34th Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America
Presented on April 16, 2018

ANALYSIS OF COMMERCIAL SATCOM ALTERNATIVES CLOSING GAPS IN NATIONAL SECURITY SPACE

Richard A. VanderMeulen
Viasat Inc., ric.vandermeulen@viasat.com

Meredith Caligiuri
Viasat Inc., meredith.caligiuri@viasat.com

ABSTRACT

We examine space in context of the Department's enduring mission *"to provide combat-credible military forces needed to deter war and protect the security of our nation. Should deterrence fail, the Joint Force is prepared to win."*[1] Space and cyberspace superiority are essential enablers to this enduring mission. DoD leadership is rightfully challenging current satellite communication procurement and deployment practices to accelerate adoption of emerging technologies at the "speed of relevance"[2].

In alignment with the Department's AoA for follow-on Wideband Global Satcom System communications[3], we examine rapidly evolving private sector Satcom resilience, performance, and affordability in a warfighter context and identify the current and emerging operational gaps these systems close. We directly compare DoD's purpose-built AEHF, WGS, and leased Ku-band Satcom performance relative to private sector high-capacity satellite systems, evaluating resilience, scalability, subscriber density, affordability and investment costs. The results of the analysis show that while DoD continues to use the most expensive and least resilient Satcom services, advanced private sector satellite communications services can significantly advance DoD's enduring mission in all threat vector environments.

By 2021, private sector will add 85 times more capacity than the Department requires by 2030, enabling the DoD to adopt a Hybrid Adaptive Network architecture for users to seamlessly roam across multiple DoD purpose-built and private sector systems. This dramatically improves resilience and deterrence, imposes new costs and denies effects on adversaries, reduces Satcom expense, and enables rapid, easy, and continuous adoption of emerging Satcom capabilities.

The specific actions are: (a) explore and facilitate procuring satellite communications as a service, (b) assess private sector technology trajectories in a warfighter context, (c) deploy multi-mode terminals, and (d) advance Hybrid Adaptive Networking allowing warfighters to seamlessly roam across DoD and private sector networks; significantly enhancing the DoD's enduring mission.

COMMERCIAL SATCOM TECHNOLOGY CROSSOVER

For much of our history, the Department of Defense has been the leader in technology and innovation which resulted in the conventional overmatch that our nation has grown accustomed to. This is no longer the situation. Ash Carter, former Secretary of Defense, noted that when he began his career "most technology of consequence originated in America, and much of that was sponsored by the government, especially the Defense Department. Today, much more technology is commercial. And as many of you know, the competition is global. Lots of other countries are trying to catch up with our advances, the ones we've enjoyed for decades in areas like stealth, and cyber, and space."[4]

The present reality is private sector technology innovation and investment has surpassed that of the government and continues to accelerate at a pace much faster than the DoD. The private sector is being driven by market pressures requiring exponential innovation and performance enhancements to stay ahead of global competition. In the specific case of private sector Satcom, the industry is in a period of significant innovation

fueled by the need to competitively serve a very large global market for Broadband. There are established American and International companies, plus multiple startup companies, all pursuing the opportunity to serve passengers on over 40,000 commercial aircraft, passengers and crew on over 150,000 maritime and shipping vessels, innumerable enterprises, and over four-billion underserved and unserved homes/individuals all on a global basis. As shown in Exhibit 1, the private sector now clearly leads technology development in the communications and cybersecurity technology sectors and this technology is being integrated into the fabric of everyday life, changing society and ultimately changing the character of war.

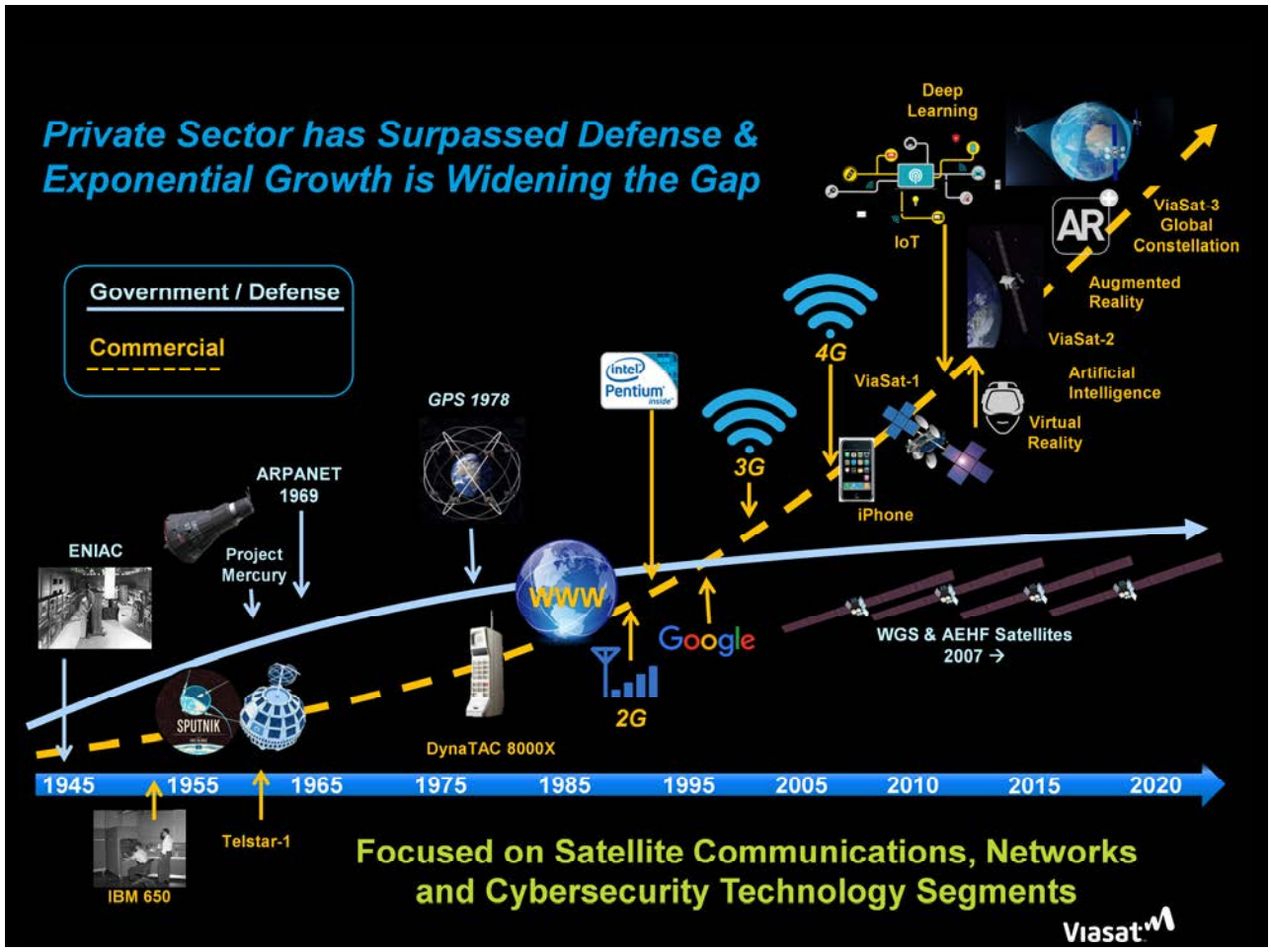

Exhibit 1: *For over 50 years, the government and Department of Defense drove technological innovations that have benefitted not only our security, but our entire society in space, internet, and GPS. Today, the private sector has surpassed defense innovation and is accelerating its rate of innovation widening the gap.*

As an example, two private sector Satcom companies have fully funded Satcom systems that are on contract and in production which will add more than triple the total capacity of all global private sector and military satellites on orbit today. The 2018 National Defense Strategy summarizes this state of affairs and discusses how the Department should view capabilities for the warfighter "Success no longer goes to the country that develops a new technology first, but rather to the one that better integrates it and adapts its way of fighting."[5]

RAPID COMMERCIAL SATCOM ADVANCEMENTS THAT CHANGE THE CHARACTER OF WAR

The Department of Defense has traditionally relied on the concept of "pools of bandwidth" generated by their own purpose-built satellites and supplemented that with private sector ad-hoc bandwidth leases for its Satcom needs. In both cases the "pools of bandwidth" are dressed with networking, including gateways and fiber backhaul, creating DoD-operated Satcom networks. In addition, the DoD process requires warfighters to generate a Satellite Access Request (SAR)/Gateway Access Request (GAR) more than 30 days in advance of their mission[6] based on operational need and then wait for access permission to be granted based on a priority scheme.

In the private sector Satcom industry, this traditional model of undressed bandwidth procurement via purpose-built satellites or bandwidth leasing is being rapidly supplanted by an end-to-end "Satcom as a Service" model. The "Satcom as a Service" model enables procurement of unlimited broadband data and ad-hoc operations directly from the end-to-end Satellite owner, operator, and service provider. In this new market approach, the end-to-end Satellite owner, operator, and service provider is targeting unlimited broadband at market affordable pricing to the consumer, enterprise, and government markets. This change in both markets served and business model is driving rapid improvements in performance, resiliency, and affordability of these private sector Satcom systems. The same technical innovations which dramatically increase the amount of capacity available in a given Satcom system, Exhibit 2, also directly improves performance in the form of end-user

