hosted payload (whether physical, electronic, or cyber) would be an attack on both the United States and the host nation, creating the risk of horizontal escalation in a crisis.

Another option to proliferate the constellation is to use on-orbit spares—fully functional satellites that are launched and maintained in a near-dormant state in space until they are needed. This approach effectively enlarges the size of the constellation, making it more resilient to a loss of one or more satellites. Like operational satellites, satellites stored in space accumulate all of the usual damage from the harsh space environment and use up expendable items, such as fuel for station keeping. Moreover, a kinetic attack that damages or destroys an operational satellite may leave debris that affects spare satellites stored in a nearby orbit, and the spare satellites themselves can be targeted. It may make more sense to store the satellites on the ground and launch them when a replacement is needed, which is discussed below as an option for making the system easier to replace.

Opportunities also exist to use disaggregation, dispersion, and proliferation in the control and terminal segments. The Air Force Satellite Control Network, for example, provides command and control for all military satellites using eight remote tracking facilities around the world.[77] DoD also operates six core teleport facilities around the world that are critical for routing data across MILSATCOM systems and connecting MILSATCOM systems to terrestrial networks. Instead of having so much capability concentrated in a relatively small number of ground sites, the military could spread these capabilities across a greater number of geographically dispersed sites.

[76] Pawlikowski, Loverro, and Cristler, "Space: Disruptive Challenges, New Opportunities, and New Strategies," p. 44.
[77] *The Air Force Handbook 2007*, p. 57, available at http://www.fas.org/irp/agency/usaf/handbook.pdf, accessed on December 18, 2012.

Make Systems Easier to Replace

A third option to address the vulnerabilities of MILSATCOM systems is to make the systems easier to replace after an attack. The current space segment architecture is difficult to reconstitute because the satellites are large, complex, expensive, and procured over long periods at low production rates. A more easily reconstituted architecture would ideally have satellites that are smaller, less expensive, and procured in larger numbers at a steady production rate.

The options for making systems easier to replace overlap in many ways with the options for dispersing and disaggregating the architecture. A payload-centric approach, for example, also makes the system easier to replace. The military could have extra payloads ready to launch on hosts to replace lost space assets after an attack. Another option is to have spare satellites in storage and ready for launch. Two key limitations in this approach, however, are cost and schedule. The spare satellites (or spare payloads) would have to be sufficiently inexpensive to allow for the procurement of reserves and they would need to be ready for launch within a short timeframe. Even with satellites sitting ready in storage, it would take weeks to months to integrate them with launch vehicles, launch them, and move them to the desired orbit. A launch-to-replace approach would also expose another vulnerability—the limited number of launch sites available to the United States, primarily Cape Canaveral in Florida and Vandenberg Air Force Base in California.

The U.S. could find itself on the wrong side of a cost-imposing strategy if an adversary's marginal cost of each attack is significantly less than the U.S. military's marginal cost of each replacement satellite or payload.

Mobile teleports and satellite control facilities could be used to replace a damaged or destroyed ground site rapidly. Mobile ground systems can be deployed worldwide via cargo aircraft or stored in theater in a protected facility. A rapidly deployable mobile ground system can be used to create uncertainty in the planning of a potential adversary, since it will not know in advance when or where a mobile site might be deployed.

Making satellites easier to replace may be a viable option to reconstitute capabilities from a small-scale, limited-duration attack. Yet, in a more protracted conflict where an adversary is able to attack U.S. satellites repeatedly, it can quickly become cost prohibitive to replace them. Once again, the United States could find itself on the wrong side of a cost-imposing strategy if an adversary's marginal cost of each attack is significantly less than the U.S. military's marginal cost of each replacement satellite or payload. Moreover, the stockpile of satellites or payloads sitting ready at the start of the conflict could quickly be exhausted in a protracted conflict. Even with an active production line available, it would likely take months to years to build additional satellites or payloads—much longer than combat forces may be willing to tolerate during an active conflict. A more effective approach may be to attack the source of an adversary's ASAT capabilities on Earth before launching replacement satellites. This assumes, however, that the locations of these capabilities (launch sites, radars, etc.) can be reliably located and their destruction can be confirmed—a questionable assumption if U.S. space capabilities have already been degraded by an initial attack.

Use Alternative Means of Communications

A fourth option for mitigating the vulnerabilities of MILSATCOM is to find alternative means of communicating. One of the most commonly used alternatives is commercial SATCOM. Rather than designing, building, and launching its own unique satellites, the military can lease SATCOM services from commercial providers. Commercial SATCOM provides several advantages, including no development costs and the flexibility to expand or reduce capacity as needed. Commercial SATCOM has proven invaluable over the past decade of operations in Iraq and Afghanistan, where warfighter demand for high-bandwidth applications, such as live video feeds from UAVs, has grown exponentially. By some estimates, up to 80 percent of DoD's current SATCOM requirements have been met using commercial SATCOM systems.[78]

Commercial SATCOM systems, however, are not designed for a contested communications environment. They offer virtually no protection from physical, electronic, and cyber attack. Security is a particular concern for commercial satellites because they can be owned or operated by a foreign entity, may connect to ground stations in foreign countries, and may be used simultaneously by a foreign government or foreign-controlled entities. For example, Doug Loverro, Deputy Assistant Secretary of Defense for Space Policy, recently testified before Congress that DoD-leased commercial SATCOM services to support urgent warfighter needs from a Chinese company.[79] This particular lease may have made sense because the Chinese company was the only provider with bandwidth available in the theater it was needed. But at times commercial satellite bandwidth may not be available for lease when and where it is needed—regardless of what company or country controls the satellites. For these reasons, commercial SATCOM is not a viable alternative in situations where communications are of vital importance and communications are contested.

