35th Space Symposium, Technical Track, Colorado Springs, Colorado, United States of America
Presented on April 8, 2019

NATIONAL SECURITY SPACE GOVERNANCE EMPLOYING HYBRID ADAPTIVE NETWORKING FOR ENSURED SATCOM ACCESS IN GLOBAL RESPONSE OPERATIONS

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

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

ABSTRACT

Deployed global response teams have limited access to terrestrial and LOS communication networks, necessitating access to Satcom Networks for timely information and response. Traditionally, National Security Space (NSS) governance of Satcom supporting these missions has been dispersed among AFSPC, DISA, ARSTRAT, and RSSCs for Space, Networking, and Services for terminals and platform integration. Recently, a new model emerged with Warfighter units procuring Transport Network Satcom access directly via Service Level Agreement (SLA) contracts. Governance in this new model is between the warfighter unit and their Satcom Network access provider.

This paper outlines these governance models and presents a means to incorporate them into a NSS structure based on a unified Space Command responsible for delivery of ensured Space Effects in benign and threatened environments, protection and defense of Space systems, and continued preservation of Space as a business domain.

This paper describes how existing and emerging technologies can be leveraged into NSS governance and operations while enabling warfighters ensured access to the latest information, resources and experts that can aide in their efforts. This paper provides a framework and network architecture for improving connectivity with layers of enterprise hybrid networks by allowing the dissemination of data through multi-network terminals and Wi-Fi hotspots. The paper describes the network architecture and governance structure that ensures communication is available to global response teams, leveraging multiple existing and future satellite networks, to provide layered assurance and resilience, and ensuring continuous access to resources to that improves overall effectiveness of their mission or deployment.

PROBLEM STATEMENT

The Department of Defense's (DoD's) enduring mission is *"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] In order to deter war and protect the security of our nation, the DoD needs highly-assured, resilient satellite communication (Satcom) and cybersecurity-defended Satcom Networks that are operable in the presence of any adversarial threat across the full spectrum of environments benign through contested.

Historically the DoD has served its enduring mission Satcom with a National Security Space (NSS) governance model dispersed among AFSPC, DISA, ARSTRAT, and RSSCs for Space, Networking and Services for terminals and platform integration. In this model the DoD or Military has used purpose-built Satcom Networks employing their own purpose-built Satellites or used commercial satellites through transponder leasing or acquisition to establish their own Satcom Networks. The DoD has referred to this as MilSatcom and ComSatcom, however both are DoD or Military governed Satcom Networks employing DoD or Military networking, gateways, backhaul, and terminals operating over DoD or commercial leased or acquired bandwidth. For the DoD to improve the governance of their Satcom Network performance (i.e. coverage, capacity, or speed), assurance (i.e. availability or A_o), or resilience (i.e.

availability or A_o in a contested environment), the DoD or Military has to make significant new investments in new satellites or commercial satellite capacity and parallel new investments in networking, gateways, backhaul, and terminals. Either of these solutions requires significant investment and time often on the order of $5-10B and 5-10 years.

Recently, a new governance model has emerged with Warfighter units procuring Satcom Transport Network access directly via Service Level Agreement (SLA) contracts. Governance in this new model is between the warfighter unit and their Satcom Network Access provider. In this new model, the Private Sector Satcom Network Providers have deployed, or govern, their own end-to-end Satcom Networks comprised of their own satellites, networking, gateways, backhaul, and terminals. A fundamental advantage of this new governance model is the recognition by the Private Sector Satcom Network Providers that adversaries are developing electronic jammers and other cyber weapons that can render the historical commercial and most defense satellite communications inoperable.[2] This realization is driving fundamental improvements in the new Private Sector Satcom Networks and establishing the concept of diversity in communications as a way to create further resiliency in the face of growing threats, per Brig. Gen. DeAnna Burt, director of operations and communications at Air Force Space Command[3].

Examples of the historical NSS governance approach are visible today and in the FY20 budget planning/request leading to 2028-2030 fielded improvements for 1) Protected Tactical Satellites (PTS) to improve the anti-jam performance of DoD satellites, 2) Protected Tactical Enterprise Services (PTES) ground segment and gateways to improve networking for WGS, commercial satellite capacity, and the eventual PTS satellites, 3) Protected Tactical Waveform (PTW) to improve anti-jam network performance and upgrade terminals to operate on WGS, commercial satellite capacity, and the eventual PTS satellites, and 4) Evolved Strategic Satcom to improve the NC3 mission.

Since Space and cyberspace superiority are essential enablers for the DoD's enduring mission, and since the DoD historical NSS model to make improvements is characterized by investment periods of over 5-10 years and over $5-10B, the Problem Statement becomes, is there a better way? Is there a way to accelerate adoption of emerging technologies at the "speed of relevance"[4] to gain performance, assurance, and resilience even in contested environments?

This paper explores how to establish Satcom assurance and resiliency for global response missions aggregating existing DoD Wideband Satcom and modern broadband High Capacity Satellites (HCS) governance models and technologies at the "speed of relevance." The approach aggregates the DoD or Military purpose-built Satcom Networks employing DoD or Military networking, gateways, backhaul, and terminals with new globally deployed Private Sector Satcom Networks into a layered framework for offering resiliency and capacity improvements in a cost-effective manner that together can meet current and future geographically distributed communications needs.

To this end, and in sharp contrast to the historically approach DoD or military purpose-built, General John "Jay" Raymond, Commander of Air Force Space Command, told Lawmakers his vision for Satcom is for users to be able to "roam" rapidly among different satellite service providers or constellations[5], or employing the aggregation of DoD and Private Sector governed Satcom Networks.

MULTI-NETWORK PROTOTYPING

Viasat recently participated in NATO's Euro-Atlantic Disaster Response Coordination Centre (EADRCC) training exercise in Eastern Europe. During this exercise, Viasat demonstrated the ability to deploy portable multi-network terminals that can be set up within minutes (shown in Exhibit 1) for enabling assured, resilient and reliable communications for emergency personnel, without needing to rely on accessibility or availability of terrestrial

networks. Other enterprise organizations, including the Red Cross, use similar methods to enable communications during their emergency and disaster response missions for ensuring access to the necessary information and experts. Using an integrated multi-network ecosystem with hybrid networking maximizes the emergency and global response mission capabilities and resilience by providing simultaneous and layered access to multiple networks. And, since these networks can span multiple orbital regimes and operate over different frequency bands, they provide multi-path diversity through independent ground infrastructure, network management capabilities, and cyber defense implementations. Because of this multi-network approach, military and first responders have inherent protections against single point of network attack or failures, resulting in high-speed connectivity across environments and situations.

The NATO exercise demonstrated and proved the benefits of resilient connectivity during global response missions. Access to multiple overlapping Ku and Ka-band networks enabled first responders and disaster response units resilient access to time-critical information for delivering the necessary care or aide to maximize the overall success of the mission. By enabling access to communications with remote experts in their field, a coordinated effort with remote specialists and technical experts is possible. For response units to access multiple networks to optimize assurance and resiliency, it requires three key elements:

1. Multi-network terminals that can dynamically operate on multiple networks (i.e. supporting frequency bands, orbital regimes, and network access waveforms/protocols),
2. A fabric or layers of independent Satcom Networks (or Service Providers), and
3. Hybrid Adaptive Network (HAN) Management Portal for DoD (or Customer) access, ordering and monitoring to support provisioning and remote service management requests.