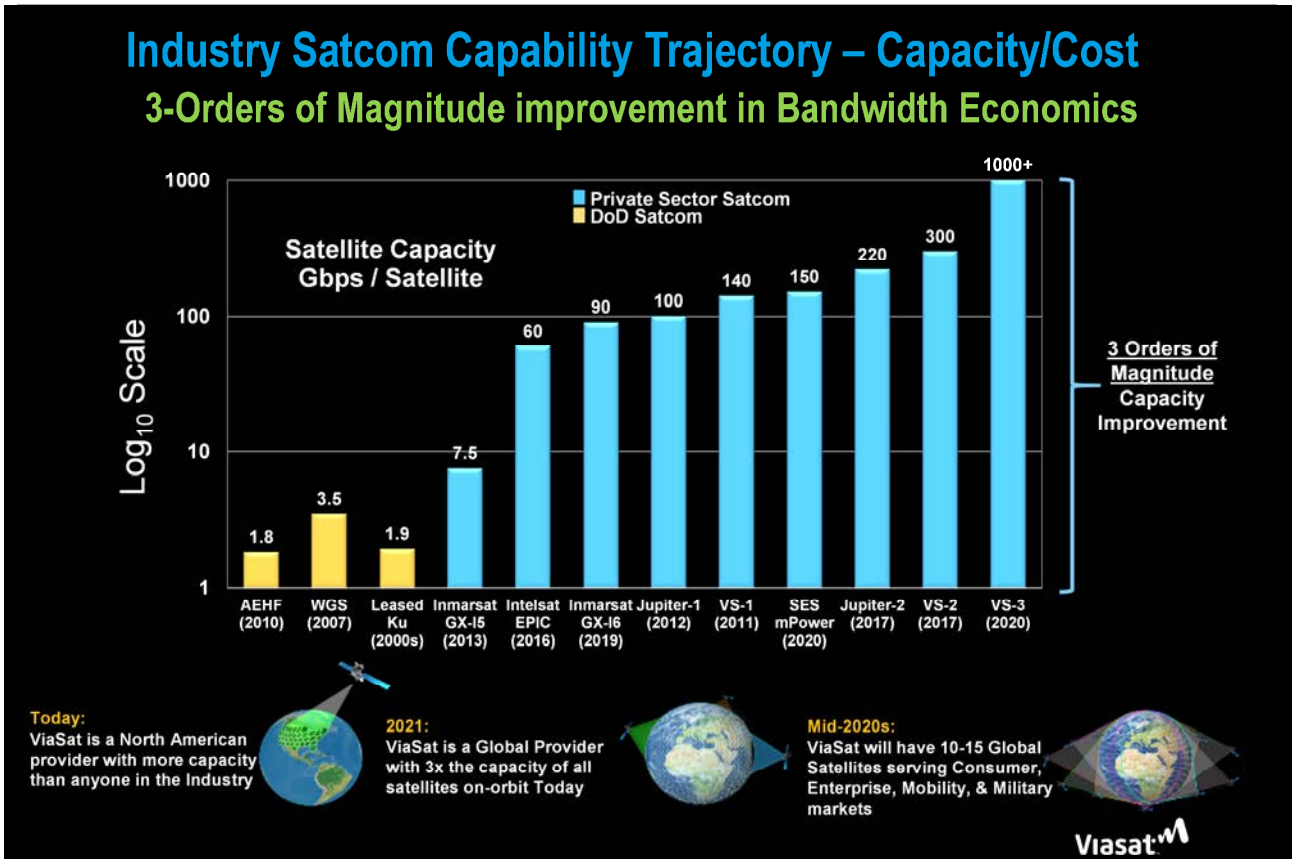

Exhibit 2: *In less than a decade, or the typical development time of a Department of Defense purpose-built satellite, private sector Satcom innovation has approached 1000-fold improvement in Satcom capacity, performance, resilience, and cost.*[7]

speed and data volume or caps; improves resilience in the form of anti-jam protection, teleport exploitations, and cyber-defenses; and improves affordability. Commercial, Enterprise, and Government customers are employing

these capabilities with service level agreements providing performance and resilience that exceeds those of the DoD's at a much more affordable price.

A good example of the improvements in end-user performance is Viasat's recent announcements offering (1) unlimited data plans with speeds up to 100 Mbps for consumers; (2) hundreds of Mbps of in-flight connectivity services per aircraft for commercial airlines, business jets, and high-value government aircraft; and (3) up to 1-Gigabit per second (Gbps) speeds for use in maritime, oceanic and other corporate enterprise applications such as oil and gas platforms.[8]

The same technology innovations that provide higher speed service, unlimited data plans, and market competitive affordability into the broadband market can be used to improve the DoD's enduring mission with increased performance, resiliency against current and emerging adversary threat vectors, and improved affordability. Exhibit 3 introduces the improved warfighter performance, or end user terminal data rates that should be expected in benign, contested, and even nuclear scintillated environments. DoD end-user terminals and platforms should be operating with speeds equivalent to or better than those provided to the equivalent commercial user; e.g. broadband consumers, commercial airlines, business jets, oil and gas platforms, cruise ships, and other corporate enterprise applications. These capabilities can be delivered at prices significantly less than is spent today for services that are at least an order-of-magnitude less capable in speed, capacity, and resilience.

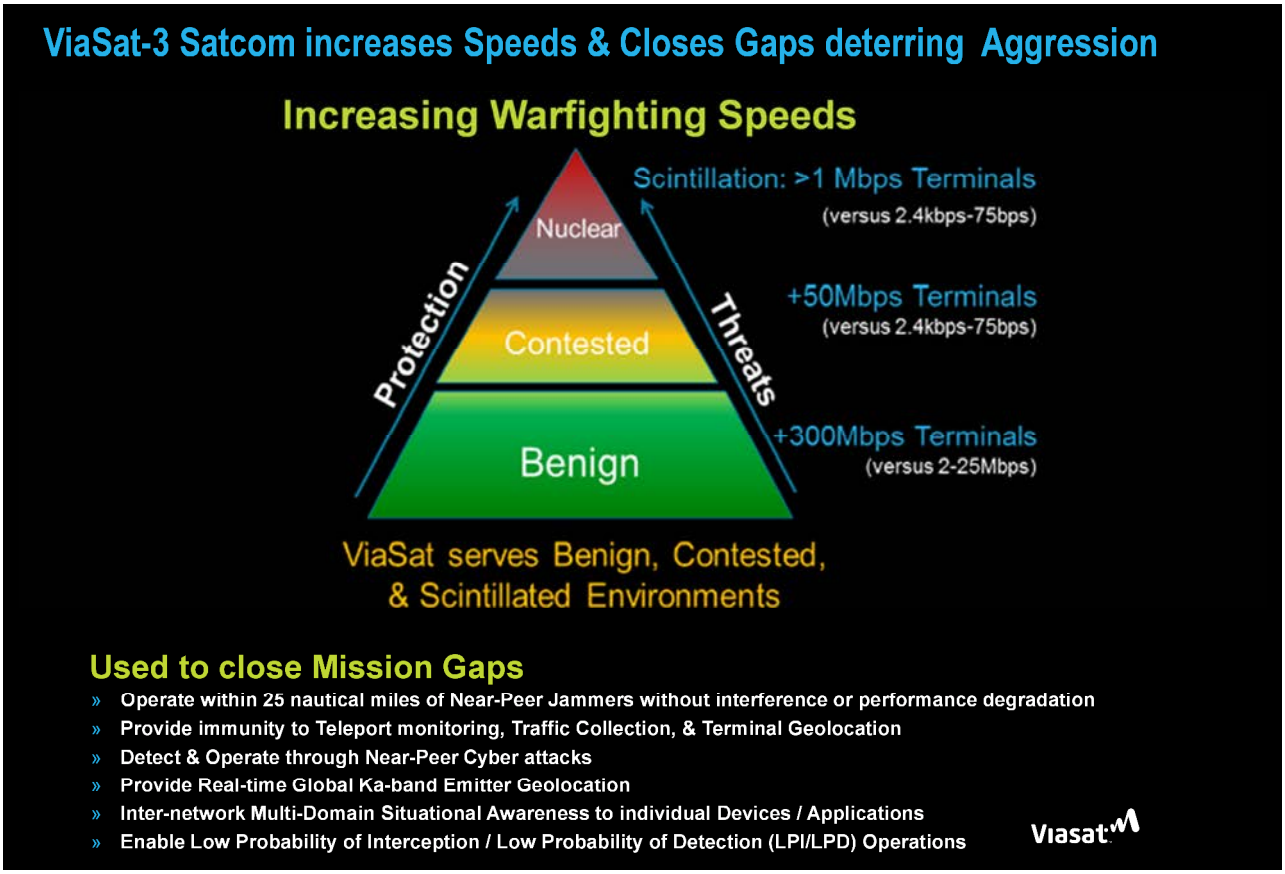

Exhibit 3: *The technology innovation used to dramatically improve capacity economics, or capacity per satellite, enables service providers to provision services at much greater speeds with unlimited data plans, at dramatically more affordable marketing competitive pricing, while also closing many of the operational gaps that exist in using existing Department of Defense purpose-built satellites and leased bandwidth.*

Today, ground-breaking private sector Satcom systems are globally available from multiple end-to-end "Satcom as a Service" providers. The mere adoption of Satcom services from any of these end-to-end Satellite owner, operator, and service providers will immediately enhance resilience and mission assurance for joint warfighters over what is provided by the Satcom systems employed today. Adoption of these new capabilities imposes added cost to adversaries; while simultaneously denying the adversary the ability to interfere with U.S. Satcom, thereby strengthening deterrence and increasing lethality. These benefits are a consequence of private sector competitive innovation seeking to serve very large markets and demands for fixed, mobile, and global broadband communications. In addition, commercial customers have a growing expectation that Satcom-based broadband will provide broadband services comparable to terrestrial providers at competitive pricing.

RESILIENCE PERFORMANCE ANALYSIS

Adversaries continue to exhibit both the willingness and a growing ability to put our government space and cyber systems at risk. Department of Defense purpose-built Satcom systems often take 7-10 years to acquire, develop and deploy, and are very difficult and expensive to modify/upgrade once deployed; private sector satellite communication systems can be conceived from scratch and deployed in under 5 years, and employ flexible architectures and DevOps concepts that allow for rapid modifications, upgrades, and near-instantaneous response to security concerns. This ability to modify/upgrade/improve much faster than the DoD has led to private sector Satcom surpassing the performance and resilience of DoD purpose-built and leased Satcom systems. Therefore, a key element of the DoD's space strategy must include adoption of these innovative private sector systems to deter aggression and warfighting in the space and cyber domains.[9]

Over the past decade private sector Satcom service providers have invested significant capital to harden their satellites and networks against scintillation, electromagnetic interference and cyber threats to secure their C2 up/down links, reduce single points of failure in teleport and ground infrastructure, and to automate their operations, maintenance, and cyber security processes. These investments have led to exponentially improved hardening, security, and operating concepts based on current and emerging threats to their business and operations models.

State of the art of satellite communications networks have progressed from satellites that were capable of delivering roughly 5Gbps and could support hundreds or thousands of users, to satellite systems in 2020 that will provide well over 1Tbps of capacity and support tens of millions of simultaneous users—a 3 order of magnitude improvement over roughly 15 years (the average lifespan of a DoD purpose-built asset). In the 2020s, the private sector trajectory will undoubtedly field Satcom systems that boast 10Tbps or 100Tbps throughputs.

The generation of Satcom systems the DoD uses today, including leased Ku-band, WGS, and AEHF, are based on designs that were completed in the late 1990s/early 2000s. These then state-of-the-art generational designs were optimized for wide area coverage and strategic force structures present prior to the pervasive multi-polar space and cyber threats being contended with today.

In support of the Department, we created a direct performance measured comparison of the DoD's purpose-built and leased commercial Satcom services and private sector high-capacity satellites (HCS) Satcom services. This comparative analysis used a combination of cost and resiliency factors. The data used in this analysis is based on publicly-released data for DoD purpose-built and leased Satcom; as well as for the private sector Satcom systems, with the exception of the Viasat circa 2025 data which includes capabilities known internally to Viasat.

The space cost metric was computed based on publicly released source data on the cost of the various satellite systems, including satellite, launch, and insurance (if applicable), combined with the network or satellite capacity. The resulting metric is expressed in number of Mbps generate per million dollars of investment cost, or Mbps/$M. This is very relevant metric, since the nature of private sector companies is to create a positive return

on invested capital; thus, the cost to generate bits is linked to the speed and quantity or capacity of bits that are provided to a customer at a given price. Generating more bits per invested dollar is the enabler to providing greater end-user speeds and unlimited data plans at affordable pricing.

The resilience metric was also computed using publicly-released source data evaluating criteria and standards required for users to sustain communication in different environments in the presence of current and emerging threats. The resulting metric is expressed as a percentage against the various resilience criteria and standards such that the higher percentage score would present more resilience in the presence of current and emerging threats. The resilience analysis established objective criteria or standards for the rejection of interference, acquisition and operation of space and terminal segments in a denied GPS environment, defense against cyber-threats, immunity against teleport monitoring and collections, defense against kinetic or non-kinetic threats, ability to enable low probability of intercept/low probability of detection (LPI/LPD) network operations, performance in scintillated atmospheric conditions, operations in very high subscriber density deployments, and even future unanticipated threats.