Depending on the altitude and number of aircraft used, an aerial communications layer can provide high-capacity communications to supplement or replace MILSATCOM within a region. If equipped with payloads using some of the passive protection features described above, such as FHSS, on-board processing, interleaving, and encryption, an aerial layer can be resistant to jamming and cyber attack. However, it would be cost prohibitive and logistically infeasible to provide global coverage using an aerial layer because of the number of aircraft required. Moreover, the aircraft used to provide an aerial communications layer can only operate in permissive airspace. They are by definition high emitters and can be targeted by air defense systems. An aerial communications layer is therefore not a viable alternative in situations where the air domain is contested.

Terrestrial radio frequency (RF) communications (e.g., radio towers) are a viable alternative for users needing to communicate over relatively short distances. While terrestrial communications can employ many of the same protective features to resist jamming and cyber attack, these systems require a relatively permissive ground environment for the military to field and operate them. Users must have physical access to an area and be within line of sight of a ground station or another user. Terrestrial RF communications are therefore not a viable alternative for users needing to communicate beyond line of sight or where the ground domain is non-permissive.

A fourth alternative is to change the way systems operate to reduce their communications needs. UAVs, for example, could employ greater on-board capabilities to analyze sensor data autonomously, only transmitting data with a high probability of interest to analysts on the ground. A less autonomous approach is to simply store the data locally rather than processing or transmitting it in real-time. The Air Force's Gorgon Stare wide-area imaging pod for Predator and Reaper UAVs, for example, produces far more data than it can transmit over existing terrestrial and SATCOM systems. Instead, a lower resolution video stream is transmitted in real-time while the remainder of the data is stored on board and downloaded for analysis after the vehicle lands. A store-and-forward approach can also be useful in a contested communications environment. Data can be stored locally when communications are being jammed or when a platform wants to avoid detection and then transmitted

[78] Rosenberg, "DOD's reliance on commercial satellites hits new zenith."

[79] House Committee on Armed Services, Subcommittee on Strategic Forces, *Hearing on Fiscal Year 2014 National Defense Authorization Budget Request for National Security Space Activities*, 113th Congress, 1st session, April 25, 2013.

once communications are restored. A store-and-forward approach, however, is not an attractive alternative for time-sensitive operations.

Summary

Amron Katz noted in his 1972 memo that U.S. space assets, "have been protected by assumption—the belief that nobody would interfere with their operation." He went on to write:

> Even in the absence of evidence that the assumption rests on questionable premises, it should have been clear that the line of development we were pursuing—a predictable manifestation of U.S. style—might itself greatly influence or change the other guy's behavior. Said simply, we are tempting him with juicier targets than we used to.[80]

This chapter presented four options to make MILSATCOM systems less vulnerable to attack and, thus, a less appealing target for adversaries. In a constrained funding environment, however, not all of these options can be pursued in parallel. Moreover, priorities differ among MILSATCOM users, with some options being better or worse for a particular set of users depending on their operational needs.

Protected MILSATCOM systems like Milstar and AEHF maximize the level of protection for a limited set of users (mainly strategic forces) by employing many of the passive defenses described above. This high degree of protection, however, comes at a high price. An AEHF satellite, for example, costs roughly four times as much as a WGS satellite.[81] A key question for the future MILSATCOM architecture is, given the range of threats the nation is likely to face in the space domain, should some level of protection be extended to all MILSATCOM users? Moreover, do all users of protected MILSATCOM systems need the highest level of protection provided? In a resource-constrained environment, the balance of risk among different types of MILSATCOM users may need to be adjusted. It may be preferable, in some instances, to provide a lower level of protection to a larger number of users rather than a high degree of protection for a small number of users.

In a resource constrained environment, the balance of risk among different types of MILSATCOM users may need to be adjusted.

The existing protected MILSATCOM architecture lumps together tactical and strategic protected users on the same systems. But tactical and strategic users face very different threats in the space domain. Tactical users, for example, are more likely to experience downlink jamming because at times they operate in closer proximity to adversaries, while strategic users are more concerned about nuclear threats to the U.S. homeland. The following chapter evaluates the options presented to improve the protection of MILSATCOM systems in the context of mission requirements to illustrate the tradeoffs involved in meeting the MILSATCOM needs of combat forces in a more contested environment.

[80] Katz, "Preliminary Thoughts on Crises: More Questions Than Answers," p. 5.

[81] The cost of each additional WGS satellite is approximately $400 million; see Department of Defense, *Selected Acquisition Report Summary Tables* (Washington, D.C.: Department of Defense, December 2011), p. 6. The cost of each additional AEHF satellite is approximately $1,550 million; see House Committee on Armed Services, Subcommittee on Strategic Forces: *Hearing on Budget Request for National Security Space Activities*, 112th Congress, 2nd session, March 8, 2012, p. 108.

CHAPTER 4: SUPPORT FOR COMBAT FORCES

The future threat environment for the U.S. military is likely to be increasingly contested in all domains. As more sophisticated adversaries seek asymmetric means to counter the overwhelming advantage of U.S. forces in conventional military operations, the technologies needed to contest U.S. military operations in the air, sea, land, and space domains could proliferate to less advanced nations and non-state actors. The 2012 Defense Strategic Guidance made countering these threats a priority for the military, specifically highlighting the importance of efforts to protect space-based systems:

> In order to credibly deter potential adversaries and to prevent them from achieving their objectives, the United States must maintain its ability to project power in areas in which our access and freedom to operate are challenged… Accordingly, the U.S. military will invest as required to ensure its ability to operate effectively in anti-access and area denial (A2/AD) environments. This will include implementing the Joint Operational Access Concept, sustaining our undersea capabilities, developing a new stealth bomber, improving missile defenses, and *continuing efforts to enhance the resiliency and effectiveness of critical space-based capabilities.*[82] [emphasis added]

The challenge for the future architecture is to balance costs and risks so that all MILSATCOM users have an adequate level of protection—i.e., no fronts are left undefended.