Exhibit 1: *A multi-network transported satellite terminal easily sets up to operate on DoD or Private Sector Satcom Networks employing independent satellites, networking, gateways, and backhaul.*

Thus, the transition from the historical DoD NSS model is the deployment of a multi-network terminal since the fabric of independent Satcom Networks are being deployed by both the DoD using their own purpose-built Satellites or using commercial satellites through transponder leasing or acquisition augmented by the global deployment of end-to-end HTS Satcom Networks.

ENHANCED RESILIENCE WITH HYBRID ADAPTIVE NETWORKING

There are two means to increase the overall resilience of Satcom Networks in all environments including contested. The first means would be to make better networks. This requires an understanding of the current and emerging threats and threat vectors in addition to significant investments in time and money. The second means would be to agilely roam across the fabric of networks as suggested by both Gen Raymond and Brig Gen Burt. Exhibit 2 depicts these two approaches for creating a highly assured and resilient networking for use by global response missions or military units. In the first approach, the DoD and Private Sector investments improve the individual Satcom Network performance and availability (A_o) through exquisite new satellites, networking, ground segment and terminals. This requires substantial capital investment along with a long development lifecycle, by either the DoD or Private Sector, in order to define an end-to-end system that provides the enhanced performance and is defensible against a wide-array of possible threats (including future threats). Often, this approach requires synchronously deploying entirely new ground, space, terminal, and network infrastructure to operate and access

the new capabilities. While this approach seeks to address all possible combinations of existing or future threats, it continues to create a single point of attack or failure that could ultimately strand users without necessary communications in the event of an outage.

The second approach achieves high availability and resiliency through path diversity, thereby eliminating any single point of attack or failure. This approach delivers an overall combined resilient solution using the attributes and capabilities of various independent native networks or layers. The more networks or layers added to the integrated network, the higher the assurance, resiliency and availability. And, contrary to the first approach, this resilient solution can achieved at the "speed of relevance" by leveraging existing independent networks with multi-network terminals and an integrated enterprise HAN management system that can intelligently manage and monitor remote users, networks and threats across the space, ground and cyber domains.

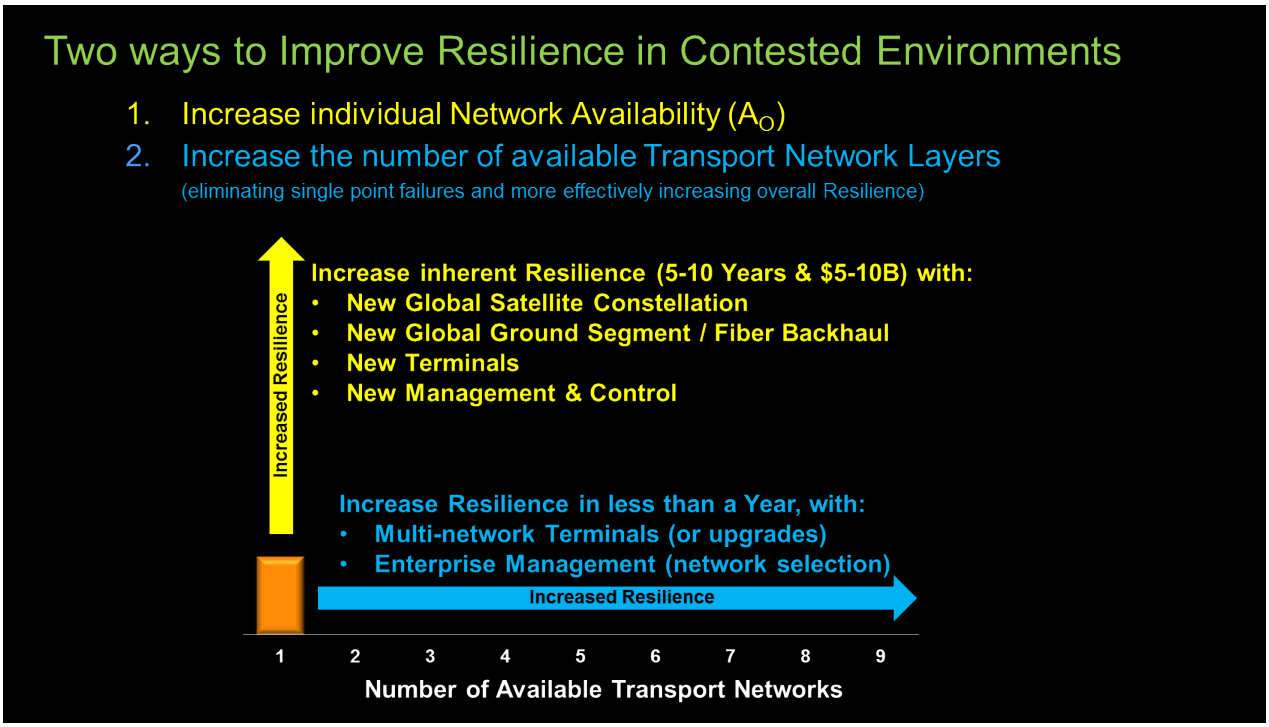

Exhibit 2: *Two approaches to increasing network resilience, investments in new Transport networks or investments in agilely roaming across layers of Transport networks.*

ENHANCE NETWORK RESILIENCY AND AVAILABILITY THROUGH LAYERING

Since the deployment of the DoD governed WGS, AEHF, and commercial satellite capacity Satcom Networks, multiple Private Sector Satcom Networks have been developed and deployed their own governed Satcom Networks. The collective investment in these new Satcom Networks, which exceeds $30-40B over the last 10 years, has created the multiple layers or a fabric of advanced private sector transport network layers that can augment the DoD Satcom Networks. These multiple end-to-end service provider networks offer innovative improvements in resiliency and capacity over the networks the DoD employs today, since they have been built with knowledge that Space has become a congested, contested, and competitive domain.

By aggregating these DoD and private sector Satcom Networks from many providers, the DoD will immediately enhance resilience and mission assurance for their warfighters operating in benign, threatened, and contested environments. Adoption and layering of existing and new capabilities immediately increases resilience and creates

deterrence by imposing new cost on adversaries; while simultaneously denying the adversary the ability to interfere with all of the individual layers of Satcom networks. As shown in Exhibit 3, while a single transport network may only offer 40% availability within a contested environment, the overall availability can be drastically improved by adding additional transport layers or networks. Essentially enabling the DoD the ability to maneuver among the networks and hide within the volume of commercial traffic positioned to serve commercial air, maritime, enterprise, and consumer traffic.