Exhibit 4 and Exhibit 5 provide a summary of this analysis both graphically and in a tabular format. In order to graphically show the breadth of DoD and private sector systems on a single graph, two scales for the cost metric are required since the Satcom systems range from highly unaffordable or expensive systems that generate only a few Mbps per million dollars of investment, to Satcom systems generating over 8,000Mbps (i.e. 8.1Gbps) per million dollars of investment. To serve the broadband market demand with both speed and unlimited capacity or data volume requires that these private sector systems generate the most bits for a given investment as one of their key dimensions of value, namely affordability.

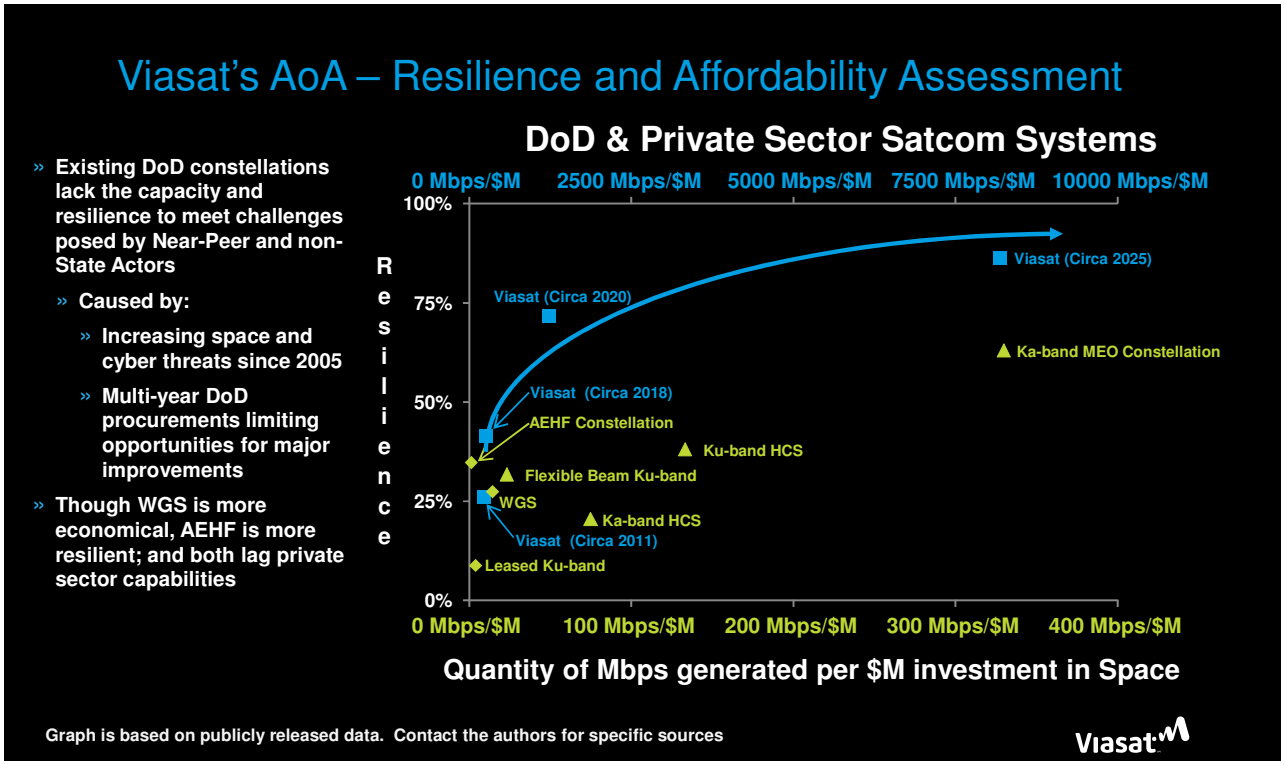

Exhibit 4: *Current and emerging private sector systems are able to generate orders-of-magnitude more capacity for the same investment with a trajectory to provide better resilience against current and emerging threats, while the Department of Defense continues to acquire the most expensive path for the US taxpayer and does not evaluate the private sector promise for improved resilience for the Warfighter.*

Since the 2015 NDAA, the Department of Defense has been encouraged to trial or experiment with pathfinders and pilots to improve their understanding of the acquisition and performance capabilities of private sector systems. To date the pathfinder and pilot efforts have been focused on the DoD's acquisition of leased Ku-band bandwidth, which as shown in Exhibit 5, is the most expensive and least resilient system for providing Satcom services.

Any perceived or real adversarial gains against the DoD's purpose-built and leased Satcom services is essentially offset by length of time that these systems have been in use. Current purpose-built designs, as well as their ground and end-user terminal segments, are a result of multi-year production programs using designs dating to 2005 or before: at least 3 generations old compared to today's fielded private sector designs. In contrast, private sector systems have gone through multiple generational upgrades, reflecting the continual market-driven design and capability improvements demanded by the market.

***Exhibit 5**: Resilience and Capacity: Private sector Satcom has surpassed DoD purpose-built and use of leased Ku-band Satcom.*

Satcom System	Resilience	Cost (Mbps/$M)
AEHF	35%	1.5 Mbps/$M
DoD Leased Ku-band	9%	4 Mbps/$M
WGS (1-3)	23%	6 Mbps/$M
WGS (4-7)	25%	10 Mbps/$M
WGS (8-9)	27%	14 Mbps/$M
Flexible Beam Ku-band	32%	23 Mbps/$M
Ka-band HCS	20%	75 Mbps/$M
Ku-band HCS	38%	133 Mbps/$M
Viasat (Circa 2011)	26%	232 Mbps/$M
Viasat (Circa 2018)	41%	267 Mbps/$M
Ka-band MEO Constellation	63%	330 Mbps/$M
Viasat (Circa 2020)	72%	1241 Mbps/$M
Viasat (Circa 2025)	86%	8192 Mbps/$M
Scale	< 10 %	2005 Market (~ 5Mbps/$M)
	11- 39%	≤ 10 x better
	≥ 40 %	≥ 10x better

Many of the technology innovations created to improve Satcom broadband performance directly enhance resilience, elements of deterrence, and the mission assurance for the DoD's Satcom/DoDIN networks. For example, technologies like geographic gain discrimination to limit interference from beams using the same frequency reuse plan plus aggressive frequency reuse, both increase total system bandwidth and in-beam capacity while also reducing the effects of current high power interferers or jammers.

Key elements of resilience that have been introduced into private sector designs to meet competitive market forces and demands include:

- Interference Rejection (A/J) via Beam Roll off Rejection
- Interference Rejection (A/J) via Nulling and Processing Rejection
- Interference Rejection (A/J) via Bandwidth Rejection
- Immunity to Teleport Monitoring, Traffic Analysis, and Terminal Geolocation
- Operations in the presence of near-peer cyber threats including known attack vectors and behavioral analysis to identify and counter new attack vectors
- Operations in very high Subscriber Density Deployments (i.e. very high capacity in a small regional location).

When these new elements of resilience are introduced into the DoD's Satcom services, with the corresponding upgrades in the end-user terminals, advances to the DoD's enduring mission could include capabilities including:

- Operations in Denied GPS Environments with independent of GPS-based PNT
- Ability to deter Kinetic/Space-based attacks with multi-path layered services often employing a variety of different defense mechanisms

- Operations enabling Low-Probability of Intercept/Low-Probability of Detection terminals
- Operations in Scintillation without heavily degraded data rates
- Ability to perform Geolocation of emitters
- Multi-domain Situation Awareness.

Private Sector and DoD Satcom Service Assessment

The goal of the 2018 National Space Strategy to transform to more resilient space architectures directly supports the DoD enduring mission.[10] To this end, several private sector Satcom service providers have stated that they have systems that exhibit better resilience against current and emerging threats than the systems currently employed by the DoD.[11, 12] To date these private sector performance statements have not been formally assessed and measured in combat-like conditions against a scorecard. Evaluating and assessing the resiliency capabilities and attributes of private sector and purpose-built DoD networks will allow the DoD to understand a) which networks are capable of meeting DoD specified resilience requirements and b) provide the framework for constructing Service Level Agreements that define the effectiveness of the service network for meeting each of the resilience categories. The quantitative measurements provided in Exhibit 6 allow for a systematic and consistent evaluation against existing and future networks that would allow the DoD to ensure the Hybrid Adaptive Networking is constructed with the most resilient options within each service area.

***Exhibit 6**: Thoroughly and quantitatively assess private sector Satcom services and technology trajectories in a warfighter resiliency context.*

Resilience Category	Measure of Effectiveness
Interference Rejection (A/J) via Beam Roll off Rejection	1) The average distance (in degrees) of the -3dB gain contour from beam center 2) The ratio of the distance from the center of the beam to the average distance (in degrees) of the -3dB contour to the distance from the center of the beam to the -30dB contour (i.e. the 1000-fold suppression contour)
Interference Rejection (A/J) via Nulling and Processing Rejection	1) How deep are the in-beam nulls that the system is capable of producing (and the corresponding resolution of the nulls) in dB 2) The width of the nulls (in degrees) at +10, +20, and +30 dB relative to the depth of the null 3) Total number of nulls the system can crate, and/or the ratio of the number of in-beam nulls that the system can produce to the number of beams in the system
Interference Rejection (A/J) via Bandwidth Rejection	1) Amount of spectrum available to the satellite system (GHz). 2) Amount of spectrum that the system can place in a single beam (GHz) 3) Amount of spectrum that can be received and/or transmitted by a single terminal (if different than (2))

***Exhibit 6**: Thoroughly and quantitatively assess private sector Satcom services and technology trajectories in a warfighter resiliency context.*

Resilience Category	Measure of Effectiveness
Operations in Denied GPS Environments	1) Duration system can remain operational without the use of GPS at the user terminal 2) Duration system can remain operational without the use of GPS at the Hub/Gateway 3) Duration system can remain operational without the use of GPS (satellite(s)) 4) Ratio of system throughput without GPS to system throughput with GPS
Operations in presence of Near-Peer Cyber attacks	1) Number of Cyber security accreditations: CNSSP No 12, NIST800-52, ISO-27001, etc. 2) Response time (Seconds) to identify DDOS attack of 100Mbps/sec or greater 3) Response time (Seconds) to modify routing to mitigate DDOS recognized DDOS attack 4) Size of a DDOS attack the system can operate through without impacting performance 5) Measured ability to recognize and halt known attack signatures 6) Time to recognize a behavior change in both network operations and network traffic
Immunity to Ground Teleport Monitoring, Traffic Analysis, and Terminal Geolocation	1) Proximity to ground site (km) that would enable teleport monitoring (within -3dB; refer to measurements in the "Interference Rejection (A/J) via Beam Roll off Rejection" section) with similar G/T receiver as system gateway 2) Percentage of uplink/downlink data stream that can be monitored, analyzed or used for data collection or geolocation from a single ground site 3) Number of independent communications paths between gateways and meet-me points
Deter Kinetic/Space-based attacks with Multi-path Resilience/Obscuration and/or Defenses	Number of space assets in a single theatre
Operations enabling LPI/LPD end-user terminals	1) Maximum spectrum available for use by a single terminal (GHz) 2) Support for Direct Sequence Spread Spectrum Waveforms (yes/no) 3) Support for Frequency Hopping Spread Waveforms (yes/no) 4) Minimum operational C/N for system.

