

## **ADVANCED ENTERPRISE SITUATIONAL AWARENESS REPORTING FOR ENHANCING SPACE OPERATIONS**

**Craig Miller**

Viasat Inc., [craig.miller@viasat.com](mailto:craig.miller@viasat.com)

**Fred Taylor**

Viasat Inc., [fred.taylor@viasat.com](mailto:fred.taylor@viasat.com)

**Meredith Caliguiri**

Viasat Inc., [meredith.caliguiri@viasat.com](mailto:meredith.caliguiri@viasat.com)

### **ABSTRACT**

Enterprise SATCOM Networks generate end-to-end Situational Awareness (SA) combining space, security, network, and cyber operations to inform space operations decisions. This SA extends from Warfighter Applications through the space systems to DoD networks (DoDIN) to aid in making informed decisions in conflict. This information provides a comprehensive picture of the health of the networks used by warfighters, the environment/domains in which they are operating in, and provide Indications & Warnings to identify threats. This information is essentially to effectively maneuver across government and commercial SATCOM transport network layers to enable Multi-Domain Operations employing a resilient space enterprise used by warfighters.

This paper explores the different types of situational awareness that is available within space networks and how it can be combined with the advanced capabilities of Enterprise SATCOM networks to inform operational decisions, disseminate mission critical information to warfighters, and provide improved connectivity to the spectrum of users. The information available extends from individual user Situational Awareness through the DoDIN to include information useful for detecting cyber threats, monitoring atmospheric and space weather, identifying intentional and unintentional interference sources, gateway health, and other potential outages or interruptions.

Additionally, the paper discusses how emerging technologies will be able to offer improved effectivity in the presence of interference sources by limiting its effects by countering and isolating any interference sources. In addition to inherent resiliency measures being deployed with future COMSATCOM networks, users can further improve overall effectiveness of their communications by employing multiple layers of resiliency through path diversity made possible with hybrid networking to ensure access to multiple transport networks. When combined with networks that have advanced protections in place to detect, monitor, and mitigate the effects caused by threats, a resilient network framework is available on demand for warfighter operations in conflict regions.

### **EXPANDING NETWORK MONITORING CAPABILITIES FOR IMPROVING NETWORK RESPONSE**

The ability to communicate is essential to successful military operations. The 2017 National Security Strategy calls for uninterrupted and secure communications and services under all conditions.<sup>1</sup> Fundamental to fulfilling this mandate is Enterprise Situational Awareness providing decision-makers at all levels to use data to understand the operational environment and make sense of information to analyze multiple simultaneous situations, scenarios, threats, and courses of action. Situational awareness forms the basis of decision in a dynamic, diverse communication ecosystem. The stove-piped, segmented approach to situational awareness does not work for high-velocity operations against a sophisticated adversary in a contested environment where threats

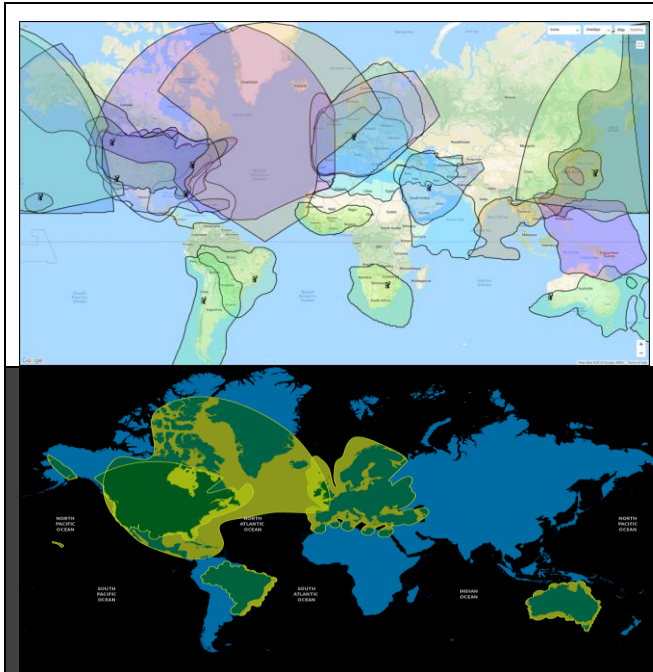
can vary widely in type and scale, from localized events contained in a single region to global events that might span localized, regional, and global boundaries. Warfighter's decisions must be supported with the best possible information to mitigate attacks and ensure successful operations. Key attributes of Enterprise Situational Awareness are persistence, interoperability, pervasiveness, and availability, not only regionally but globally all of the time across constituencies. Enterprise Situational Awareness is a force multiplier that provides operational agility creating an environment in which there is a shared level of understanding, identification, synchronization, and response based on risk considerations, indicators, objectives and outcomes. Satellite networks are more than the spacecraft and should be pervasive and inclusive of all network transport layers. Network outages limit operational agility and simultaneity of action and may limit essential understanding of key network terrain for cross-domain operations. Networks should also provide visibility, status, and reporting of all elements in the network architecture from the backhaul through the satellite to the end user devices/applications and consider relationship-based interactions of components and users, priorities, and threats inside and outside of the enterprise.