The current MILSATCOM architecture already provides an impressive degree of protection for some MILSATCOM users. Strategic users and some tactical users on AEHF and Milstar enjoy a high degree of protection from electronic and cyber attack. However, the vast majority of DoD's SATCOM users—those using WGS, DSCS, MUOS, UFO, and commercial systems—operate with little or no protection. Under the currently planned architecture, only 7 percent of total U.S. MILSATCOM capacity is provided by protected systems.[83]

Just as the French did not attempt to build a Maginot Line around their entire border, the United States should not attempt to make all MILSATCOM systems protected to the level of AEHF. The challenge for the future architecture is to balance costs and risks so that all MILSATCOM users have an

[82] Department of Defense, *Sustaining U.S. Global Leadership: Priorities for 21st Century Defense* (Washington, DC: DoD, January 2012), pp. 4-5.

[83] Assumes a fully deployed six-satellite AEHF constellation with a total capacity of 1.2 Gbps (see Department of Defense, *Selected Acquisition Report for AEHF*, December 31, 2011, p. 9); and an eight-satellite WGS constellation with a total capacity of 17.1 Gbps (see DoD, *Selected Acquisition Report for WGS*, December 31, 2011, p. 7).

adequate level of protection—i.e., no fronts are left undefended. This chapter evaluates options for protecting MILSATCOM by examining the operational needs of the combat forces it enables. Three key mission areas are explored: global surveillance and strike, special operations, and strategic forces. While many important MILSATCOM users fall outside these areas, these three are used to highlight some of the difficult challenges and tradeoffs involved in designing the next generation MILSATCOM architecture.

Global Surveillance and Strike

The global surveillance and strike (GSS) mission area includes a broad set of conventional (non-nuclear) capabilities designed to project power on a global scale with precision and persistence. It includes airborne platforms, such as long-range bombers, tactical fighters, manned surveillance aircraft, and unmanned aircraft used for both strike and surveillance. It also includes naval platforms, such as submarines, destroyers, and carriers, which serve as mobile operating bases to conduct surveillance or launch strikes using carrier-based aircraft or standoff weapons, such as Tomahawk cruise missiles. As A2/AD capabilities grow more sophisticated and proliferate around the world, long-range strike capabilities will become more important. A2/AD capabilities are designed to challenge the ability of U.S. forces to project power within a region by restricting freedom of action or preventing the deployment of forces within an area of operations.[84] To counter this threat, the United States will need to be able to operate forces over longer distances using platforms that are more difficult for an adversary to detect and target.

The GSS mission area can also be called the "space-enabled reconnaissance strike complex" because it is critically dependent on space-based capabilities, such as MILSATCOM.

The GSS mission area can also be called the "space-enabled reconnaissance strike complex" because it is critically dependent on space-based capabilities, such as MILSATCOM.[85] GSS platforms need global coverage and the ability to communicate over long distances. Surveillance platforms need to transmit information at high data rates to support advanced sensors, such as multi-spectral high-resolution streaming video. Strike platforms need to receive targeting data in real time to be effective in a non-permissive environment. In contested airspace, for example, stealthy strike aircraft (whether manned or unmanned) would put themselves at risk using active sensors to detect targets, since active sensors emit electromagnetic waves than can potentially be detected. Instead, other platforms operating at a safe distance can use active sensors to detect, identify, and track mobile targets and then relay that information to strike platforms—a concept known as off-board queuing. This means both manned and unmanned aircraft are critically dependent on communications links when pursuing mobile targets in contested airspace.

GSS communications are vulnerable to uplink jamming, detection, and interception. A more sophisticated adversary may also attempt to use a cyber attack to seize control of a satellite or use a directed energy weapon to disable a satellite. An attack against a ground station is less of a concern for this mission area because it requires an adversary either to launch a precision-guided missile attack over a significant distance (i.e., they would need a GSS capability of their own) or to use a special operations or terrorist-like attack against a ground station. For conventional GSS missions, an adversary would likely be reluctant to attack a satellite using a kinetic ASAT weapon—if they have such a capability—because it could quickly escalate and broaden the conflict. Likewise, a nuclear attack against space systems would fundamentally and radically escalate the conflict from the conventional level to the strategic level.

[84] For an overview of A2/AD challenges, see Department of Defense, *Joint Operational Access Concept Version 1.0* (Washington, DC: Department of Defense, January 17, 2012), pp. 6-7.
[85] Kueter, "The War in Space Has Already Begun," p. 1.

Given the threats of most concern for the global surveillance and strike mission area, passive defenses are an attractive option for addressing the vulnerabilities of MILSATCOM systems. Using encryption, FHSS, antenna nulling, on-board processing, interleaving, and satellite cross-links, for example, would make communications more difficult to jam, detect, and intercept. Nuclear hardening of the satellites and hardening ground stations against conventional attack should be a lower priority since these threats are less of a concern for the GSS mission area.

Dispersing and disaggregating MILSATCOM systems to make them more difficult to target is also a viable option for protecting GSS communications. In particular, this option increases the resiliency of the architecture to losing a satellite, whether from an adversary seizing control of a satellite through cyber attack or disabling a satellite using a directed energy weapon. A dispersed MILSATCOM constellation could also use satellites in LEO. Because these satellites are 22,000 miles closer to earth, the transmission power required to and from the satellite is much lower, making the signal emanating from a terminal more difficult to detect.[86] Satellites in LEO are also moving relative to the earth, making them more difficult to target with an uplink jammer because the jammer's antenna must be able to track the satellite as it moves across the sky. Because GSS platforms are inherently mobile, many of the MILSATCOM terminals they use already employ tracking antennas that could be adapted to track satellites in LEO, although the handover of links from one satellite to another would pose a challenge.

Making MILSATCOM systems easier to replace is not an attractive option because there would not be sufficient time to get a replacement satellite on orbit and operational in a short-duration conflict of several days or weeks, during which time GSS operations would be degraded.[87] In a protracted conflict (months to years) where an adversary can repeatedly target MILSATCOM systems, the available stock of replacements could be exhausted and the time required to make new replacements could exceed the duration of the conflict. Moreover, an adversary could use this as a cost-imposing strategy by forcing the United States to spend much more to reconstitute space assets (or prepare to reconstitute them in advance of a conflict) than it costs to destroy them.