***Exhibit 6**: Thoroughly and quantitatively assess private sector Satcom services and technology trajectories in a warfighter resiliency context.*

Resilience Category	Measure of Effectiveness
Operations in Scintillation	1) Interval to detect (seconds) scintillation effects (attenuation & phase distortions) 2) Dynamic Range (in dB) available to system to mitigate amplitude attenuation 3) Interval (in seconds) to modify operating point in response to amplitude attenuation 4) Interval (in seconds) to compensate for phase distortions 5) Interval (in seconds) to modify system avoid frequencies affected by scintillation 6) Geographic localization (in km^2) of detection and response to scintillation effects.
Operations in High Subscriber Density Deployments	1) Capacity density in a pre-defined perimeter (Mbps/km2) 2) Amount of capacity that can be provided to a single user in Mbps
Geolocation of Emitters	1) Error of the actual to measured location of the emitter source in km. 2) Time required to geolocate emitter (seconds)

Summary and Observations of the Resilience Performance Analysis

General (retired) William Shelton, former Air Force Space Command Commander, deftly described how "we expect our local power company to continuously provide the power we need to heat and cool our houses, and to run our myriad electrical devices. When a power outage occurs, we are outraged and quickly call the power company demanding to know when service will be restored. Space services are now a utility as well."[13]

As we think of space services as a utility, especially layering DoD and private sector systems, the value of approaching Satcom as a Service for the DoD's broadband needs will provide a greater degree of mission assurance under all conditions and enable accelerated access to advanced private sector Satcom layers for greater capacity and resiliency.

Considering the performance advantages in Exhibit 3 and the resilience/cost analysis in Exhibit 4 and Exhibit 5, our Analysis to achieve the DoD's enduring mission, to deter war and if necessary win, at the "Speed of Relevance", has identified several compelling observations.

1. The DoD's enduring mission will not be enhanced until the DoD employs Satcom with higher resilience against current and emerging adversary threats. Alternatively, continuing to use the systems first put into use in 2007 or before will only further erode the DoD's enduring mission.
2. In order to employ more resilient Satcom, the DoD will need to make changes, i.e. modification or replacements, to the terminals the DoD has deployed and uses.
3. Terminals that support multi-network operation (i.e. multi-vendor and/or multi-band) immediately and significantly add resilience while enabling incremental upgrades to the installed terminal base thus preserving interoperability. This will reduce cost and significantly enhance the DoD's enduring mission to deter war, and if necessary win.

4. Private sector Satcom suppliers are already employing multi-band and multi-network terminals to ensure uninterrupted access to broadband connectivity as they roam on a global basis.
5. Private sector Satcom suppliers are already employing Enterprise Management Systems enabling seamless roaming across multiple satellite networks and even multiple bands within their regional and global networks.
6. Private sector Satcom services supporting global air mobility and roaming are immediately, starting in 2018, available to evaluate, demonstrate, and employ multi-band and multi-network roaming. This will immediately and significantly enhance the DoD's enduring mission.
7. Pathfinder funding, like Pathfinder #4, currently intended to pool another 5-years of leased Ku-band capacity, could be used to immediately "pilot" acquisition models to buy "Satcom as a Service" to initiate multi-network roaming and growing into hybrid networking.
8. Pilot funding could immediately, starting in 2018, assess private sector Satcom services and technology trajectories, thoroughly and quantitatively in a warfighter context including RF, cyber, and kinetically contested threats.
9. Pivoting to any one private sector HTS Satcom service, through simple terminal modifications and replacements, would provide an immediate order-of-magnitude cost or investment advantage as well as improve resilience. This could start in 2018.
10. Continued investments in Protected Tactical Service/Protected Tactical Waveform (PTS/PTW) for use on Leased Ku-band will not effectively improve resilience. Their narrow 36MHz channel allocations and wide-beam architecture, allows jamming or interference to be effective from 1000s of miles down range.
11. Continued investments in DoD purpose-built solutions with upgrades including PTS/PTW provide only small incremental resilience improvements at significant investments and continue the DoD's dependence on the most expensive Satcom services.
12. Hybrid Adaptive Networking enables a pivot from acquisition-based competition which lies on the government technology trajectory to market based competition which lies on the private sector exponentially improving trajectory to enhance the DoD enduring mission at the speed of relevance.
13. The most cost effective and timely way to adopt private sector Satcom services while maintaining and encouraging further innovation is to achieve interoperability with an open standard interface at the network layers. Attempts to specify at the waveform or modem layer will stifle private sector innovation and reduce market based competition, diminishing the benefits of Hybrid Adaptive Networking.

In summary, the **Department is at a crossroads. One path is the continuation of a Satcom architecture that will further erode the DoD enduring mission**, representing the largest burden on taxpayers. The **other path enhances the DoD enduring mission**, increases warfighter Satcom performance in multi-domain operations, increases resilience against the current and emerging threat vectors, and improves affordability therefore reducing taxpayer investments.

HYBRID ADAPTIVE NETWORKING TO ENHANCE THE DOD'S ENDURING MISSION AT THE SPEED OF RELEVANCE

In order to more decidedly improve resilience and deter aggression into space and cyber, immediately, the DoD should adopt a Hybrid Adaptive Networking approach. Between today and the in-service launch of WGS

flights 11 and 12, private sector Satcom service providers, including Inmarsat, SES, and Viasat, will add 4.2Tbps of global Satcom capacity. This is over 285 times more global Satcom capacity than will be provided by these two regional satellites.

In further context, this new private sector capacity is over 85 times more than the projected Department demand by 2030. Since this projected usage is ~1% of the new global capacity and since this capacity is intended to serve the total Broadband market, the DoD could establish pay for usage contracts and roam across all of these and their own networks. The solution would be to deploy a Hybrid Adaptive Network architecture depicted in Exhibit 7 allowing seamless roaming across the full extent of DoD purpose-built and private sector Satcom system.

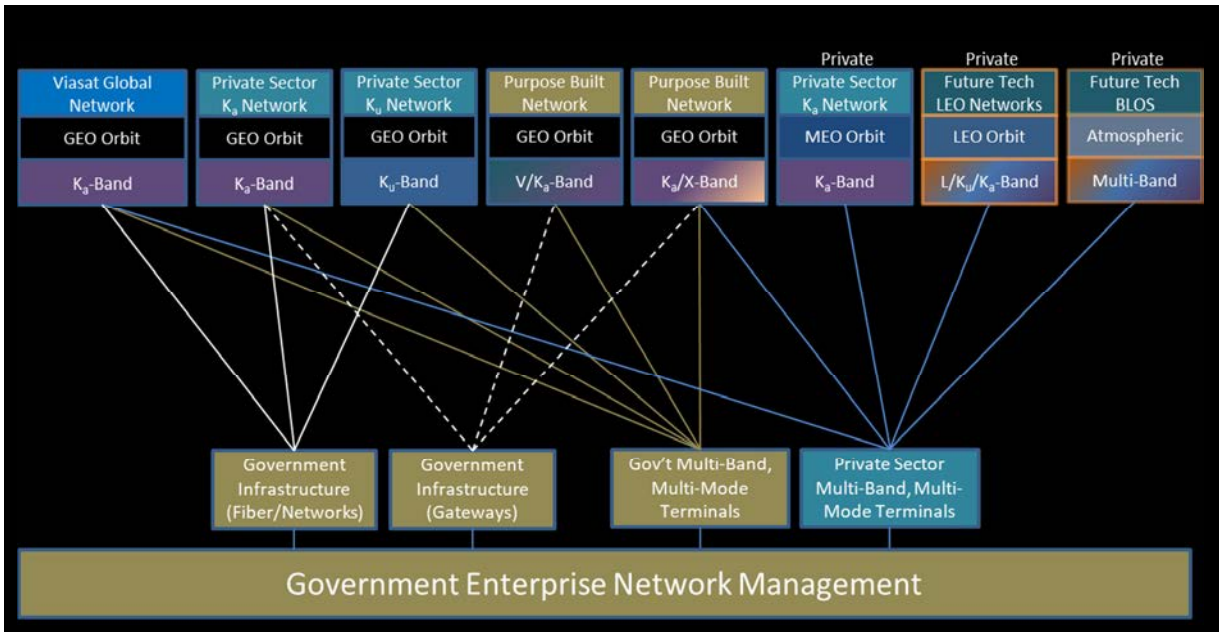

Exhibit 7: *A Hybrid Adaptive Network Allows Government to Use Multiple, Independent Networks as a Single Communication System. This approach addresses growing demand while enabling warfighting contracts of deception and maneuver to be added to the Satcom and Cyber-defense missions.*

Investing in purpose-built systems for unique DoD requirements as a low-risk bridge towards a Hybrid Adaptive Network is valid; however, investing solely in purpose-built systems poses significant risks to warfighter communications, encourages adversary aggression in the space and cyber domains, and levies additional costs on taxpayers without true warfighter benefit. Instead, the DoD can enable a highly reliable architecture with a multi-orbital space asset constellation, integrated cyber defense capabilities, orders of magnitude more capacity, and multi-dimensional resilience through distributed ground sites that are invulnerable to intentional and unintentional interference sources.

To maximize mission assurance, the overall network architecture must consider the entire set of systems comprising the end-to-end communications network. Resilience and mission assurance should be viewed as layered concepts that can be measured in many ways and at varying levels. Individual satellite communication networks have different levels of resilience, based on their system and network attributes. Layering of the individual networks forms a multi-network ecosystem without a single common denominator or attack vector. From the end-user's perspective, the objective is rapid access to a network of networks in which multiple transport options are available at any given time and at any given location, including: multiple transponders or beams from a single satellite; multiple satellites from one private sector provider; multiple Satcom networks from multiple different private sector providers; and a mix of government (AEHF, WGS, leased Ku, etc.) and multiple private

sector Satcom networks. A Hybrid Adaptive Network architecture can maximize overall mission assurance by layering heterogeneous networks with different attributes (e.g. orbital regimes, frequencies, beam sizes, waveforms, gateways, networking protocols, network management and terrestrial networks) into a unified operational environment.

Because of the dynamic nature of threats in the space, ground and cyber domains, there will never be a single system that is fully defensible against all possible threat vectors. Scoring individual systems against defined resiliency capabilities provides a comprehensive assessment for evaluating existing and emerging network attributes. No single network theoretically ever achieves 100% resiliency; thus, combining multiple networks into a cohesive hybrid network will result in the greatest overall resilience possible.

As new private sector and purpose-built networks become operational, each added network to the hybrid network will dramatically improve the overall Hybrid Adaptive Network resilience. As shown in Exhibit 8, as early as tomorrow, Ka-band terminals operating with existing European theater Ka-band networks have a combined resilience more than double the resilience of two WGS. The three constituent networks can be combined to have an overall network resilience score of 56.97% with each of the networks achieving individual resilience scores less than 30%. The resilience improvement available with existing systems highlights the benefits of a layered solution that would make disruption from adversaries significantly more difficult. Adversaries would need the willingness and the capabilities to disrupt multiple systems: space assets, ground sites, backhaul networks, etc.

Exhibit 8: Combined Hybrid Network Resilience for Existing Technologies

Hybrid Network (Circa 2018)	Network Resilience Score
European Ka-band HCS	26%
Ka-band HCS	20%
WGS (8-9)	27%
Overall Hybrid Network Resilience	56.97%
Resilience Scale	< 10 %
	11 - 39%
	≥ 40 %

Evaluating networks that will be operational in the 2020s timeframe, the overall hybrid network resilience will achieve a resilience score that is greater than 94%, greater than could be generated by any of the DoD purpose-built or private sector systems alone (shown in Exhibit 9).