This recognition is most evidenced by DoD's emphasis on Multi-Domain Operations (MDO) which harnesses the vast amount of information from joint and allied sensors to quickly fuse data into decision-quality information to create effects simultaneously, from any domain or component from anywhere in the world."<sup>2</sup> A prerequisite and enabling capability for the MDO operational concept is ubiquitous situational awareness provide by space and terrestrial networks and the ability to share information at the "speed of need." Space capabilities, and associated situational awareness, are essential elements of Multi Domain Command and Control (MDC2). The Joint Force has placed a premium on Space Situational Awareness (SSA) to protect & defend space assets and deliver operational effects to terrestrial warfighters. The Air Force has relied on SSA to understand what is in space and what is going on in the space domain as it relates to sustained satellite operations for continuous preparation of the battlespace by accessing sensors and systems to gather intelligence, synchronize operations, manage resources, and support decisions.<sup>3</sup> However, SSA in MDO must address the entire enterprise to include the backhaul, satellite, network, gateways, terminals, and spectrum.

The importance of having holistic, cross-domain understanding of the situation has been clearly illustrated in recent military exercises in which Functional Teams required a Common Operating Picture (COP) for Enterprise SATCOM Situational Awareness to provide greater end-to-end comprehension of operational priorities, availability, performance, operational impacts, and threats. However, existing DoD tools lack the necessary level of fidelity, scope, information, and accuracy. In contrast, private sector networks have built Common Operating Environments with real-time situational awareness tools for sustained network operations and assured service delivery to millions of devices across the enterprise. Brigadier General Chance Saltzman, a visionary space professional and architect of the Air Force's Multi Domain Operations strategy, pointed out that the Air Force knows there is a host of commercially available, state-of-the-art technology that will enable the service to make faster decisions, provide better situational awareness and assured direction of forces.<sup>4</sup> Advanced private sector network enterprise tools and displays are in use today at many commercial managed service providers that could be rapidly adopted or modified for DoD specific use in space operations for MDC2 without the long-lead time and expense to develop a comparable tool by the DoD. This service offering could complement other existing tools for an expansive catalog of capabilities depending on user needs.

### PRIVATE SECTOR INNOVATION APPLIED TO ENTERPRISE SITUATIONAL AWARENESS

In order for commercial satellite communication networks to improve their overall resilience, reliability and availability the private sector has made significant investments in management tools, active cyber defense, security and monitoring, network awareness, and data analytics to gain Enterprise Situational Awareness to protect their networks. System operators have increasingly demanded better insight into performance capabilities and response options to accelerate their ability to deliver assured service, respond to anomalies, mitigate outages, and satisfy time-sensitive requirements across the space, ground, terrestrial, cyber and terminal architecture. As a result, networks are being continually enhanced to provide improved methodologies for identification, categorization, and management of these highly-complex and integrated multi-layer networks. First-tier, modern communication networks, including Viasat's global space-ground network, have developed advanced tools, protocols and automated responses that enable better monitoring of key performance parameters, state of health of both the network and users populating the enterprise, and system-wide knowledge of network interactions. For example, Viasat's integrated network topology currently connects users over dozens of Ku- and Ka-band satellites across different waveforms, orbits, ground networks, modems, and terminals to service hundreds of thousands of users across domains. This enterprise architecture is able to flexibly manage fixed residential and mobile airborne/sea-based users without pre-defined capacity assignments to seamlessly connect millions of user devices across multiple networks and securely deliver over 450 TB of user traffic each day. The enterprise management requires advanced capabilities that allow efficient and effective detection and mitigation of issues to limit outages, isolation of threats, and achieve overall Quality of Service for a diverse user population.

	<p>Global situational awareness for sustained operations and enterprise management across:</p> <ul style="list-style-type: none"><li>• Multiple Ku and Ka satellites</li><li>• Distributed ground stations</li><li>• Fiber/TCOM infrastructure</li><li>• Operations and Management Infrastructure.</li></ul> <p>With decision aids to enable comprehensive management and monitoring to serve mobile, fixed and airborne users.</p>
<p><b>Exhibit 1:</b> Global Service Networks holistically manage users across multiple space/ground networks using advanced SA monitoring to minimize outages, mitigate threats and respond to service anomalies.</p>	