Alternatives to MILSATCOM are not an attractive option for the GSS mission area. Commercial SATCOM, for example, provides virtually no protection from jamming, detection, and interception. Both an aerial layer and terrestrial RF communications require a permissive operating environment, which cannot be assured (particularly in the early phases of conflict) given the spread of A2/AD capabilities. Altering operations to reduce the need for MILSATCOM, such as using a store-and-forward concept, is also not viable for GSS because mobile, transient, and emerging targets need to be identified and prosecuted in near real time.

Special Operations

Special operations forces (SOF) are small-footprint, rapidly deployable units that can operate covertly to conduct reconnaissance, counter-terrorism operations, counter-weapons of mass destruction operations, and unconventional warfare. SOF units can also be used for civil affairs, training, and internal defense for foreign governments. Special forces often operate over long distances in remote

[86] MIT Industry Systems Study, *Communications Satellite Constellations* (Cambridge, MA: Massachusetts Institute of Technology Engineering Systems Learning Center, 2003), p. 5.

[87] It would take at least several days or weeks to: 1) mate a satellite with a launch vehicle; 2) move the launch vehicle into position for launch; 3) fuel the vehicle; 4) prepare the launch range; 5) wait for a launch window to open (depending on the desired orbit); 6) move the satellite to its intended orbital slot; and 7) perform on-orbit checkout of the satellite. Normally this process takes several months.

regions with little infrastructure or other support. They can be called upon to operate in non-permissive environments where avoiding detection is a paramount concern. The key attributes needed for SOF communications are range, wide-area coverage, and low probability of detection and interception.[88] SOF users also need to communicate on the move using relatively small handheld or man-packable terminals.

The risk of physical attacks against satellites and ground stations is relatively lower for SOF communications because SOF units tend to operate covertly. An adversary would be unlikely to launch a physical attack against satellites or ground stations without knowing if special operations forces are in fact being used against them. If an adversary did take such a step, the conflict would likely escalate beyond the use of SOF to include GSS forces. Since physical attacks against the space segment and ground stations are less of a concern, options that protect against these threats are less important for SOF users.

The primary vulnerabilities for SOF communications are detection and interception.

The primary vulnerabilities for SOF communications are detection and interception. Hardening SOF communications against electronic and cyber attack using encryption, FHSS, and on-board processing are viable options to improve protection from detection and interception. Jamming is less of a concern for SOF users because an adversary must first detect their presence before they can attempt to jam communications. While SOF users do not necessarily need a dispersed and disaggregated MILSATCOM constellation to protect against anti-satellite weapons, a large constellation of satellites in LEO could be advantageous in other ways. Communicating with satellites in LEO allows the signal emanating from the terminal to be lower power, making it more difficult to detect. Alternatively, the terminal can use a smaller antenna, making it easier to transport.[89]

Making MILSATCOM systems easier to replace and finding alternatives to MILSATCOM are not viable options for SOF communications. Replacing a satellite or ground station within the timeframe of a typical SOF operation is infeasible. Likewise, commercial SATCOM, an aerial communications layer, and terrestrial communications are not viable alternatives because SOF must be able to operate in contested environments.

Strategic Forces

Strategic forces include the nation's arsenal of nuclear weapons, the platforms that deliver these weapons, and the assets used to detect a hostile nuclear attack. The key communications requirements for strategic forces are to maintain positive command and control of nuclear forces and early warning systems before, during, and after a nuclear attack. Maintaining this global connectivity is a critical element of deterrence—knowing that the United States has an assured ability to launch a devastating counter attack can deter an adversary from launching a first strike. Due to the nature of the weapons they command, strategic forces' communications must confront nearly all types of threats, including jamming, cyber attacks, ASAT weapons, and ground station attacks.

Protected MILSATCOM systems were originally designed with the strategic user in mind and thus already implement many of the features that make a system more difficult to attack. For example, Milstar and AEHF include: nuclear hardening to protect against the effects of a nuclear detonation in space; cross-links to reduce the dependence on ground stations; and FHSS, antenna nulling, on-board

[88] For a more detailed discussion of SOF communications needs, see Jim Thomas and Chris Dougherty, *Beyond the Ramparts: The Future of U.S. Special Operations Forces* (Washington, DC: CSBA, 2013) p. 100.
[89] MIT Industry Systems Study, *Communications Satellite Constellations* (Cambridge, MA: Massachusetts Institute of Technology Engineering Systems Learning Center, 2003), p. 5.

processing, and interleaving to protect against jamming and nuclear scintillation. These systems, however, are vulnerable to kinetic and directed energy anti-satellite weapons. The loss of just one or two protected MILSATCOM satellites could break the "ring" of cross-links among the satellites and diminish the constellation's ability to support strategic forces.

One option to address this vulnerability is to disperse or proliferate the constellation to make it less susceptible to a single-point failure. Simply adding more satellites to the constellation in different orbits would complicate the targeting problem for an adversary and make the constellation relatively more robust to attack. The downside is that all of the protected features described above add significantly to the cost of the satellites. The marginal cost of each additional AEHF satellite, for example, is $1.55 billion.[90] Adding more satellites to the constellation may not be an affordable option unless the cost of these satellites can be reduced significantly. Dispersing the constellation by dividing the same level of capability across a greater number of satellites would improve the constellation's ability to withstand a loss of one or more satellites. But the cost of a dispersed constellation of equivalent capacity and capability would also likely be higher than the existing constellation, due in part to the higher cost of launch per unit mass for smaller payloads.[91]

Buying replacement satellites in the event that a satellite is disabled or destroyed is not a viable option because of the relatively long lead-time needed to build and launch another satellite. A nuclear exchange could be over within hours or days, well before a replacement satellite could be launched even if one is waiting in storage. Moreover, in a strategic conflict, targets in the U.S. mainland could be at risk of attack, including the launch sites at Cape Canaveral, Florida and Vandenberg Air Force Base, California. Alternatives to MILSATCOM are also not viable for strategic forces because they either lack sufficient protection (commercial SATCOM), do not provide persistent global coverage (aerial and terrestrial communications), and cannot operate in non-permissive environments.