This evaluation further demonstrates that an architecture that employs multi-path layering of interoperable networks will provide the fundamental foundation for providing warfighters the best overall possible network for deterring aggression in wartime situations. Hybrid Adaptive Networking will always offer greater resilience against any possible threat vectors than any single network can.

Exhibit 9: Combined Hybrid Network Resilience for on contract networks available in 2020s

Hybrid Network (Circa 2025)	Network Resilience Score
AEHF	35%
Ka-band HCS	20%
WGS (8-9)	27%
ViaSat-3 Constellation	86%
Ka-band MEO Constellation	63%
Overall Hybrid Network Resilience	94.71%
Resilience Scale	< 10 %
	11 - 39%
	≥ 40 %

Hybrid Adaptive Network Architecture

The critical infrastructure that is central to deploying a global, resilient and integrated network requires a system that (a) allows users to roam across private sector and purpose-built networks and (b) provides operators the ability to manage users, coordinate service and have the situational awareness tools available to respond to issues. To effectively service the users, across all of the multiple layers, requires designing a platform that can meet the following objectives:

1. Both private sector and purpose-built networks should be capable of reporting metrics necessary for detecting threats (Cyber, EMI, and Outages)
2. Allow operators to perform network selection based on the unique requirements for each mission tailored to meet individual mission/warfighter needs
3. Provide the infrastructure necessary to enable users to roam seamlessly across private sector and purpose-built networks within the Hybrid Adaptive Network
4. Allow for flexible adoption of new and advanced service networks to effectively add performance and resilience capabilities.

From the stated objectives, the system architecture and key components depicted in Exhibit 10 are foundational enablers for a Hybrid Adaptive Network that encompass the following attributes:

» A ***network-layer standardized Interface*** is significantly more cost effective than requiring compatibility to modem or waveform specifications. Further it will allow for innovation to continue within the private sector for continued advancement of Satcom technology. Users connect to each other over the Network vs. over the air. This is especially important when responding to local or limited adversary attacks: end-users that are impacted by adversely effects should transition to a new member network(s), while remaining connected to other users, and without forcing other users to also transition.

» ***Enterprise Management System*** provides the real-time visualization and situational awareness processing and tools that operators require for managing users and communications throughout multiple theaters and deployments. The enterprise management system is analogous to a global ISP's network management system that includes fiber, cable, Wi-Fi, cellular transport networks. It is an end-to-end service monitoring and control system rather than a collection of subsystem controllers.

» A ***translation agent*** bridges the standardized interface to the formats used within individual purpose-built and private sector networks. Using a translation agent for maintaining operations allows for the DoD to manage users and have the necessary situational awareness information already available within existing service networks without imposing additional design burdens or stifling innovation throughout the private sector. The technical innovation of the networks does not impede traffic flow, acquisition, or interoperability.

» Future ***multi-network terminals*** able to support multiple modes and multiple bands will allow users to the ability to seamlessly operate across different transport networks (both purpose-built and private sector), further creating an end-to-end network that provides mitigation against: congestion situations, outages (space and ground), intentional and unintentional interference sources, and cyber threats. The private sector has already delivered multi-network terminals, particularly to aircraft and maritime platforms that demand seamless global roaming, and will continue to innovate in ground terminals, with cost and size reductions, etc. The private sector will develop and deliver additional multi-network terminals in response to market demand before a program of record could define, acquire and, field a purpose-built multi-network terminal.

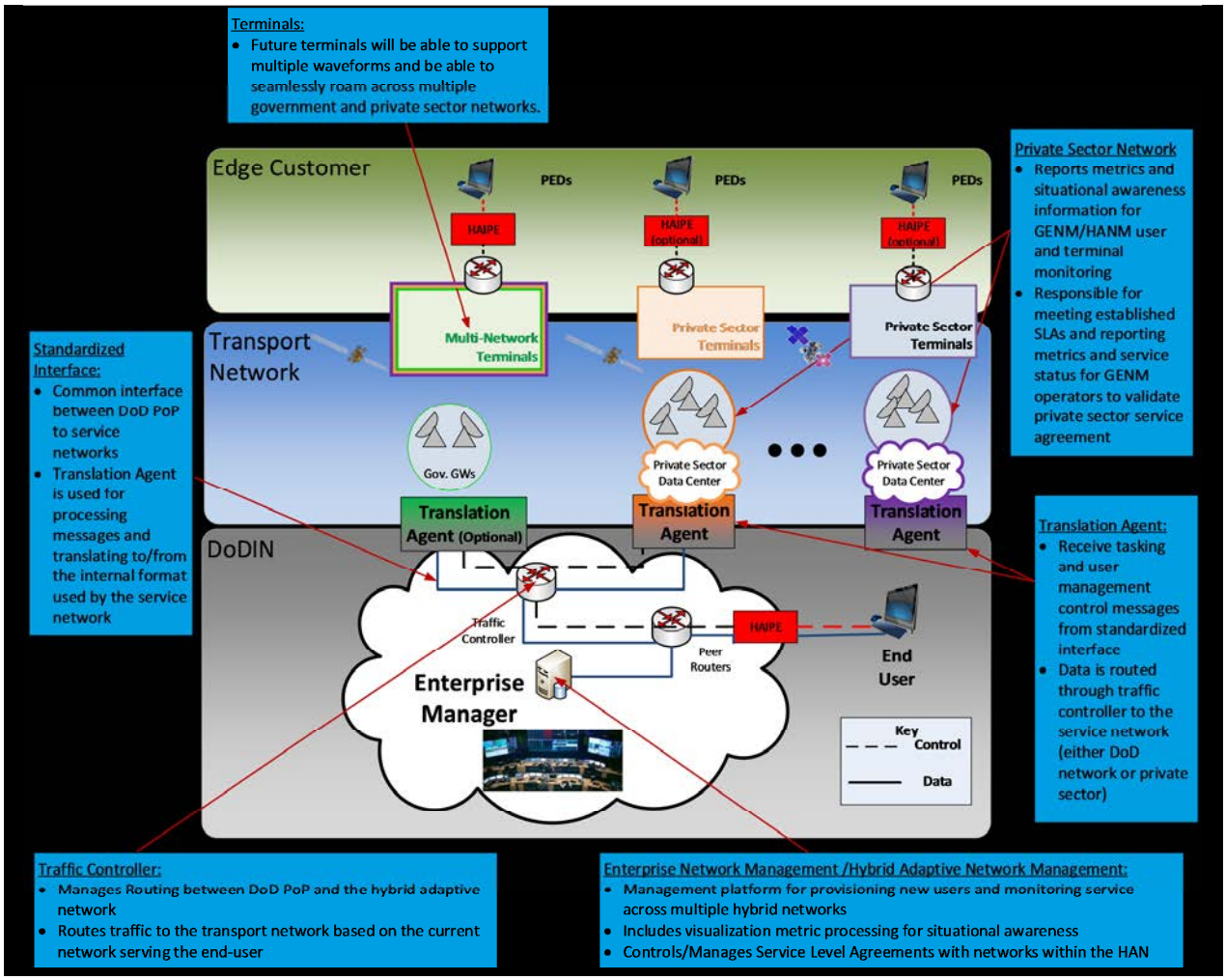

Exhibit 10: *A Hybrid Adaptive Network Allows Government to Use Multiple, Independent Networks as a Single Communication System*

Standardized Interface

Coordination and visibility across multiple disparate satellite networks is possible through a standardized interface to each constituent network that can enable seamless operation, transition, and availability for end-users. Standardizing the interface at the network layer rather than at the terminal or waveform level will allow rapid adoption of future networks into the combined Hybrid Adaptive Network. The interface (Exhibit 11) would include the ability for the Enterprise Network Manager to query each of the networks within the HAN to request service or query network capabilities with each of the networks reporting or advertising their current capabilities. The messaging exchanged across the interface will provide the necessary information for the Enterprise Network Manager to select the appropriate network for individual user operation based on unique mission needs and network capabilities.

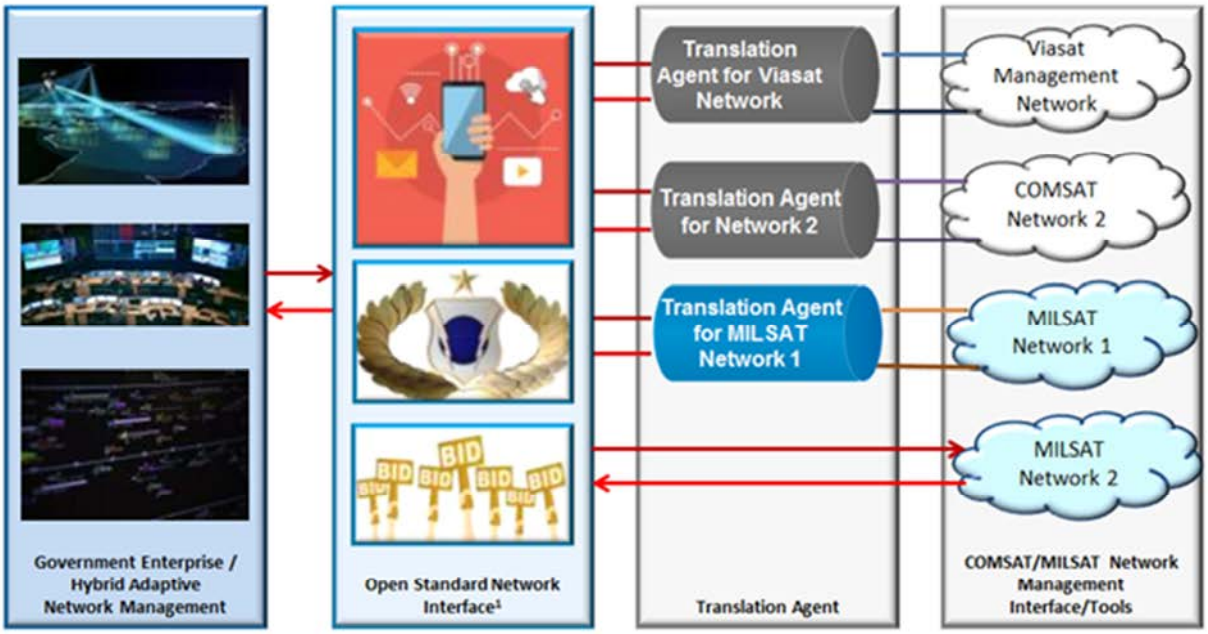

Exhibit 11: *Hybrid Adaptive Networking enables rapid adoption of DoD purpose-built and current and emerging private sector Satcom networks. The Enterprise Management system use of a Standardized Interface at the Network Layer Enables Access to purpose-built and Private Sector networks without further Enterprise Management redefinition.*

Using a translation agent integrated between the service network internal standard format and the standardized interface will allow multiple networks to interoperate with the Enterprise Network Management system for facilitating and coordinating user and service management from a centralized operations facility.

The interface design should be both flexible and scalable for rapid integration of different network architectures to allow market based competition; thereby ensuring the DoD has access to the latest technology at current market value. To maximize interoperability, the interface should be an open standard that could be based on existing or emergent commercial or government standards (e.g. OMS or UCI). Driving compatibility and interoperability at the network level (rather than the waveform or terminal) allows for rapid adoption of new capabilities while creating enduring, market-based competition that prevents vender lock-in. Allowing terminal or waveform specifications to remain unconstrained will further drive technology advancements within the private sector. These technology innovations can then be utilized by warfighters for disadvantaged or emerging operations and missions that would otherwise be limited in service availability.