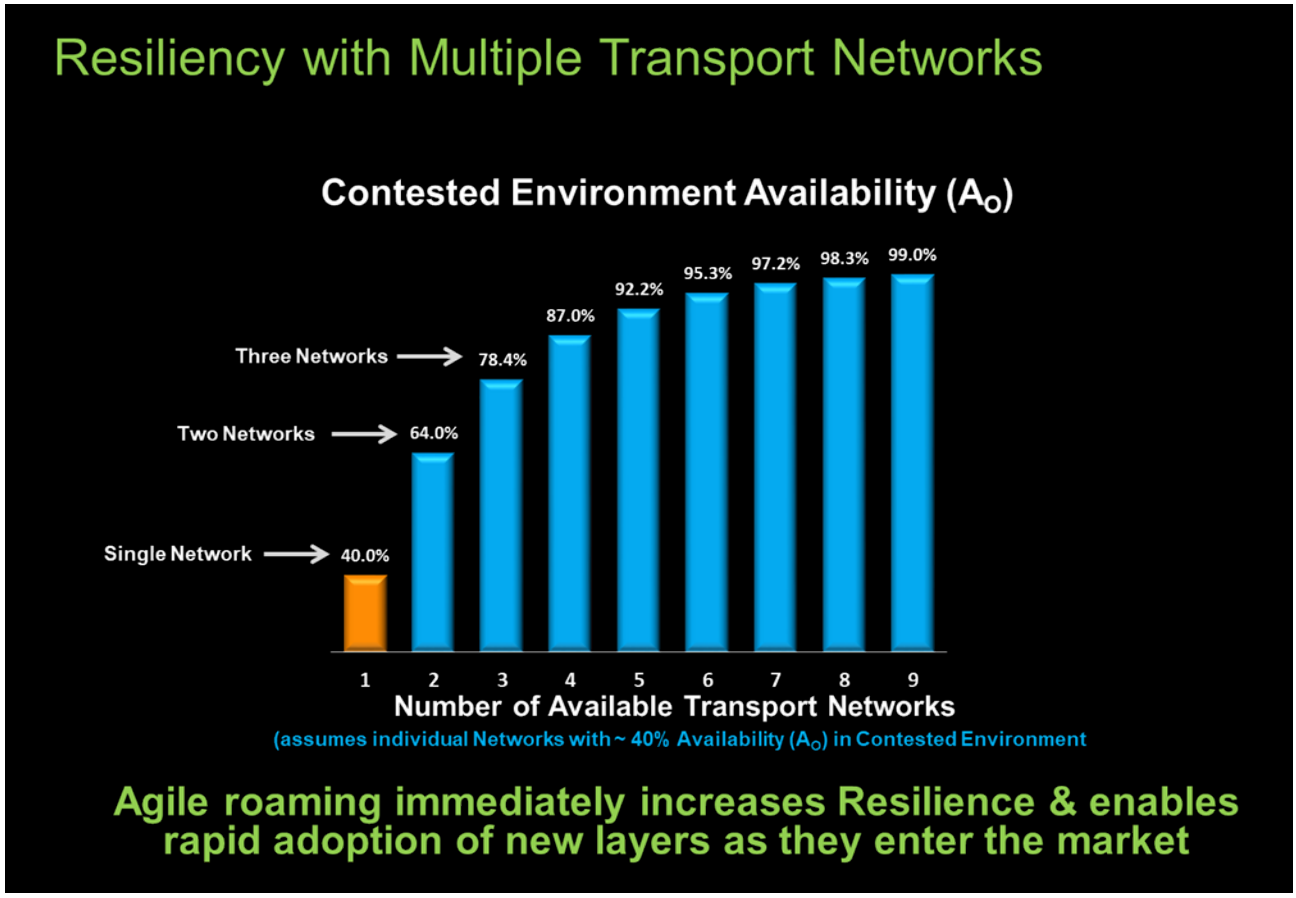

Exhibit 3: *Agile roaming among layers of independent Transport Networks can significantly increase overall availability in a contested environment relative to single network availability improvements.*

In this example, if the Availability (A_o) of single network was 40%, then the resilience or A_o in the contested environment of that single network would be equal to 1-(1-A_o of that single network) or 40%. If two networks are layered, both with an A_o of 40%, then the combined A_o in the contested environment would be equal to 1-(1-A_o first network)*(1-A_o second network) or 64%. And, so on for 3 or more networks. Thus, the resulting combined availability could exceed 78% when layering 3 networks that each has 40% contested availability. Likewise the combined availability could achieve 95% (or more) when 6 or more networks are layered. The combined network availability is continually enriched with each additional network, whether DoD or Private Sector, for delivering the highest possible mission assurance to its users at any given time.

With this approach, global response missions will have access to the most reliable and scalable network architecture that seamlessly integrates a constellation of multi-orbital space assets that together will significantly enhance connectivity to missions. Typically, warfighters and global response users have connectivity to a single purpose-built network that is often oversubscribed and/or susceptible to degradation and disruption in contested

environments, often leaving warfighters with few, if any, options to dynamically switch networks in response to congestion, outages, or other threats that impede the overall service availability.

This concept of multiple network layering has become a key element in the future vision of Air Force Space Command as discussed by Gen Raymond and in the operating concepts for the Combined Space Operations Center's (CSpOC) Satcom Integrated Operations Division (SIOD).[6]

RESILIENCE ASSESSMENT OF CURRENT AND EMERGING SATCOM NETWORKS

In order to establish a highly available layered network, it is important to use layers with complementary and diverse capabilities or attributes in order to have resiliency across multiple dimensions. To do so, Viasat defined a systematic approach that can evaluate existing and future networks to provide an overall scoring methodology that can be used for providing an availability assessment. This assessment incorporates the full spectrum of threats, as known today, to provide a baseline for modeling and evaluating the capabilities, defenses, and weaknesses of individual networks regardless of their governance. Using this approach with the existing DoD or Military provided Satcom Networks employing DoD or Military networking, gateways, backhaul, and terminals plus the current and planned Private Sector Satcom Networks a combined resilience and availability can be assessed. This allows a systematic approach for recommending network combinations that can address a comprehensive set of existing and future threats for improving the overall system resiliency through layering. In lieu of having empirically measured Availability, or $A_{o,}$ against specific threats, we have established and evaluation algorithm that uses criteria and standards employed across the Satcom industry to sustain communication across different environments providing protections against different known and future anticipated threat vectors.

The scoring, shown in Exhibit 4, is intended to establish an objective evaluation using defined criteria based on empiric network characteristics and attributes for assessing each of the different categories that include the following: 1) interference rejection via beam roll-off, 2) nulling rejection of unwanted interference, 3) operating bandwidth to support hopping/spreading, 4) acquisition and operation of space and terminal segments within a GPS-denied environment, 5) defense against cyber-threats, 6) immunity against teleport monitoring and collections, 7) defense against kinetic or non-kinetic threats, 8) ability to enable LPI/LPD operations, 9) performance in scintillated atmospheric conditions, 10) operations in very high density deployments, and 11) future unanticipated threats. Each evaluated network receives a score from 0 to 5 within each category (with 0 being the lowest score in which the network is susceptible to the threat category and 5 being the highest possible score for mitigating and minimizing the effect of a possible threat). The resilience assessment can dynamically support category weighting (0 to 1) to prioritize specific categories based on the importance or likelihood of that category of threat. By summing the scores from each category, each existing or future network can receive an overall resilience score, or A_o, calculated from the total score as a percentage of the theoretical maximum possible score that can be used to assess and compare networks.[7]

Market-driven advancements within the private sector Satcom industry continue to expand capabilities for enhancing the overall system availability and improving network performance. These same advancements offer similar resiliency enhancements for improving the mission assurance for global response missions. As an example, current private sector networks that typically employ technologies for improving the system availability with gateway diversity to minimize the effects of weather impairments also provide inherent protections against a) gateway outages and b) teleport monitoring. Additional advanced capabilities that are being deployed within private sector networks to provide improved service delivery to subscribers include:

- Interference Rejection and Mitigation technical approaches to prevent disruption from intentional and unintentional interference sources
- Immunity to Teleport Monitoring, Traffic Analysis, and Terminal Geolocation