Service delivery to a wide-range of mobile and fixed government, business, enterprise, and consumer users, network service providers leverage an expanding array of sophisticated decision and automation tools to operate, monitor and manage their enterprise networks that fluctuate with user demand. This includes secure local and remote access to correlated information within a response relevant timeframe. The essence of this functionality is to provide system intelligence engines or network operators with pertinent information to understand what is occurring across the enterprise and make timely, appropriate decisions. The challenge is not necessarily having enough data but rather having the right data necessary for a decision at the right level and the right time. A large volume of data from across the enterprise that can be used to make connections, understand relationships and priorities, and highlight interdependencies enables the generation of high-confidence decision-quality information. In a highly dynamic environment the quality of decision is not necessarily measured in speed but more accurately by the ability to rapidly weigh options, assess risks, and take appropriate action to meet SLAs within a changing context defined by network status, user needs and threats. Viasat's, and others, operational agility and reliability is maintained by applying integrated Enterprise Situational Awareness for resilience, elasticity, and efficiency in competitive and contested environments. Private sector High Capacity Satellites (HCS) network service providers collect and use data analytics from their networks to quickly isolate, detect and respond to issues; and through a sophisticated enterprise architecture, conduct proactive performance analysis and optimization to service a myriad of operational use cases. Several data analytics capabilities, including machine learning systems, provide network operators and managers valuable insights into each distributed and complex network that enable them the ability to respond quickly and effectively to changes across the networks.

#### **COMPREHENSIVE SITUATIONAL AWARENESS FOR ENHANCED SATCOM MONITORING**

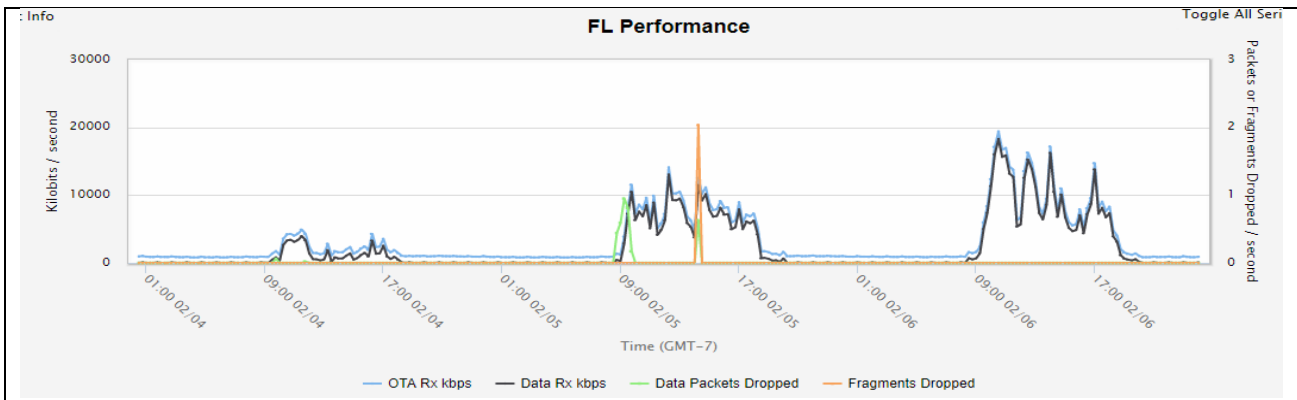
Key performance indicators (KPIs) are used to measure operational performance and success in fulfillment of service level agreement/operational priorities. Real time status by extracting data feeds from existing network COPs or defining new COP Metrics are used to detect anomalies and quickly identify performance irregularities that span traffic rate metrics, service flow information, signal quality data, and beam related information. Sensors and automation tools provide intelligent operational status, performance characteristics and mission trends of each segment of the network enterprise. Detailed analytics are used to optimize performance and proactively respond to potential outages through preventative measures. When required, operators are alerted of potential issues and can actively "drill-down" on network elements from the satellite to the end user terminal in real-time.

The objectives for using integrated metrics is to enhance (1) the visibility of threats or issues across the SATCOM domain (2) identify issues (preferably before they occur) that impact service delivered to the warfighter that would impact their ability to maintain reliable communications. While this is inclusive of monitoring space based threats for detecting interference (intentional or unintentional) against a space asset or monitoring for orbital conjunctions, it requires expansion to include each of the integrated elements necessary to operate a SATCOM Network. This is inclusive of (a) Space assets, (b) Ground sites or gateways (antennas, modems, physical infrastructure), (c) Data Centers or Network Operations Centers, (d) Fiber, (e) Cyber Operations Centers, (f) Space Operations Centers. The idea is to utilize a system that allows for the inspection of the network health at the macro level and allow for operators to drill-down into detailed performance information to isolate and identify specific issues.