Enterprise Network Manager

Enabling operations of a Hybrid Adaptive Network requires the introduction of an over-arching management system that allows users to seamlessly roam from one network to another as mission requirements demand. For a heterogeneous network to function globally and in high-density regional theaters, with users that require different mission assurance protections and capacity demands, a centralized Enterprise Network Management system must be in place for coordination and management of the individual transport networks. Some of the elements for architecting a network manager for managing global user groups include:

- *The network manager platform must be both agile and resilient.* In order to react to continuously evolving mission requirements and a changing threat landscape, the network manager must be scalable to support adding additional private sector and DoD networks to the HAN. With a flexible architecture, as advanced technologies come to market, the network manager platform would not require re-definition since it can accommodate any number of global service networks.
- *Real-time situational awareness metrics reporting and tools must provide the visibility and infrastructure for detecting and strategically responding to threats within global environments.* (Exhibit 12) The information and metrics provided by service networks provides operators the ability to make informed decisions in wartime missions to ensure communications remain intact through military operations.
- *Leverage private sector investments in applications and management capabilities.* Many private sector service providers have operational tools and infrastructure for managing service across multiple assets and networks. Any future Enterprise Management System should leverage these existing and emerging hybrid management technologies for network selection, situational awareness monitoring, metric reporting and analytics, and threat intelligence sharing.

Satcom Exchange – Satcom as a Service Acquisition

Employing a "Satcom as a Service" acquisition model will provide the most control of "operational effects" and the most cost effective solution for the DoD since it provides a collection of networks that can be tailored to provide service throughout the world depending on the precise needs of the mission (resilience, capacity, mobility, active cyber defenses, etc.). It will allow warfighters to gain access to global constellations of service from any of the service provider networks within the Hybrid Adaptive Network. This resilient option will continually provide the DoD the ability to leverage the innovative technologies and available capacity provided by the private sector at a more economical cost per Mbps. Since service providers have invested in the development, infrastructure, and operation of future technological capabilities the DoD will be able to utilize these systems to support increasing global bandwidth demands without compromising the overall resiliency of the network. Additionally, because this architecture prevents vendor lock-in, the DoD will no longer be constrained by older legacy systems and long acquisition cycles. Instead, they will be positioned to dynamically and flexibly scale to acquire service on networks that offer the capabilities needed for future missions. As a result, they will also benefit from the decreasing price per bit trajectory that will continue to decline with future commercial HCS available in the mid-2020s as the next-generation systems become increasingly more capable and economical. As shown in Exhibit 13, with multi-Tbps systems, the capital cost of private sector capacity has rapidly declined from $53M to well below $1M per Gbps of overall capacity cost.

Government users can select from a wide-range of service options to meet specific mission needs using service-level agreements (SLA) between the service provider and the end-user (including government users) that define the construct of the service that will be delivered to the end-user. Particular aspects of the service – scope, quality, availability, throughput, and anomaly responsibilities – will be agreed between the provider and the user. The SLA could specify how various traffic classes are treated and other service-level objectives. Additionally, the SLA could also contain agreements between the parties on how to monitor compliance and responses for situations where service-level objectives are not met. For example, if an outage is not corrected by the network operator within the SLA allocated time, then a credit, or other penalty, would be issued towards bandwidth costs for the month.

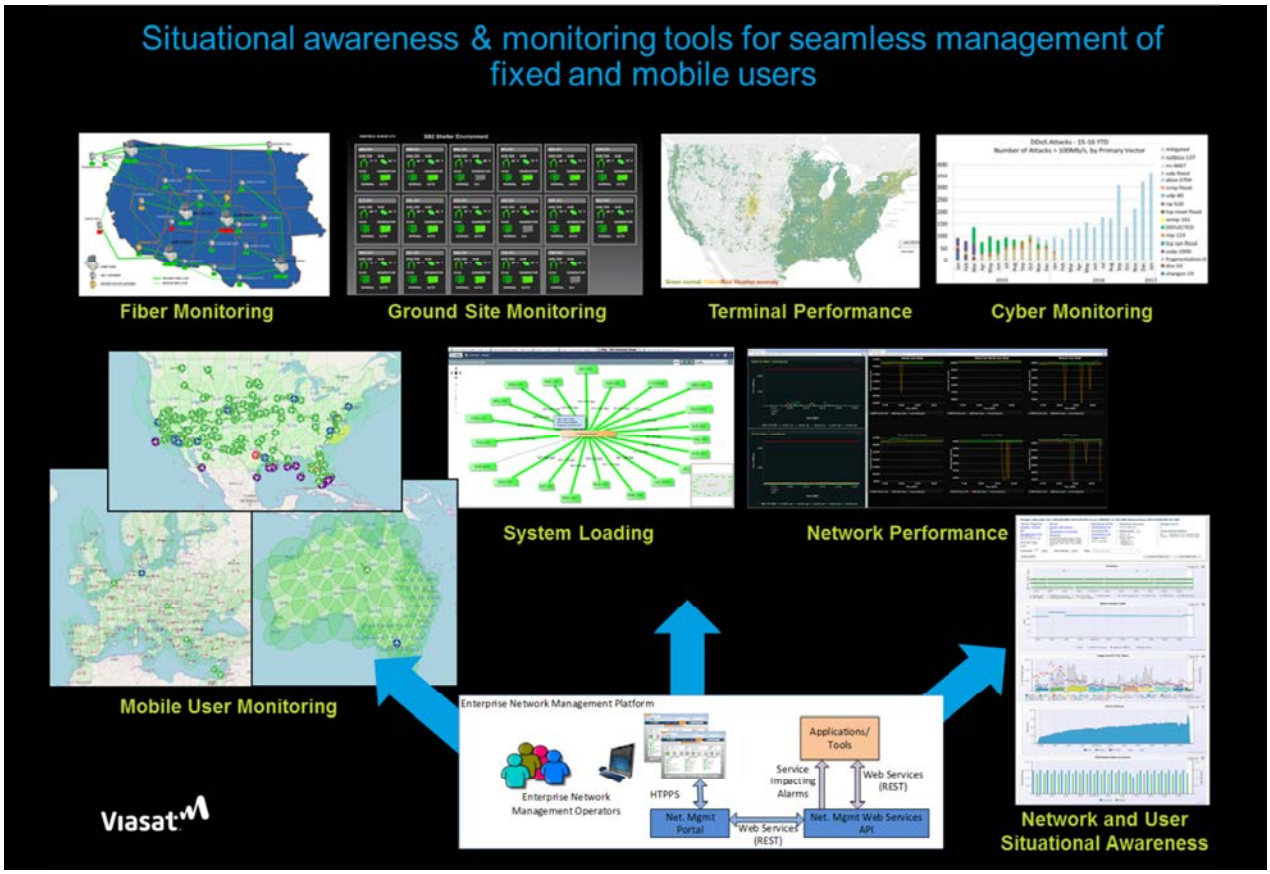

Exhibit 12: *Enterprise Network Manager provides the situational awareness to manage users and missions across global theaters.*

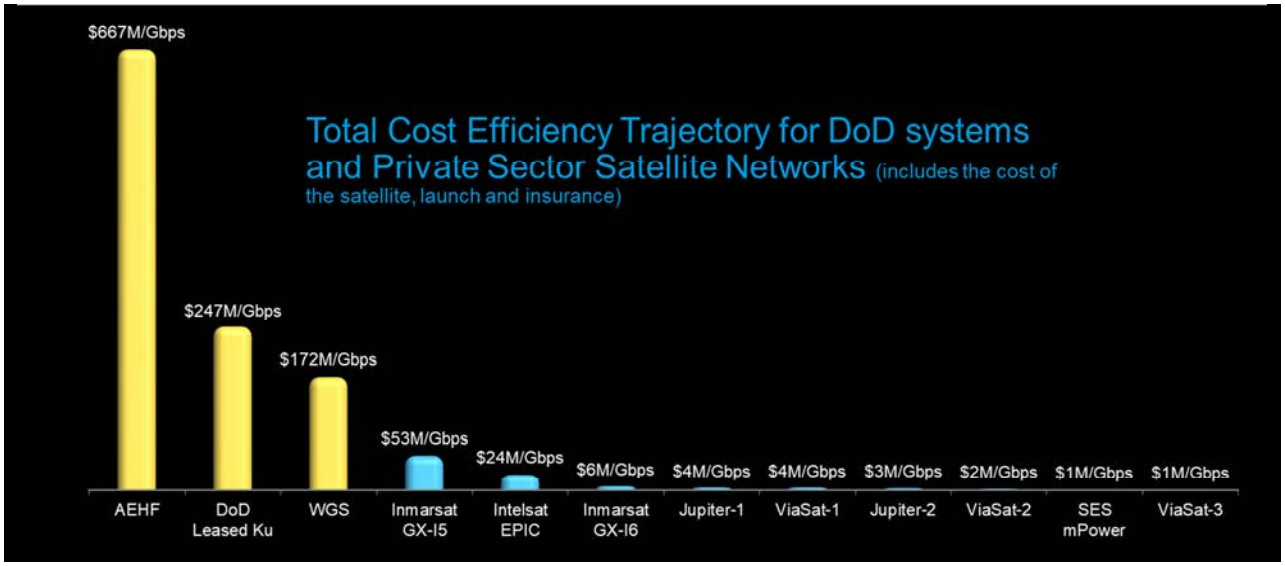

Exhibit 13: *Private Sector Trajectory: The investment cost required to generate a Gbps of capacity is rapidly decline as these systems target the Global Broadband market that demands more capable and economical Satcom to provide Terrestrial comparable performance.*

To meet warfighter needs in global environments the DoD should acquire Satcom as a Service at the network level as part of a hybrid network through the SLA. This will drive intense competition to enhance warfighter

mission effectiveness, constantly improving resilience and mission assurance, reinforcing deterrence against aggression, and gaining developmental and operational cost savings. Satcom enterprise partners can provide bundled capabilities to include support services, network infrastructure, and multi-mode terminals that meet unique warfighter SLA requirements within the Hybrid Adaptive Network architecture. This negates the need to negotiate ad hoc contracts across a range of Satcom providers. An enterprise level contract with SLA options for desired performance, resilience, assurance, and deterrence will reduce cost, time to deliver, and complexity to deliver operational effects.

Service providers offer flexibility for the DoD operators through the standardized interface to provision, request and schedule service that meet individual user demands using blanket purchase orders from a centrally managed Enterprise Management System. The most efficient approach integrates commercial and government network controllers as an aggregated enterprise to allow the government to pay on a burst consumption basis rather than frequency allocation basis.

In acquiring "Satcom as Service" the control aspects move from a RDT&E design specification and test program to desired "operational effects" embedded within the construct of the SLA. The importance of including "operational effects" in the construct of the SLA is to ensure warfighters receive desired or required operational capabilities. The operational effects need to move beyond concepts like Data Rates, committed, peak, minimum usage, etc., and add assured mission performance or Operational Availability (A_0) in the presence of adverse effects, scalability to support fluid operations, and prioritization responsive to mission importance.