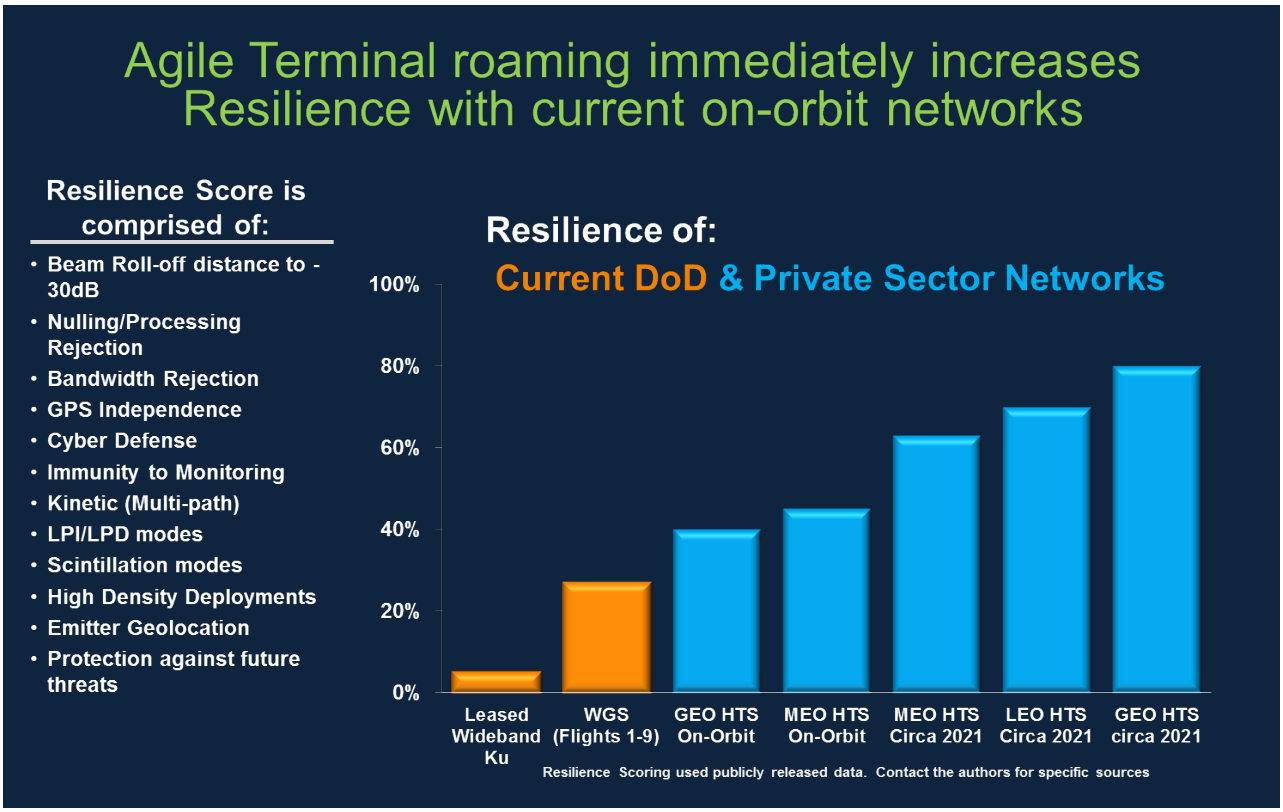

Exhibit 4: *Viasat quantitatively assessed DoD purpose-built and commercial leased Satcom Network with the currently and in development Private Sector Satcom Networks. Not surprisingly, the newer systems built with the knowledge that space has become congested, contested, and competitive have better resilience performance.*

- Integrated real-time end-to-end techniques to mitigate and counter the effect of near-peer cyber threats including current and evolving vectors using behavioral analysis for identifying new signatures and vectors
- Flexibility to service high density deployments with a large number of users/subscribers within a small geographic region

By adopting service provider networks that offer these operational protections within a HAN framework, global response missions will have direct access to advanced capabilities that improve their resiliency in the presence of evolving threats. And, when using multi-network terminals that can be simply upgraded to support access to additional layers of networks, deployed units will be able to dynamically maintain connectivity in the presence of threat situations that previously were damaging to the mission's success. And, this will allow missions and users to access advanced market-driven capabilities that include:

- Access to integrated multi-domain situational awareness for user and threat monitoring across geographically distributed units and networks
- Sustained operations in GPS denied environments with access to networks capable of providing GPS-independent PNT
- Path diversity deterrence against kinetic or space-based attacks for users to roam across multiple independent networks (and space, ground, and terrestrial infrastructure) that overlap in geographic coverage
- Operations enabling Low-Probability of Intercept/Low-Probability of Detection terminals

- Operations in Scintillation without impacting the overall performance
- Ability to geo-locate, mitigate the effect of, and monitor the presence of intentional and unintentional emitters

Current and planned private sector and government networks require continuous evaluation of their capabilities and resilience claims in order to identify possible attack vectors that could potentially result in communication impairments. Using this resilience evaluation methodology that accommodates changes in threat vectors provides a framework that can adapt to changes in a) threat vectors used by adversaries and b) technology and network attributes being employed to mitigate and respond to threat vectors. By independently and systematically evaluating the resiliency assertions and capabilities of the networks used by warfighters and missions will further show the necessity of utilizing a Hybrid Adaptive Network approach to create a portfolio of private sector and DoD systems that used to support future missions. Using the construct of a service agreement that defines the performance and resilience capabilities, each mission can receive the necessary protections and connectivity, regardless of the threat environment or situation. Additionally, from evaluating the unique capabilities of each network used within the HAN, it will allow network selection to be intelligently based on:

1. Unique requirements for each individual mission
2. Evaluated capabilities of the networks
3. Current known threats that could impact the effectiveness of the mission

Using each of the inputs (requirements, capabilities, threats), a recommended primary network can be determined that can best satisfy the requirements of the mission while simultaneously mitigating any known threats based on the inherent mission assurance capabilities or attributes of the network.

HAN LAYERED MODEL FOR ACCESSING TECHNOLOGY ADVANCEMENTS

By taking the individual performance and resiliency capabilities of government networks and combing them with on-orbit private sector networks, the combined resiliency is improved to achieve more than 80% resiliency today. This combines existing GEO assets with the additional performance and resiliency benefits of existing MEO HTS networks, as shown in Exhibit 5. By allowing users to roam across each of the constituent layers allows current global response missions to improve effectiveness through (a) increased overall network availability and (b) access to additional capacity offered by each of the individual layers. With a unified space governance focusing on promoting and advancing a framework that can adopt a scalable network of networks approach, it will enable the aggregated network to be further enriched as additional networks become operational. By 2021, the overall network can achieve more than 90% availability and resilience within a contested environment by enabling mission access to multiple networks at LEO, MEO, and GEO. This further shows a necessity to focus on the resiliency of integrated aggregated network instead of single exquisite system(s) that requires significant cost and time for development/production. And, even with an exquisite satellite system, it creates a single point of failure that could eventually be compromised while simultaneously inviting adversaries to use focused targeting.

There are several inherent benefits to transitioning to a service-based model to access networks. First, it allows for market-based competition that will enhance network attributes that effectively improve network capacity, resilience and mission assurance of existing systems. With this, global response missions will be able to continually enhance their capabilities with reliable and resilient networks by simply using and promoting the features that deliver successful communications to users.