Summary

As the military seeks to shift its focus from the past decade of major stabilization operations in Iraq and Afghanistan to the emerging A2/AD threats in the Pacific, MILSATCOM systems must shift their focus as well.

While the three mission areas highlighted here, GSS, SOF, and strategic forces, do not encompass the full range of U.S. military capabilities or mission sets, they are three of the U.S. military's highest priority missions and are likely to remain so for the indefinite future. As the military seeks to shift its focus from the past decade of major stabilization operations in Iraq and Afghanistan to the emerging A2/AD threats in the Pacific, MILSATCOM systems must shift their focus as well. Unprotected wideband and narrowband systems, which proved invaluable for ground forces in Iraq and Afghanistan, are not well suited for an environment in which communications are contested. Just as the MQ-1 Predator UAV is not a viable capability for penetrating defended airspace because the aircraft is not stealthy, the unprotected communications link used by the Predator is not a viable option for use against an adversary with electronic attack capabilities.

Table 2 summarizes the options for improving the protection of MILSATCOM from the third chapter and the applicability of each for the mission areas explored in this chapter. Improving defenses, particularly passive defenses, is a good option for all three mission areas to protect systems from electronic and cyber attacks. Dispersing, disaggregating, or proliferating the architecture is a good option for the GSS and strategic forces mission areas to protect systems from physical attack, although these approaches may be unaffordable unless the cost per satellite is reduced significantly.

[90] House Committee on Armed Services, Subcommittee on Strategic Forces, *Hearing on Budget Request for National Security Space Activities*, 112th Congress, 2nd session, March 8, 2012, p. 108.
[91] See Figure 7.

Making systems easier to replace is not a viable option for any of the mission areas because the time needed to prepare and launch a replacement system is too long for a short-duration conflict and the stock of replacements could be exhausted in a protracted conflict. Alternatives to MILSATCOM, such as an aerial layer or commercial SATCOM, are not viable as well because GSS, SOF, and strategic forces need to operate on a global scale in contested environments.

TABLE 2: SUMMARY OF MILSATCOM OPTIONS FOR THREE EXAMPLE MISSION AREAS

Options to Improve Protection		***Global Surveillance and Strike***	***Special Operations***	***Strategic Forces***
Improve Defenses	***Passive***	Good option to improve protection from electronic and cyber attack and enable operations in a non-permissive environment.	Good option to improve protection from electronic attack and enable operations in a non-permissive environment.	Good option to improve protection from nuclear attack, electronic attack, and cyber attack.
	Active	Attacking the source is a good option to counter ASAT threats. Shoot back, maneuver, and escort satellites are less desirable options due to the costs and potential for space debris.	Less relevant because ASAT threats are a lower risk for SOF missions.	Attacking the source is a good option to counter ASAT threats. Shoot back, maneuver, and escort satellites are not viable options due to the cost and potential for space debris.
Disperse, Disaggregate, Proliferate		Good option to improve protection from physical attacks on satellites and ground stations. May not be affordable unless the cost per satellite is reduced.	Less relevant because the risk of physical attack is lower for SOF missions.	Good option to improve protection from physical attacks on satellites and ground stations. May not be affordable unless the cost per satellite is reduced.
Make Systems Easier to Replace		Not viable because replacement time is too long in a short-duration conflict and replacements could be exhausted in a protracted conflict.	Not viable because replacement time is too long for typical SOF operations.	Not viable because replacement time is too long for a nuclear conflict.
Find Alternatives to MILSATCOM		Not viable because GSS forces need global coverage and must operate in contested air, land, and communications environments.	Not viable because SOF need global coverage and must operate in contested air, land, and communications environments.	Not viable due to the lack of nuclear hardening and global coverage.

CHAPTER 5: A STRATEGIC CHOICE IN SPACE

The twin challenges facing MILSATCOM of a more contested space domain and more constrained funding environment are challenges for other military space systems as well. While U.S. military planners and strategists largely recognize that the air, sea, and land domains are likely to be increasingly contested in the future, the growing threats in the space domain are often less recognized and discussed. Space is a contested domain of modern warfare, and as the threats to space systems grow and proliferate it will increasingly affect the ability of space systems to enable other weapon systems in the air, sea, and land domains. As Congressman Ed Markey has noted, "American satellites are the soft underbelly of our national security."[92]

A day without space could quickly become a decade without space if next-generation space systems are designed for the wrong threats or acquisition programs fail due to cost overruns and delays.

The next-generation architecture for future space systems presents an important strategic choice for defense planners. Should the U.S. military invest in the capabilities required to contest the space domain and maintain assured access to space-based capabilities? A number of studies by DoD and independent research groups have sought to highlight the implications of a day without the enabling capabilities provided from space. As the previous chapter demonstrated, the alternatives to space systems are not appealing for key users of space-based capabilities, such as global surveillance and strike, special operations, and strategic forces. Moreover, due to the long lead times in developing and fielding space systems, a day without space could quickly become a decade without space if next-generation space systems are designed for the wrong threats or acquisition programs fail due to cost overruns and delays.

Six specific recommendations are offered to meet the needs of combat forces based on the threats MILSATCOM systems face, the budget constraints likely to be imposed, and the options available.