The A_0 or assured capacity and speed of service must be assured to each user asset/device even in congested and contested areas of operations where multiple assets must be supported simultaneously in the presence of:

- All Weather conditions
- Teleport outages regardless of cause
- Fiber outages regardless of cause
- Cyber outages caused by previously know or NSA/DHS government-furnished-information (GFI) signatures
- Interference or jamming within an operational range to the jammer (i.e. 25, 50, 100 nautical miles).

The Scalability or always on, always available, and easily scalable to support rapid, unscheduled access must also be assured. When in the defined coverage area, the Satcom service must readily allow any terminal asset to access the network at any time without a priori scheduling.

Prioritization must support prioritized missions/users and automatically prioritize users within the coverage area, both forward link (FL) and return link (RL), assuring that the highest priority missions take precedence above all others mission of lesser priority. The result, is a service acquisition model that will continue to drive private sector companies to manage their operations as an enterprise providing end-to-end service delivery for the best user experience. Visibility and control of all critical aspects of a Satcom network ensures that any upgrades or modifications to a single element of the network are done in consideration of the enterprise as a whole. By procuring Satcom as discrete elements, the DoD is unable to take advantage of the private sector capabilities available to maximize warfighter benefit.

Continuous Performance Improvement at the Speed of Relevance

With Hybrid Adaptive Networking, the DoD will be able to adopt continually advancing technologies and capabilities without incurring significant cost to change the underlying system infrastructure. When a new Satcom service with a translation layer that conforms to the standardized interface is fielded by a private sector company, it can be introduced to the Enterprise Management System without architecture changes. Adopting new networks and capabilities is merely terminal interoperability not multiple network re-definition.

By taking immediate action to develop an Enterprise Management platform for integrating and interoperating with private sector networks, the DoD will be able to add or inter-change networks with minimal integration. Creating a Standard Interface enables the private sector provider's to implement a translation agent(s), providing a bridge between the formats used by the private sector network and the standardized interface. Adding new private sector providers merely requires terminal interoperability and not re-architecture of the Enterprise Management platform. In regions or deployments requiring additional performance or resilience capabilities, the system would able to (a) dynamically support the addition of new networks within the desired area and (b) support adding additional or upgraded SLAs from service providers already operating within the hybrid network. Overall, this architecture provides the ability for the DoD to achieve continuous performance improvements at the speed of relevance.

Warfighters have developed tactics, techniques, and procedures reliant on Satcom availability. Operational missions consider the availability of communication to synchronize multi-domain operations, conduct net-centric warfare and coordinated schemes of maneuver. Plans are developed, exercised and trained based on full-availability of Satcom as well as plans for when Satcom is degraded. However, current systems are threatened and may not perform in a contested environment. Warfighters should be given the assurance that Satcom systems will perform when and where they need them. Multi-domain Operations requires assured communications, which can be met through proper implementation of operational SLAs and careful management of enterprise network resources. Hybrid Adaptive Networks facilitate service delivery across the enterprise affording warfighters access to required capabilities on demand by commercial provider's part of the HAN. In order to offer high service availability to both warfighters, resiliency options must be considered throughout the network and include each component and asset within the end-to-end system.

HAN Warfighter Advantage

The Hybrid Adaptive Network architecture approach provides warfighters high assurance data delivery services in both contested and congested operational environments. For an adversary to disrupt all communication options available to warfighters using a Hybrid Adaptive Network would require targeting multiple DoD purpose-built private sector Satcom networks, each with different mitigation techniques, satellites, ground segments, beam laydowns, orbital regimes, and frequency bands. Furthermore, some networks, with very small spot beams, would require adversaries to deploy jammers to be active in each of the beams. By creating an integrated and seamless hybrid network that connects at the network layer, different user groups can operate across different transport networks, and thereby make it increasingly difficult for adversaries to disrupt entire missions.

As DoD and private sector Satcom services each individually evolve their capabilities to make disruption of service cost prohibitive and significantly more difficult, the aggregate layering of the Hybrid Adaptive Network organically deters aggression in ground, space and cyber domains through:

- **Disaggregation:** Separating or routing High Value Missions across multiple protected networks
- **Diversity:** Multiple networks, frequencies, operators; surrogate capabilities (SA, C2, PNT, BFT, etc.)
- **Distribution:** Routing on dozens of DoD and private sector Satcom networks with no single point of failure
- **Deception:** Missions operating overtly, covertly, or even wartime reserve modes across multiple networks
- **Protection:** Hardened and Heterogeneous Networks rapidly evolving to threats and market demands
- **Proliferation:** Missions spanning multiple DoD and private sector networks.[14]

Another critical attribute obtained through the adoption of a Hybrid Adaptive Network is the ability to respond to surge scenarios requiring a high subscriber concentration of capacity within densely populated regions,

e.g. urban warfare. Since modern private sector HCS Satcom networks are being designed to service millions of users within a small geographic footprint, they are similarly capable of meeting surge demand during potential wartime situations. Technology innovations include designing networks with: very small spot beams, aggressive frequency re-use, multiple space assets in a single region, and the ability to dynamically move capacity. These innovative technologies are being deployed today and being further enhanced in next generation systems which will be operational in the early 2020s. This flexibility, coupled with a hybrid network composed of multiple managed service networks provides layered Satcom options available to end-users that can guarantee they will have the communication capacity available to support current and future mission needs. Network selection can be dynamically tailored for individual missions and user needs from any of the available networks in the HAN. Having multiple service networks available to warfighters will reduce the adversary's ability (while also imposing significant cost) to disrupt entire missions, requiring them to deny and disrupt each of the individual service networks operational within a theater.

Exhibit 14 and Exhibit 15 are two examples. Both are notional depictions contrasting service structures, one using DoD purpose-built capabilities and the other using a full layered architecture with DoD purpose-built and private sector systems. The time frame for these notional comparisons is the year 2022 using Satcom systems that are currently in development or on-orbit (using publicly released data and goggle earth).[15] Exhibit 14 represent a

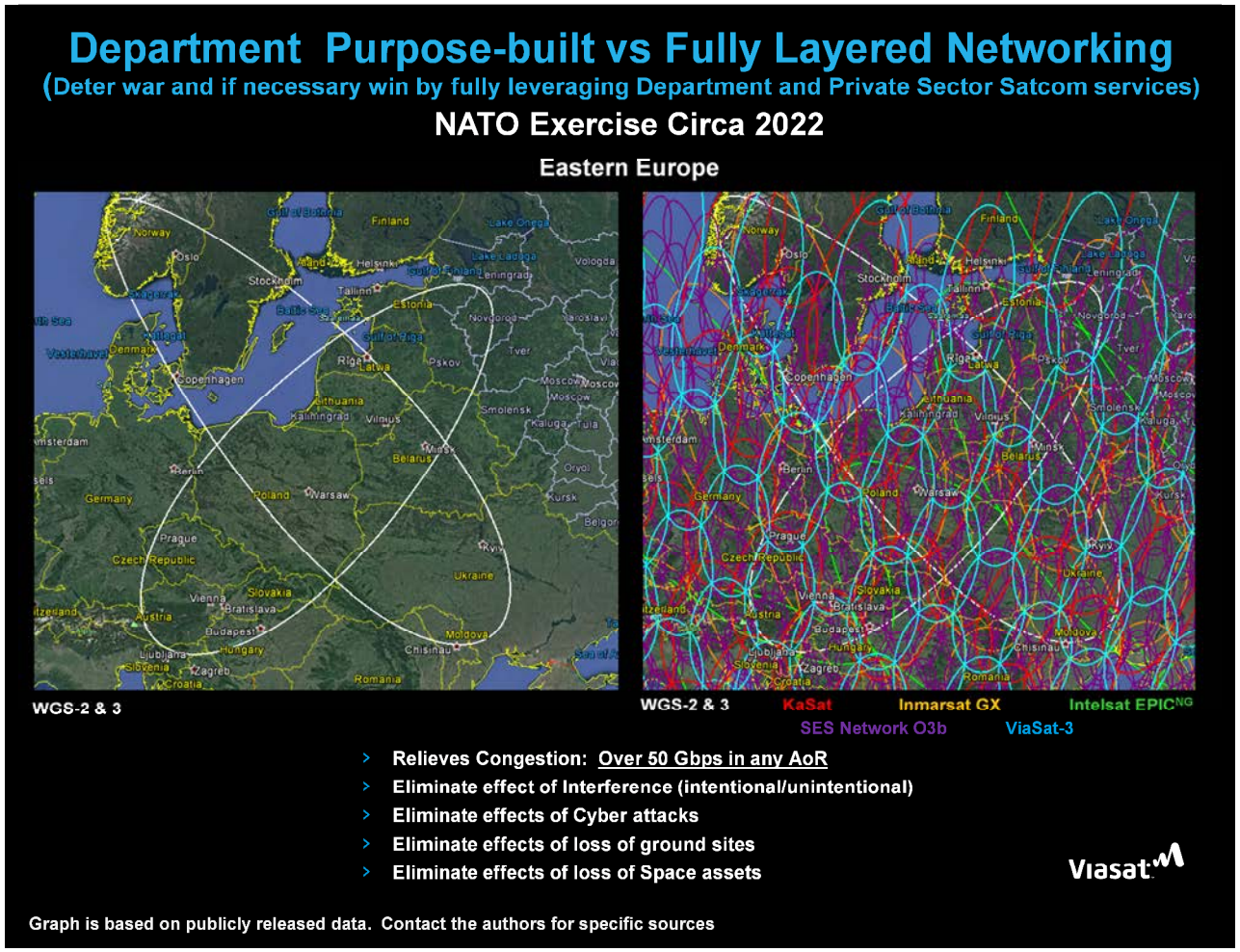

Exhibit 14: *Department of Defense versus Hybrid Adaptive Network architecture in Eastern Europe: Circa 2022 capabilities that could be employed to fulfill Satcom service during a NATO exercise.*

typical NATO exercise in the Eastern European region and Exhibit 15 represents a potential Freedom-of-Navigation (FoN) exercise in a key shipping route like the Straits of Malacca.