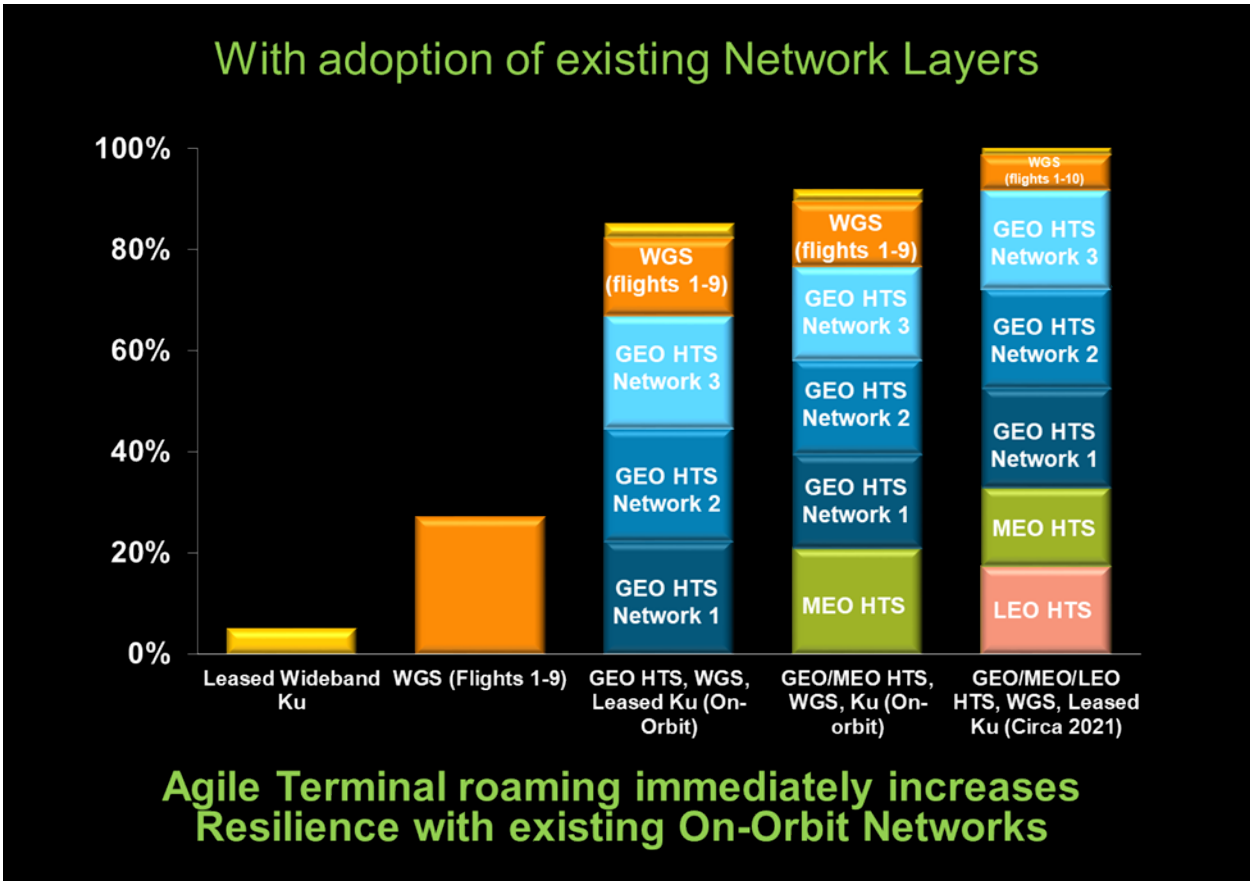

***Exhibit 5**: With the deployment of multi--network the DoD can dramatically increase assurance and resilience in contested environments at the "speed of relevance".*

ADAPTIVE SERVICE MODEL FOR ACCESSING TECHNOLOGY ADVANCEMENTS

This service oriented approach typically has a well-defined Service Level Agreement (SLA) that describes the agreed level of performance (data rates, latency, etc.) expected by a user from a network operator and defines the metrics by which the service will be assessed. In support of global response operations, SLAs could be expanded to include additional operational capabilities or protections that further define the service delivery capabilities. These protections could include:

- Service availability undisrupted through ground site or teleport outages
- Protections against ground site or teleport monitoring
- Service assurance across weather anomalies
- Service availability through intentional or unintentional fiber outages
- Integrated Cybersecurity protections against known or discovered signatures, in real-time
- Protections against Interference or jamming within a user-defined range to the jammer

The importance of including mission assurance protections within the construct of the SLA is to ensure missions receive the necessary performance, regardless of the threat environment (benign vs threatened). By defining the capabilities, the combined network can seamlessly provide the service delivery necessary to enable operations through any threat situation with the ability to access the layers of networks. With intelligent hybrid

adaptive networking, the service agreement would be to the aggregated network which would allow users to access any combination of Satcom networks for maintaining connectivity. This model uses a single service agreement for enabling seamless management and routing of users based on real-time threat intelligence (or other service impacting issues) for guaranteeing users receive the necessary protections and performance.

To successfully meet each service requirement or request, the hybrid network requires path diversity to seamlessly move users across disparate networks that overlap within service regions. This provides the necessary redundancy and resiliency as it offers multi-band, multi-orbit, and multi-network options to maneuver and roam amongst independent private sector and government networks. Since this construct is designed to be scalable and adaptable to support adopting native networks that can be accessed from multi-network terminals, global missions can simply be enhanced by integrating the HAN Management Portal into the unified Space Command (for requesting service and monitoring fulfillment) and by promoting and utilizing multi-network terminals that can access different combinations of networks.

Using a hybrid networking model, service across any region from integrated networks is readily accessible today for allowing missions to access to a Hybrid Adaptive Network without a priori scheduling. Additionally, since disparate users and global response missions require different performance and network protections, hybrid networking service agreements can be defined to support each combination of mission and operation priorities for enabling automatic prioritization management for users within a coverage area that can guarantee that the highest priority missions take precedence.

ENTERPRISE MANAGEMENT FROM WITHIN A UNIFIED SPACE COMMAND

Accessing the aggregated layers of a Hybrid Adaptive Network is possible through a HAN Management Portal that delivers three foundational capabilities necessary to support Air Force Space Command operations, namely 1) service ordering, 2) mission tasking and 3) accessing Situational Awareness (SA) information across multiple private sector and government networks.

The HAN Management Portal provides unified access for Air Force Space Command operators to enhance their ability to centrally order, manage, fulfill, and monitor users. The HAN Management Portal uses an open standard interface for performing service tasking and facilitating access to each of the constituent transport networks. This tool allows for space, cyber, physical and network operators to access network situational awareness and health to form a common operating picture across multiple networks. This will enable users and operators to a) dynamically request service with mission requirements and priorities and b) examine threats, outages or performance information from each constituent network that allows operators the ability to drill-down into individual user health and performance. Because of the dynamic nature of the HAN architecture, mission priorities and network requirements can be modified and updated near real time without advanced planning. As an example, this can include increasing the amount of bandwidth needed to support additional users at a remote site or changing mission assurance capabilities to add additional network protections (e.g. integrated cyber defense or switching to a network that can minimize the effect of near-peer jammers).