Recommendation 1: Transition to a Three-Tier MILSATCOM Architecture

The primary recommendation of this study is to transition from a two-tier MILSATCOM architecture (protected and unprotected) to a three-tier architecture. In a three-tier architecture, the highest tier of protection would be reserved for strategic users and would be largely unchanged from the current program of record for protected systems. A new middle tier of protection would be created to extend

[92] Congressman Ed Markey, "Markey Denounces Chinese Missile Test; Calls on Bush Admin. to Strike Agreement to Ban Future Tests," Press Release, January 18, 2007, available at http://markey.house.gov/press-release/january-18-2007-markey-denounces-chinese-missile-test-calls-bush-admin-strike, accessed on November 28, 2012.

a lower level of protection to more tactical users. It would be funded by drawing resources from unprotected SATCOM programs. The lowest tier of the architecture would be reserved for all other non-essential communications and could be acquired as a service rather than a system.

Highest Tier of Protection: Strategic Users

The highest degree of protection should be afforded to strategic users, due to the range and severity of the threats inherent to strategic conflict. Strategic users include missile warning, nuclear command and control, presidential voice communications, and other key national missions. Strategic users need protection from jamming, detection, interception, kinetic and directed energy ASAT weapons, and attacks against ground stations.

In transitioning to a three-tier architecture, the highest tier of protection would be largely unchanged from the current program of record.

Strategic users are currently served by Milstar, AEHF, and IPS. These systems employ the full range of passive defenses listed in Chapter 3 to protect against jamming, detection, interception, and attacks on ground stations. They are, however, largely unprotected against kinetic and directed energy attacks against the space segment. Active defenses designed to thwart physical attacks, such as arming satellites with shoot-back systems, would likely prove cost prohibitive in a constrained budget environment. A more cost-effective approach to countering physical attacks may be to adapt conventional weapons and/or tactics to attack the source of ASAT weapons on Earth.

In transitioning to a three-tier architecture, the highest tier of protection would be largely unchanged from the current program of record. The AEHF system, currently the only protected system in production, is sufficient to meet the needs of strategic users. The size of the AEHF constellation is relatively insensitive to a change in the size of the U.S. nuclear arsenal because a minimum of four satellites operating on orbit is needed to complete the “ring” and provide global, cross-linked coverage. Additional polar systems will be needed when the current IPS reaches its end of life, but the replacement polar system could again be a modified AEHF payload hosted on a polar orbiting satellite.

Middle Tier of Protection: Tactical Users

In the current architecture, both protected and unprotected systems serve tactical users. Tactical users on AEHF and Milstar, for example, enjoy a high degree of protection from jamming, detection, and interception. On WGS, MUOS, and commercially leased satellites, however, tactical users enjoy little, if any, protection—a vulnerability that insurgents in Iraq and Afghanistan have already exploited. Only 7 percent of the current architecture’s capacity is protected, meaning many tactical users are using unprotected systems for mission critical communications.

The purpose of creating a middle tier in the next-generation architecture is to extend a lower level of protection to more tactical users.

The purpose of creating a middle tier in the next-generation architecture is to extend a lower level of protection to more tactical users. Middle-tier protection would focus on countering the threats tactical users are most likely to confront in an A2/AD environment. For example, middle-tier systems could employ passive defenses such as FHSS, interleaving, on-board processing, cross-links, and data encryption to protect tactical users from jamming, detection, and interception. The satellites, terminals, and ground facilities used in the middle tier would not need other protective measures, such as nuclear hardening.

Creating a level of protection below the threshold needed by strategic users enables a number of new options to reduce costs and expand protected MILSATCOM capacity. The middle tier space segment, for example, could be a constellation of cross-linked AEHF-based payloads hosted on other satellites. The hosted payloads could form a separate “tactical” ring of protected satellites that could be reconfigured, if needed, to join or supplement the existing strategic ring of AEHF satellites. The host satellites would not need to be nuclear hardened like AEHF, since tactical users do not require this type of protection. Host satellites could be other military satellites, commercial satellites, or satellites belonging to international partners. Because the protected payload used would be a derivative of the current AEHF payload, it would require minimal development and testing, it could share the same ground control infrastructure as AEHF, and existing AEHF terminals would be interoperable with it. An essential component of this approach is the proliferation of low-cost protected terminals to more tactical users.

AEHF-based hosted payloads would serve tactical users needing data links less than 8.2 Mbps. For higher data rate requirements, such as streaming video from UAVs, a higher bandwidth payload would be needed to protect these mission critical communications in a high-threat environment. As an interim step, high data rate users could use direct sequence spread spectrum modems in terminals over the existing WGS constellation. The use of spread spectrum modems provides an increased level of protection against jamming, detection, and interception relative to non-spread spectrum modems.[93] Spread spectrum modems are commercially available and are already being adopted by some military Ka-band users.[94] A long-term solution to provide a greater degree of protection for high data rate users would be to evolve the AEHF XDR waveform to accommodate higher data rates. However, a development effort such as this should be deferred until after the transition to a three-tier architecture is underway, given the added cost and time involved in modifying the waveform.

Lowest Tier of Protection: Non-Essential Communications

The future architecture should also explicitly include a lowest tier of protection reserved for all other non-essential communications, such as television broadcasts and internet access for deployed troops. While some of these communications currently use systems such as WGS and the Global Broadcast Service (GBS) hosted on various satellites, in the future architecture the lowest tier of protection should transition away from military owned and operated satellites. The military does not need to pay for the development and added expense of procuring unique military systems for communications that can be adequately served by commercial SATCOM service providers. This would allow the military to focus its development efforts on truly unique military communications requirements, specifically protected MILSATCOM systems in the high and middle tiers.

The lowest tier in the architecture could be acquired as a service rather than a system.

The lowest tier in the architecture could be acquired as a service rather than a system. All competitive options should be explored, including contracting for multi-year leases, buying options for commercial transponders for surge capacity, and developing a civil reserve space fleet modeled on the civil reserve air fleet.[95] The objective should be to leverage the commercial SATCOM market to reduce the cost of non-essential communications. Given the future threat environment—specifically the threat of cyber attack—even non-essential communications should still be provided with a minimal level of protection, namely data encryption.