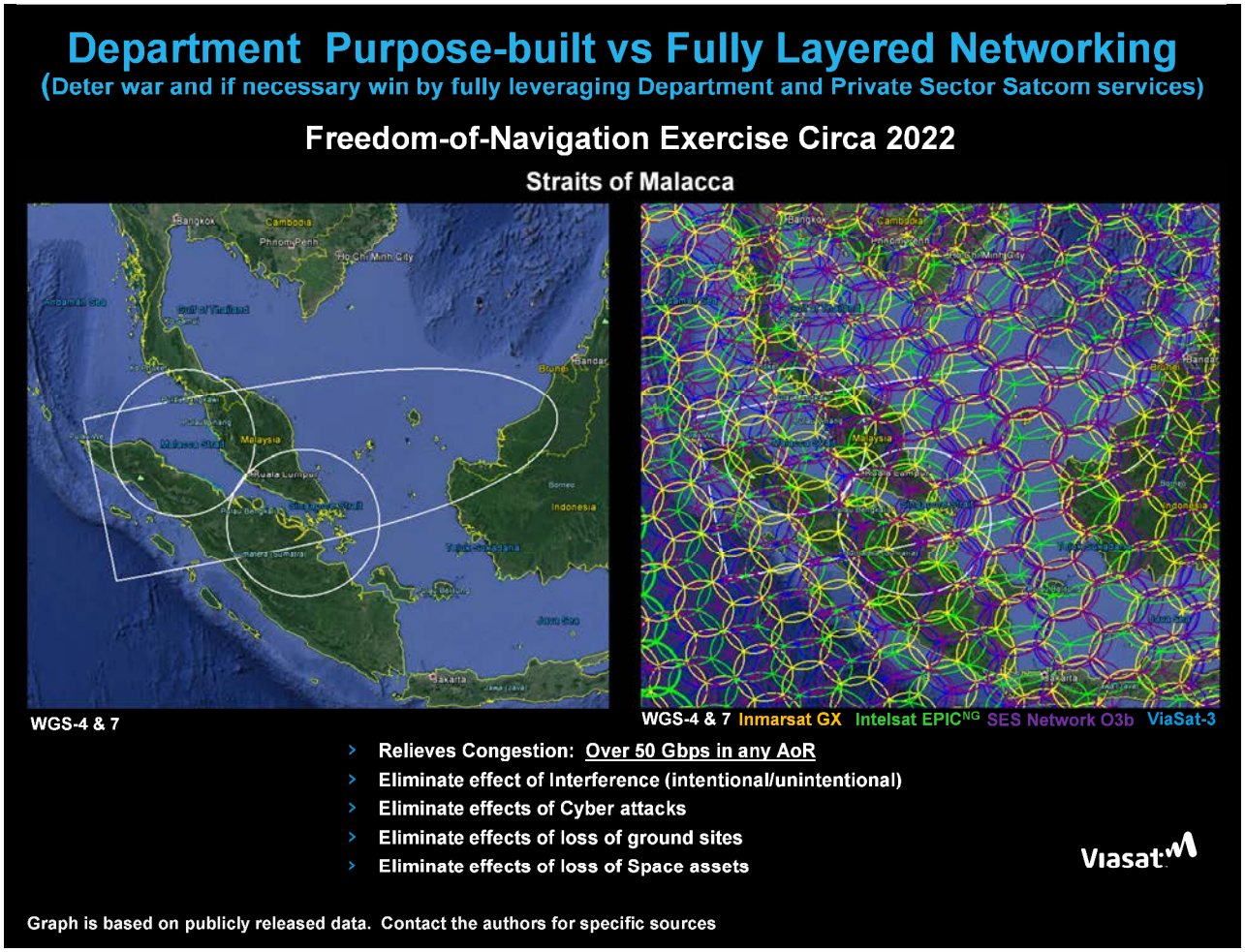

Exhibit 15: *Department of Defense versus Hybrid Adaptive Network architecture in Straits of Mope: Circa 2022 capabilities that could be employed to fulfill Satcom service during a FoN exercise.*

Each new layer added to the Hybrid Adaptive Network adds cost to the adversary and reduces the likelihood of negative effects by the adversary on the overall network. Adding deception and maneuver tactics to the Satcom and cyber domains through multi-path networking is analogous to deception and maneuver tactics in ground, air, and maritime domains. Ground forces do not consider 'taking the hill' the same way every time, nor do hill defenders remain content to prepare for the same type of attack. In the same way, the DoD can't allow adversaries to be successful in attacking our Satcom systems the same way every time. By leveraging private sector investment, the DoD can achieve Network resilience for a fraction of the cost of a purpose-built system while also imposing significant cost, technical, and material burdens on the adversary.

In summary, Hybrid Adaptive Networks are likely the only means to achieve the Wideband anticipated capacity demand for 50 Gbps in any AoR. While fulfilling the importance of capacity demand, it will similarly eliminate the effects of interference (intentional/unintentional), cyber-attacks, loss of ground sites, and loss of Space assets. The Hybrid Adaptive Network approach achieves the DoD's enduring mission to deny war and if necessary win at the "speed of relevance".

RECOMMENDATIONS

In closing, based on this analysis, there are several recommendations that will enable the DoD to meet both their near-term and long-term objectives. The results from these recommendations will immediately enhance the DoD's enduring mission and enable the adoption of a Hybrid Adaptive Networking Architecture with multi-network terminals. The recommendations create a path towards layering private sector networks and DoD's purpose-built systems further advancing the combined services available to the warfighter.

In considering the objectives of past, present and future DoD Pathfinders, they should be critically focused on creating a multi-layer communication network platform that will be highly resilient, more affordable, scalable, and will enable ongoing market-based completion among satellite network service providers. This is possible by taking the appropriate steps today with the following actions through Pathfinders and demonstrations:

1. **Immediately assess private sector Satcom services** and technology trajectories, thoroughly and quantitatively in a warfighter context including RF, cyber and kinetically contested threats.
2. Change the pilot/pathfinder acquisition model to **enable "Satcom as a Service."** Nimble acquisition will allow immediate access to the advanced technologies the private sector is bringing to the market with SLAs that define the required "operational effects", capabilities, and mitigations against current and emerging threat vectors.
3. **Immediately expand existing capabilities to encompass private sector Satcom services** that will build the framework for hybrid networking.
4. **Deploy multi-network terminals** that can support both existing and emerging networks to add overall resiliency in communications to warfighters by enabling access to additional private sector networks. Multi-network terminals will enable an immediate **pivot-off leased Ku-band.** Our analysis has shown that using leased Ku-Band for communications is the most expensive and the most disadvantaged against adversaries and therefore places unnecessary risk to the warfighter.
5. Immediately **implement a scalable Hybrid Adaptive Network architecture** through the deployment of a government Enterprise Management System that can cohesively interface with DoD purpose-built and private sector systems through the integration of translation agents to rapidly adopt the private sector Satcom systems.

While this analysis indicates several individual private sector networks are more resilient than current purpose-built government networks, overall warfighter capability can be maximized by creating a Hybrid Adaptive Network. Warfighters will then seamlessly roam across multiple private sector and government communication systems adding both deception and maneuver to Satcom or the Space Domain. Hybrid networks are enabled by flexible, multi-mode, multi-band terminals (which are already necessary, being produced and employed by the private sector), and advanced network management providing seamless roaming and user/network management across the component networks.

This analysis further recommends that a Hybrid Adaptive Network should ensure interoperation via an open standard interface at the network level. This approach maximizes the private sector ability to innovate while allowing the Department to quickly and affordably add new transport networks to their hybrid network, and will create a sea-change in acquisition for the Department. Rather than **one-time acquisition-based competition of system components** that leads to vendor lock, expensive and underperforming programs and technology; individual network service providers vying to become part of the hybrid network will **face ongoing market-based competition** for DoD business, allowing the DoD to economically ride the exponential technology advances of private sector innovation.

By making long-lasting decisions today the DoD can positively impact the effectiveness of the overall system and its ability to meet the overarching objective of providing warfighters with the highest performance and most

resilient technology possible. This can only occur by adopting an enterprise architecture that can take advantage of the rapid deployment lifecycle offered within the private sector. Together, these recommendations provide the structure for improving the effectiveness of the systems used by the DoD while eliminating the need for costly, low performance systems that lack many of the resilience traits offered within the private sector.

This paper has provided a resilient path for adapting new technologies enhancing the DoD's enduring mission at the "speed of relevance" through the adoption of a Hybrid Adaptive Network. In order to drive the changes necessary to guarantee improved communications for our warfighters, the DoD must have access to the continuum of performance and resilience technology advancements that private sector networks can offer today and in the near future.

Additionally, by leveraging the improved bandwidth economics and affordability that the market requires in developing advanced technologies, the DoD will also experience significant economic benefits. Continuing the DoD's commercial Satcom procurement model of acquiring raw undressed bandwidth and building out DoD networks, even with the added concepts of "pooled bandwidth/supplemental leases" will leave the DoD woefully short of procuring, deploying, and operating with higher performance, more resilient and more affordable commercial Satcom in operationally significant timelines.

The DoD should strive to achieve an Enterprise Network Manager that seamlessly routes DoD traffic over a host of DoD purpose-built and commercial Satcom providers responsive to operational warfighter requirements, as soon as this year. This essentially forms a "Hybrid Adaptive Network of Networks" with enhanced performance, cyber defenses, near-peer threat resilience, baseline and surge capacity, and affordability. This approach will achieve the highest possible multi-network resilience; ultimately deterring adversary aggression against these space and cyber networks due to the extreme cost to attack them, and will exponentially decrease the likelihood of a successful attack against the whole; enabling the graceful addition of new capabilities as they enter the market while providing continuous market-driven competition in terms of performance, resilience, and affordability.

Final Considerations for Follow-on Studies and Actions

As the Department of Defense moves from analysis to action to deploy resilient and capable Satcom services in support and enhance its enduring mission further investigation should provide answers to the following questions:

1. Does the private sector have protected/unprotected Satcom solutions that provide better adversary threat resilience and performance than the current and planned DoD systems?
2. Have industry claims of better performance, resilience and mission assurance been assessed and empirically evaluated?
3. If there is merit in private sector resilience claims, how quickly can the Department acquire and employ these capabilities to deter further aggression in space and cyberspace?
4. Does the private sector have suggestions on a phased, affordable terminal transition methodology that accelerates capability to the warfighter and provides increased flexibility for Satcom space and cyber systems?

The technology crossover and accelerating threat has put the **Department at a crossroads**. Commercial technology innovation is outpacing government and DoD technology innovation; and the fact that many of the technological developments are from the commercial sector means that state competitors and non-state actors also have access to them, a fact that risks eroding our conventional overmatch.[16] One road **continues the current DoD Satcom architecture further eroding the DoD enduring mission** and represents risk to the warfighter and the largest burden on taxpayers. Another road **will enhance the DoD enduring mission**,

increase warfighter Satcom performance in multi-domain operations, increase resilience against the current and emerging threat vectors, and improve affordability therefore reducing taxpayer investments.

---

[1] https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf,page 1
[2] https://www.defense.gov/News/Article/Article/1318291/mattis-dod-lines-of-effort-include-building-a-more-lethal-force/
[3] https://www.congress.gov/114/plaws/publ92/PLAW-114publ92.pdf, Section 1611
[4] https://www.defense.gov/News/Transcripts/Transcript-View/Article/630419/building-the-first-link-to-the-force-of-the-future/source/GovDelivery/
[5] https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf, page 10
[6] Infrastructure Executive (IE) Satellite Communications (SATCOM) Division Technical Support Branch (IE 22): Commercial Satellite Communications (COMSATCOM) Ordering Guide, Version 3.1, July 2017
[7] Graph is based on publicly released data. Contact the authors for specific press releases/sources
[8] http://investors.viasat.com/releasedetail.cfm?releaseid=954123
[9] http://secure.afa.org/events/Conference/2017/recordings/Wednesday-340-COCOM.asp, US STRATCOM Commander Gen. Hyten
[10] https://www.whitehouse.gov/briefings-statements/president-donald-j-trump-unveiling-america-first-national-space-strategy/
[11] https://www.intelsatgeneral.com/blog/evolution-of-commercial-satellite-technology-improves-readiness/
[12] http://spacenews.com/surprise-addition-of-military-satellites-to-the-dod-budget-irks-commercial-industry/
[13] http://docs.house.gov/meetings/AS/AS29/20170329/105785/HHRG-115-AS29-Wstate-SheltonW-20170329.pdf
[14] http://spacenews.com/loverro-defense-is-the-best-deterrent-against-a-war-in-space/
[15] Exhibit 13 and 14 beam plots are based on publicly released data. Contact the authors for specific source material
[16] https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf,page 3