As future constellations are adopted into the HAN, software-defined multi-network terminals can be upgraded without affecting the HAN Management Portals or other access networks. As shown in Exhibit 6, the various DoD procurement and “fighting Satcom” organizations will gain direct access to the HAN through a web-based portal application. As mission requirements change or service impacting issues are detected, the HAN would dynamically move users to an alternate network. Additionally, the HAN is designed to dynamically accommodate varying environmental situations and user demand profiles, it can similarly adapt to changes in mission needs. From the HAN Manager Portal, Space Command operators can immediately improve their situational awareness visibility using the unified display that interfaces directly with the aggregated independent HAN network layers. The

situational awareness will allow operators to examine network, user and threat information within cohesive and comprehensive display.

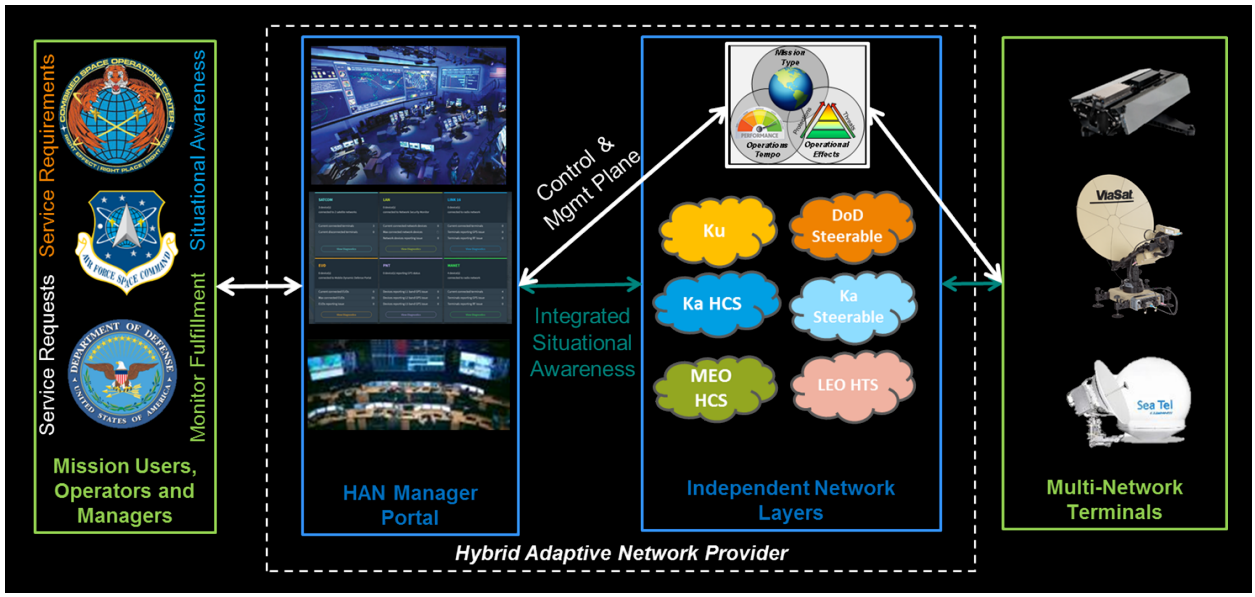

Exhibit 6: *Hybrid Adaptive Management provides integrated access to DoD and multi-orbit private sector networks for coordinated Situational Awareness monitoring, user management and control using a standardized interface.*

With access to multiple independent networks, the HAN will offer an integrated infrastructure that provides the following benefits to warfighters, missions and operators. First, by improving the overall system resilience it will deter aggression into the space and cyber domains. Additionally, the rapid capacity growth occurring from the private sector across each of the different orbital regimes will continue to increase through the 2020s and 2030s. In the next 5 years, the private sector industry leaders will together add more than 5 Tbps of additional global capacity (i.e. more than 5 times the total capacity of all communication satellites currently on-orbit). In comparison to the DoD projected capacity demands, the DoD would consume less than 1% of the total system capacity available from the private sector. By having the ability to access each of the networks within an integrated hybrid network, it provides a service-based approach for ensuring future demand can be easily fulfilled across the layers of networks. Each of the layers together can provide dynamic on-demand capacity in remote, high density deployments and across the full range of priority missions. As shown in Exhibit 7, within a small geographic footprint, users can seamlessly roam across any of the private sector and DoD networks to ensure communications remain undisrupted for the duration of the mission.[8] Each additional layer added to the integrated network offers improvements in resiliency and mission assurance such that users have the ability to intelligently and tactically maneuver while reducing the ability of adversaries to affect the overall mission. As shown in the exhibit, a user operating within the geographic region depicted, the HAN would provide protections for the entire mission through:

1. Multiple choices or options for a user to roam/maneuver across should an issue or threat occur
2. Ability to support a 'surge' in capacity demand to accommodate additional performance needs or an influx of units/users
3. Eliminate the ability of adversaries for disabling communications in a theatre through multi-path resiliency (across the ground, space, cyber domains).

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. Forces would not consider 'taking the hill' the same way every time, nor would hill defenders remain content to prepare for the same type of attack ever time.

The DoD should not enable adversaries to be successful in attacking our Satcom systems the same way every time. By combining private sector investment with those of the DoD, the DoD can achieve Network resilience for a fraction of the cost of new purpose-built systems while also imposing significant cost, technical, and material burdens on the adversary. The adoption of multi-network terminals and Hybrid Adaptive Network approach achieves the DoD's enduring mission to deny war and if necessary win at the "speed of relevance".