Recommendation 2: Pivot to the Pacific in Space

A second recommendation is to pivot to the Pacific in space by inviting key allies in the region such as Japan, Australia, and South Korea to be part of the middle tier of the architecture. Partner nations could share the costs of expanding the middle tier of the architecture and in return be given a

[93] Richard Williams and Heywood Paul, "Potential Uses of the Military Ka-Band for Wideband MILSATCOM Systems," IEEE Military Communications Conference, October 18-21, 1998, Boston MA.
[94] L3 Communications product data sheet for the MPM-1000 IP Modem, available at http://www2.l-3com.com/linkabit/pdf/Data_Sheets/MPM-1000%20IP%20Modem.pdf, accessed on June 12, 2013.
[95] David C. Arnold and Peter L. Hays, "SpaceCRAF: A Civil Reserve Air Fleet for Space-based Capabilities," *Joint Forces Quarterly*, Issue 64, 1st Quarter 2012, p. 30.

proportionate share of the global constellation. If a hosted payload approach is used, partners could allow the United States to host protected payloads on their satellites as payment in kind.

The addition of Asia/Pacific partners to the middle tier of the architecture would be mutually beneficial in several ways. It would:

- Help offset the costs of fielding more protected payloads for the United States and would be less expensive for partner nations than developing a comparable capability on their own;
- Improve interoperability between the United States and its partners, as well as interoperability among the partner nations;
- Improve the capabilities of partners to operate independently in a more contested communications environment; and
- Complicate the planning of potential adversaries because an attack against any protected satellites or hosted protected payloads would be an attack against all of the partner nations in the network and thus run the risk of horizontal escalation.

The addition of Asia/Pacific partners to the middle tier would complicate the planning of potential adversaries because an attack against any protected satellites or hosted protected payloads would be an attack against all of the partner nations in the network.

Such an arrangement would need to overcome various political and operational challenges, but it is not without precedence: Canada, the United Kingdom, and the Netherlands are already partners on AEHF, and Australia shares use of the WGS constellation. Adding additional partners for protected MILSATCOM systems could be a core component of the strategic pivot to the Asia-Pacific region called for in the 2012 Defense Strategic Guidance.

Recommendation 3: Avoid Strategic Cost Traps

Like kinetic missile defense systems, a shoot-back capability on satellites (or escort satellites with a shoot-back capability) would likely cost many multiples of the ASAT weapons they are designed to protect against. While a directed energy shoot-back system would be less expensive per shot fired, it would still increase costs by robbing satellites of size, weight, and power that otherwise could be used for mission payloads.[96] If the United States pursues a shoot-back or escort satellite capability, an adversary can impose costs by simply building more ASAT weapons and driving the United States to spend disproportionately more on shoot-back capabilities. Likewise, if the United States chose not to employ active defenses in space and instead procured replacement satellites for rapid replacement in the event of an attack, an adversary could build more ASAT weapons and force DoD to buy even more replacement satellites.

The United States can avoid falling into this strategic cost trap by steering the competition in a more favorable direction. Kinetic ASAT threats—particularly direct ascent systems—tend to be more attributable than other forms of attack. Where the attack is attributable, deterrence can potentially work—provided the risks and potential consequences for an adversary are sufficient. For example, instead of developing shoot-back capabilities in space, DoD could invest in improving its capability to attack the source of ASAT threats on Earth. The United States could also raise the consequences of an attack on space systems by bringing more partners into military space programs and hosting payloads on satellites belonging to partner nations, as recommended earlier. The goal of such efforts should be to steer adversaries to invest in other forms of attack, like electronic and cyber, where the U.S. military can compete on more favorable terms.

[96] A directed energy weapon in space would be limited in the rate of successive shots by the power constraints of the host satellite. A directed energy weapon powered by solar arrays would likely need a significant recharging period between shots, and thus could be easily overwhelmed by multiple ASAT weapons and/or decoys.

Recommendation 4: Avoid New Program Starts

One of the lessons from the TSAT program's demise is the inherent risks involved in new programs. These risks include: technological uncertainty from the incorporation of new, immature, or unproven technology; cost and schedule uncertainty involved in estimating the development effort required for systems that have never been built before; and acquisition uncertainty for competitively awarded development and production contracts where award decisions can be appealed and overturned, resulting in costly delays and re-competes. In the current strategic and budgetary environment, the military cannot afford another failed MILSATCOM program.

To resist the temptation to begin specifying new capabilities with each new contract award, the Air Force should reduce the staffs of existing program offices.

Rather than attempting to start one or more new programs to fill the gap left by TSAT, the Air Force should leverage current programs, namely AEHF, to build and evolve new capabilities. For example, the Air Force could leverage the existing AEHF communications payload, including the waveform, antennas, modems, and other components, to create a hosted protected payload for tactical users. This would reduce both cost and risk by limiting the amount of non-recurring engineering required and using flight-proven technologies. The Air Force can also keep buying AEHF satellites to replenish the constellation as needed and avoid creating another costly break in production.

The key to making such an approach work is reforming the way the government buys systems, specifically in the area of requirements management. The temptation will be strong to reopen requirements documents and begin specifying new capabilities with each new contract award. To resist this temptation and further reduce overhead costs, the Air Force should reduce the staffs of existing program offices, including government civilians, systems engineering contractor support, and personnel assigned from Federally Funded Research and Development Centers. The benefits of removing personnel from program office staffs are three-fold: 1) it would directly reduce program office costs; 2) it would reduce the number of people thinking of ways to change requirements; and 3) the contractors building the systems could reduce their overhead costs in response because they would not need as many people assigned to interface with program office personnel.