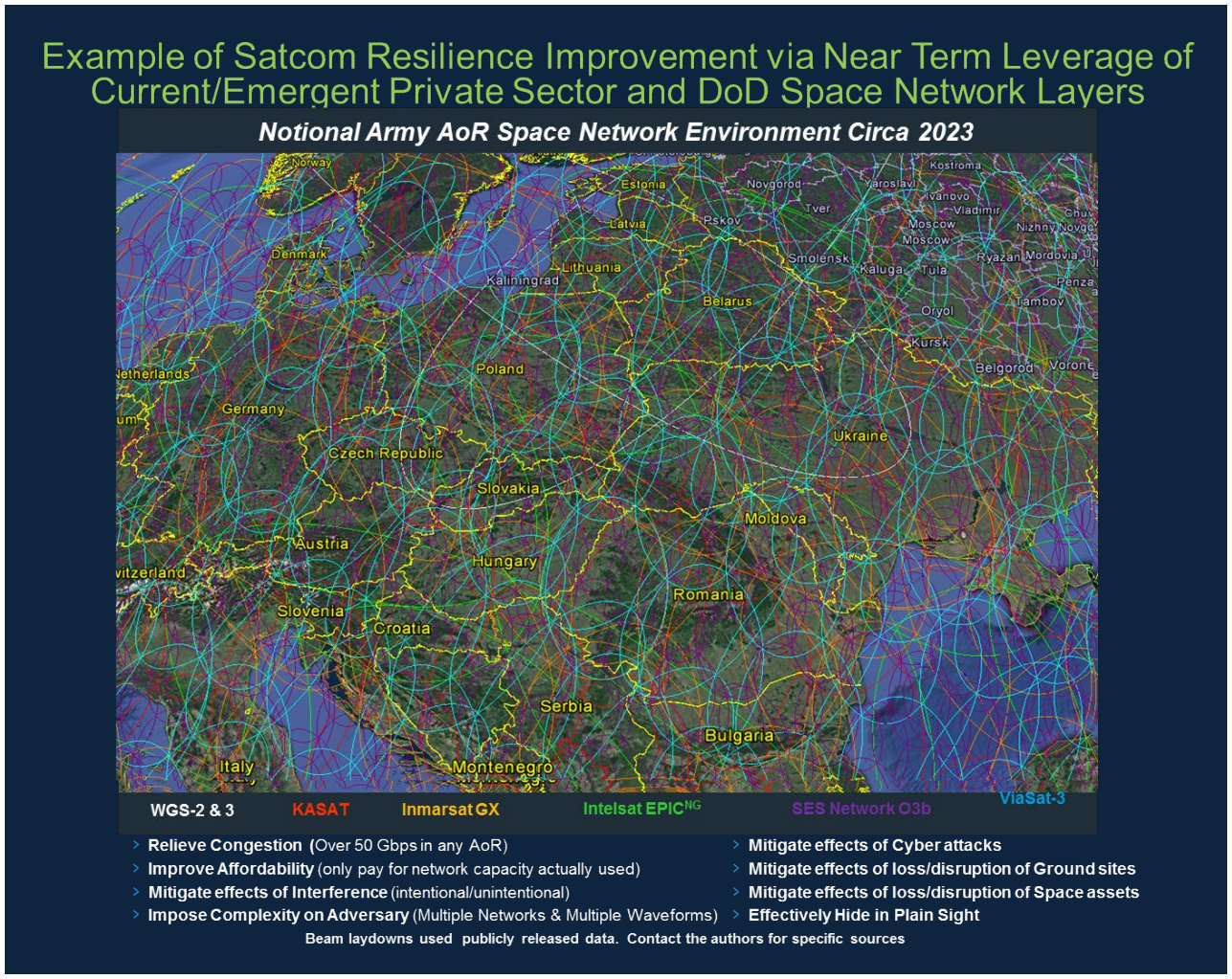

Exhibit 7: *Each layer added to the Hybrid Network improves the overall network performance and resilience by enabling path diversity across through a multi-orbit, multi-network ecosystem*

RECOMMENDATION

The fundamental recommendation is that the DOD can achieve their greatest improvement in their ability to perform their enduring mission by *agilely roaming across DoD purpose-built Satcom Network*, whether operating on DoD purpose-built satellites or commercial leased or acquired bandwidth, and the Private Sector end-to-end Satcom Networks. The path forward to implement this recommendation *merely requires that the DoD begin to employ multi-network terminals,* in cases where they desire improved resilience in contested environment and then ordering the service fulfillment for these terminals from one of potentially many HAN providers. The implement can be this simple, since the enabler is the multi-network terminals. The DoD and Private Secure governed networks exist; thus, the service capabilities and the means to acquire their services are both known.

This recommendation does not force the procurement of multi-network terminals, nor does it cause the DoD to forego their new purpose-built objectives in PATS (i.e. PTW terminal upgrade, PTES gateway, and PTS satellites) and ESS Satcom Networks, nor does it require the DoD invest in an Enterprise Management & Control system to implement multiple-network roaming. The DoD can continue to serve their existing terminals in the manner that they are served today, and when they want to order and fulfill service for an existing or multi-network terminal(s), they can choose to do this ordering and fulfillment via one of potentially multiple HAN providers that offer/fulfill aggregated independent Satcom Network layers through a web-based application or Portal.

Consider other portal applications that are commonly used today, consumers can order/fulfill a service or product from Amazon, from EBay, from another portal connecting customer to providers, or even directly from a provider(s). *This recommendation is merely* a means to leverage the DoD and Private Sector capabilities for dramatically *increasing resilience and deterrence in contested environments, today, while removing vendor lock and enabling continuous market-driven competition.*

The resulting OV-1, shown in Exhibit 8, has the DoD creating enduring access to numerous DoD and Private Sector Satcom Networks and even Line-of-Sight (LOS) Networks while creating market-driven competition and the ability to incorporate new Satcom and LOS Networks as they become available in the marketplace at the “speed of relevance”.

By adopting multi-network terminals and using a HAN Provider ordering/fulfillment service enables global response operations to achieve resiliency across all environments, situations and regions. This architecture creates a framework for accessing the layers of private sector networks and Government purpose-built systems. Together, they will provide enhanced connectivity to further advance the combined services available to disaster response teams, telemedicine units, and other global response users. Ultimately, the success of the operation is dependent on receiving access to experts, resources and leaders to be able to provide time-sensitive mission data, care, and response. Employing multiple networks within a single region, a hybrid network can ensure resilient connectivity to terminals and platforms. In order to take advantage of the benefits of hybrid networking, the following recommendations will facilitate and expedite user access to HAN Providers:

1. Deploy existing and future multi-network terminals that can interoperate on multiple private sector and DoD networks that can be software upgraded to support additional future networks (shown in Exhibit 9)
2. Leverage infrastructure available from Satcom Network Providers that facilitate access to multiple networks for expanding hybrid networking
3. Adopt HAN Management portals and capabilities within mission planning, monitoring and managements tools and infrastructure. The integrated tools and capabilities allow unified management and monitoring across independent networks and diverse regions

4. Independently and systematically evaluate current and private sector networks to identify weaknesses or limitations within each network and determine which combinations of networks will provide mitigations against possible threat vectors.

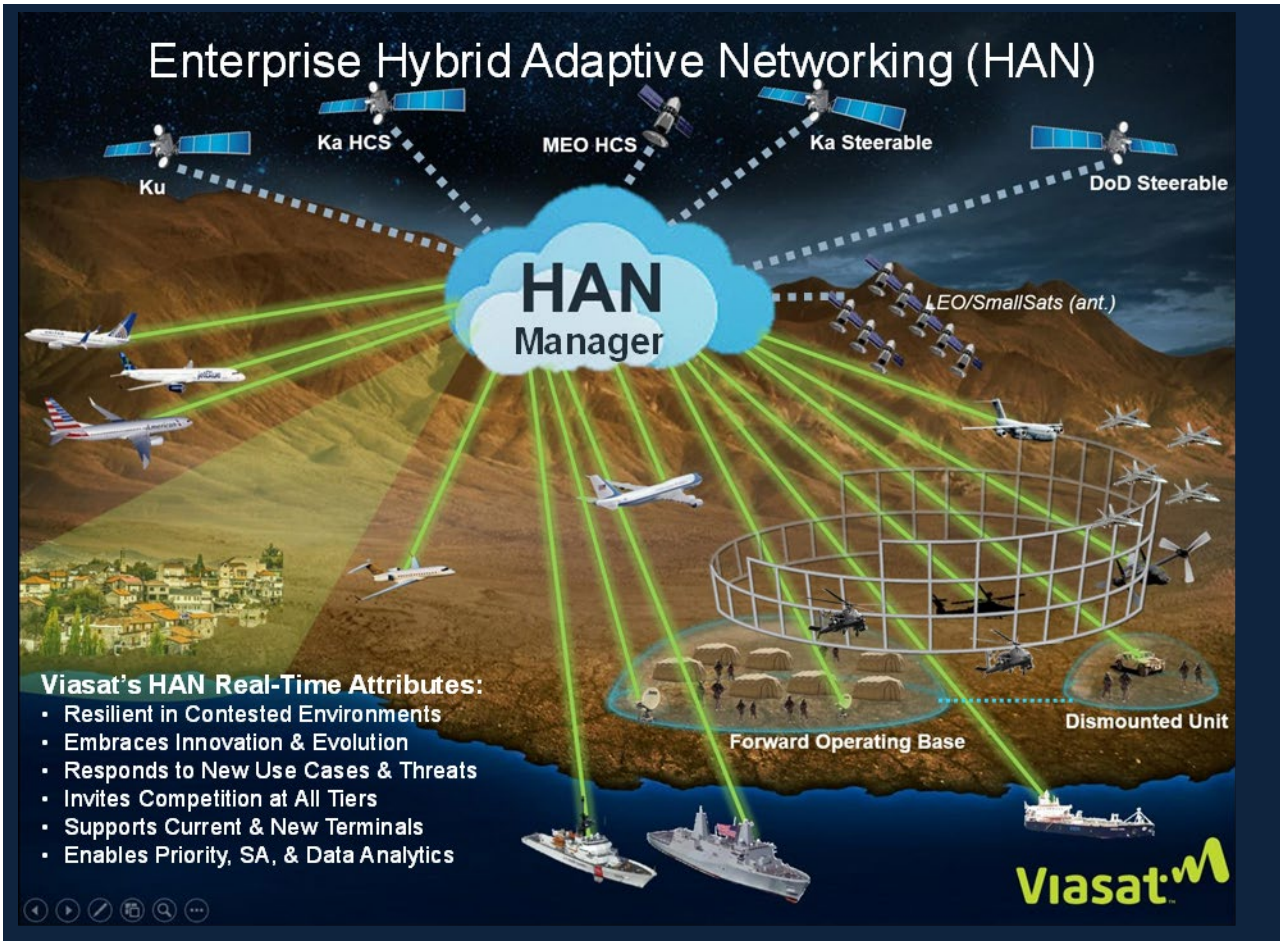

Exhibit 8: *Multi-network terminals and ordering/fulfilling service through a HAN Provider creates assurance and resilience in Contested environments, embraces innovation and evolution, enables timely response to new use cases and threats, invites competition at all tiers (terminals, Satcom Network Providers, HAN Providers, etc.), and supports the existing and future terminals, while enabling priority and Network Situational Awareness and Data Analytics.*

In conclusion, while the above analysis indicates that several individual private sector Satcom Networks are more resilient than current DoD purpose-built, overall warfighter capability can be maximized using multi-network terminals to use all of the existing and forthcoming capabilities. Warfighters will gain the ability to seamlessly roam across multiple private sector and government communication systems adding both deception and maneuver to Satcom or the Space Domain. The recommended implementation 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 creates 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 and aggregating HAN 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.

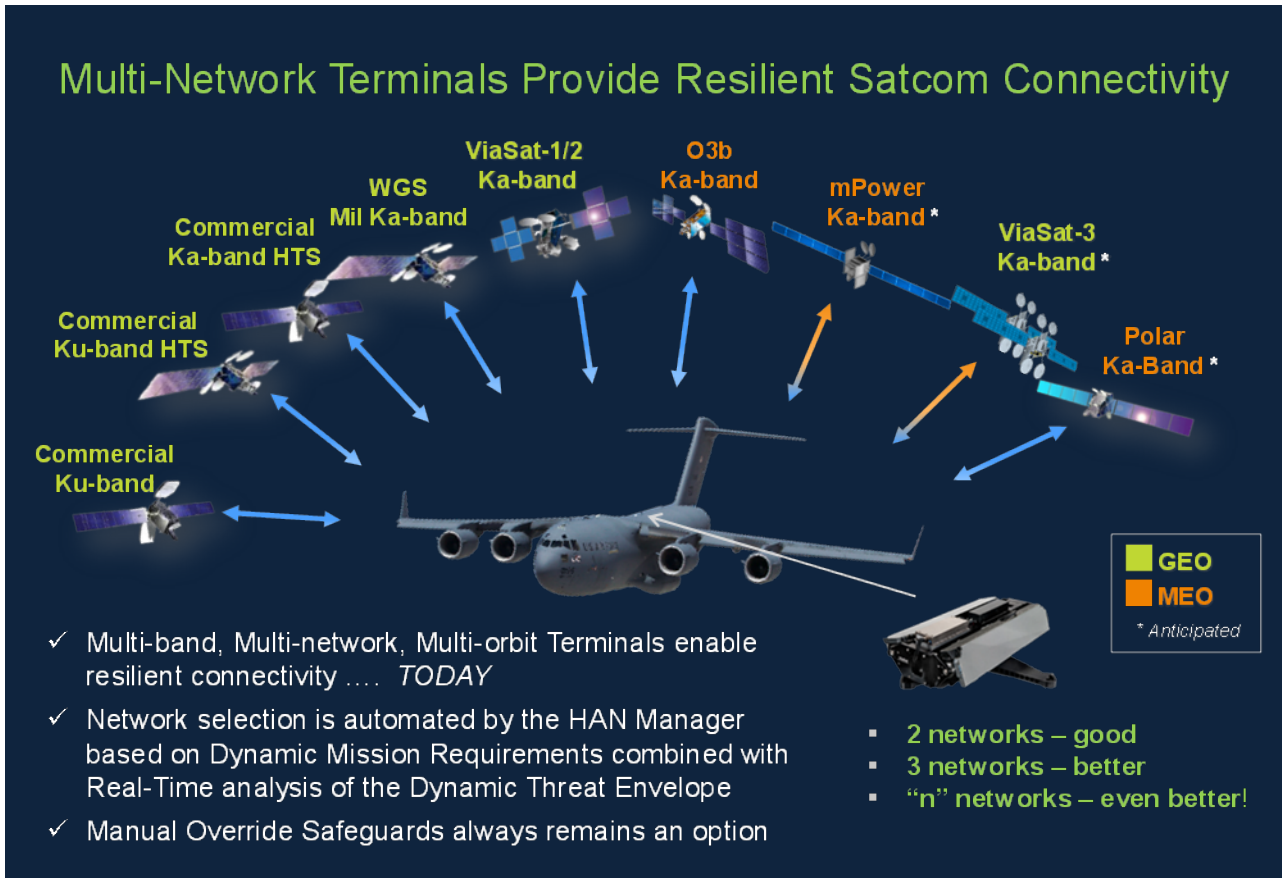

Exhibit 9: *Multi-network terminals like the ones employed today by the USAF that have shown mission interoperability on Ku, WGS and Commercial Ka, MEO Ka are the foundation to continue to leverage the new capabilities of advanced GEO, MEO, and LEO Satcom Networks.*

---

[1] https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf,page 1
[2] https://spacenews.com/future-military-satcom-system-puts-cybersecurity-first/
[3] https://spacenews.com/future-military-satcom-system-puts-cybersecurity-first/
[4] https://www.defense.gov/News/Article/Article/1318291/mattis-dod-lines-of-effort-include-building-a-more-lethal-force/
[5] https://spacenews.com/space-force-proposal-shifts-satellite-communications-procurement-to-air-force-secretary/
[6] https://www.stratcom.mil/Portals/8/Documents/CSpOC_Factsheet_2018.pdf
[7] Exhibit 4 and 5, the resilience scoring of the individual networks are based on publicly released data. Please contact the authors for specific source material and detailed scoring assessment.
[8] Exhibit 8, the beam plots are based on publicly released data. Please contact the authors for specific source material