Recommendation 5: Use Competition Where Competition Exists

Another important way to reduce costs and risks is to use competition more appropriately. In a free-market oriented society, competition is often advanced as a universal solution to drive down costs. But the military space sector of the industrial base is not a traditional free market with many buyers and sellers and limited regulation. The military space sector can be more accurately characterized as a monopsony, with the U.S. government as the sole customer and regulator. Moreover, there are a limited number of vendors capable of producing the unique systems, subsystems, and components DoD requires—just one or two vendors in some cases—resulting in a monopsony-duopoly (one buyer, two vendors) or a bi-lateral monopoly (one buyer, one vendor). In these instances, free-market oriented solutions, like competition, can have unintended consequences if used inappropriately.

As the only customer for military-unique MILSATCOM systems, DoD pays the full development costs of these systems through cost reimbursable development contracts or higher fees on fixed-priced contracts. In order to create an opportunity for competition, DoD often pays two or more contractors to develop the same system. This redundant development work adds to the overall program cost. Even if DoD pays for the development work only once and gives the same design specifications to two or more companies, it must still pay for the development of more than one production line. Once development work is complete, DoD often down-selects to a single vendor for production using a competitive process. This effectively ends the competition and grants the winner a monopoly for future procurements of the same system and later creates pressure to begin a new program to allow for more competition. Alternatively, DoD can split the award between competing contractors to maintain the prospect of on-going competition, but both contractors receive a smaller order and neither progresses as far down the learning curve as they would if only one firm were awarded the entire order.

Proponents of competition argue that the additional costs from redundant development work and reduced learning can be offset by the competitive pressure among contractors to drive down prices. A game theory-based analysis of this assertion reveals, however, that the effectiveness of competition in reducing program costs depends on the way a competition is structured and program-specific factors, such as development costs and the total quantity of items procured. In some situations, competition can actually create an incentive for contractors to drive up prices over time.[97]

In MILSATCOM, competition can be an effective tool to drive down costs, improve performance, and incentivize innovation for products where new development is not required and more than one contractor already produces the products DoD needs, such as launch vehicles and satellite buses. For products where only one contractor currently supports DoD, however, a sole source award—while not ideal—may cost the government less overall than an artificial competition that pays a second contractor to perform redundant development work or operate a redundant production line. Ultimately, competition that is not self-sustaining by natural market forces is not healthy for industry or cost-effective for the government.

Ultimately, competition that is not self-sustaining by natural market forces is not healthy for industry or cost-effective for the government.

Several opportunities exist for DoD to use competition more effectively in the acquisition of the next-generation MILSATCOM systems. The Air Force has already made progress opening the military launch market to a new competitor, SpaceX, that independently developed a family of launch vehicles without DoD funding. Using a payload-centric acquisition approach for satellites would enable the military to compete satellite buses separate from payloads. Companies that build satellite buses for commercial or other military applications but do not have expertise in building military communications payloads may be more inclined to bid if the payload is procured separate from the bus. It would also enable the military to sole source either the payload or bus (when appropriate) to avoid forcing an artificial competition.

DoD could use competition more effectively in terminal acquisitions—where the barrier to entry is lower than in satellites or launch vehicles—by pursuing an industry-developed low cost protected terminal. Rather than writing requirements, starting a new terminal program, and paying industry to develop new terminal designs to meet these requirements, DoD could buy industry-developed terminals that pass a standard set of test criteria for basic interoperability. By writing test criteria instead of requirements, DoD can let industry innovate and then buy the best of what emerges.

Recommendation 6: Consolidate MILSATCOM Budgets and Authority

A final recommendation is to reexamine the organizational structure of the MILSATCOM enterprise. As noted in Chapter 2, a key programmatic issue for MILSATCOM is the synchronization of programs across the space, control, and terminal segments. Synchronization is a particular concern for MILSATCOM systems because all three segments of the architecture must be fielded in order for

[97] For a detailed explanation of a game theory-based approach, see Todd Harrison, "The Effects of Competition on Defense Acquisitions," *Defense Acquisition University Research Symposium*, September 2012, available at http://www.csbaonline.org/2012/10/19/the-effects-of-competition-on-defense-acquisitions/, accessed on June 13, 2013.

the system to be fully functional. When a satellite is launched without terminals that can fully utilize its capabilities, for example, it is a wasting asset on orbit. A root cause of synchronization issues for MILSATCOM is that each of the Services independently fund and manage their own MILSATCOM programs.

One solution would be to consolidate MILSATCOM programs, budgets, and operations under one Service. The Air Force would be the most likely candidate to assume this responsibility, since it already manages the largest share of the MILSATCOM enterprise. The other Services could transfer MILSATCOM programs, operational units, and their associated budgets to the Air Force. For example, instead of the Navy and Air Force both having acquisition offices for MILSATCOM satellites, the two could be combined under one organization. The Navy's MUOS program office in San Diego, which manages the development and procurement of narrowband MILSATCOM systems, could be transferred to the Air Force's MILSATCOM Systems Wing in Los Angeles, which already performs the same acquisition functions for wideband and protected MILSATCOM systems. Likewise, operational units for MUOS and WGS from the Navy and Army, respectively, could be consolidated under 14th Air Force. In addition to creating better alignment of authorities and budgets for MILSATCOM and enabling the Air Force to better control MILSATCOM synchronization, these consolidations could also reduce overhead costs and eliminate overlapping roles and missions among the Services.

Final Thoughts

If the U.S. military is committed to a strategy of assured access in the face of A2/AD capabilities, as the 2012 Defense Strategic Guidance states, then the Department must adapt its space systems to operate in a more contested environment. MILSATCOM systems provide core infrastructure services upon which other weapon systems depend. Combat forces at all levels are dependent on MILSATCOM for reliable, global communications in the air, sea, and land domains, and the military's use of MILSATCOM is growing exponentially. A key issue is that the space and communications domains are becoming increasingly contested, and too many tactical users rely on systems with little or no protection. In a constrained budget, however, it is cost prohibitive to increase protected MILSATCOM capacity by starting new programs or continuing to conduct business as usual. For the Department to bridge the gap between the capabilities needed and the funding available, it must fundamentally rethink the next-generation MILSATCOM architecture and be willing to make some difficult trades.