Space operators must be able to anticipate, develop, analyze, validate and prioritize SATCOM requirements in conjunction with operations in space, cyber, air, land and sea. This is done by developing performance and threat indications & warning to create specific SATCOM situational awareness requirements in which the system can intelligently convert those requirements into network tasks for execution, monitoring, assessing, location and resourcing. For instance:

**User Traffic Metrics:** Traffic (IP or Ethernet) user data metrics (examples shown in Exhibit 2) provide a first-order view of user traffic to identify whether a user terminal is receiving appropriate service in accordance to their service level agreement. This information allows operators or mission managers to quickly identify an outage or issue with the service being delivered to a user. Traffic metrics might include the following:

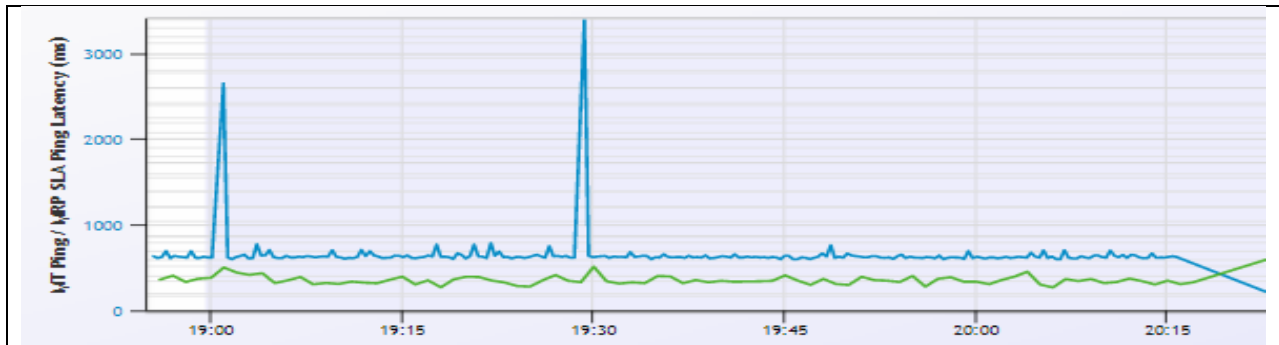
- Traffic data rate (kbps): sent (RL), received (FL), dropped or malformed
- Traffic data packet rate (pkt/s) to include sent, received, dropped or malformed



**Exhibit 2:** Example Display to quickly identify any service fulfillment issues to an individual user by monitoring performance information (e.g FL data rate and packet loss)

**Quality of Service:** Service-based traffic metrics to include traffic type information and other network health related details. This information is useful to ensure the network experience meets the mission requirements or objectives (e.g. protection against cyber threats; meets user experience requirements for latency and/or jitter)

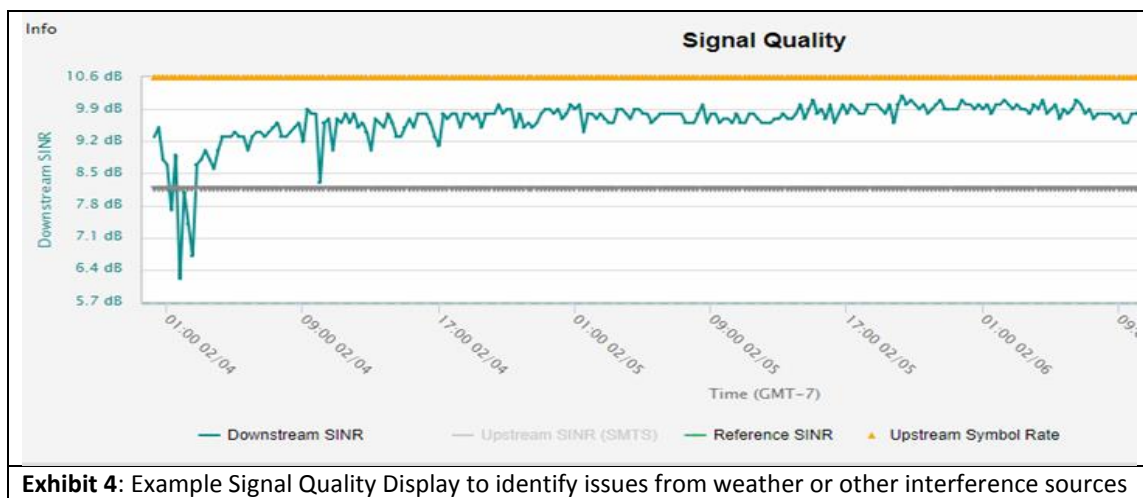
- Traffic type (e.g. UDP, TCP; etc.) for performing cyber analytics
- Protocol in use to identify cyber-related issues
- Quality of Experience metrics for monitoring round-trip time or latency for isolating issues (in Exhibit 3)



**Exhibit 3:** Example Latency Monitoring to Identify QoS related issues for service fulfillment monitoring, particularly during latency impacted communications or missions

**Link Performance Metrics:** SATCOM link performance metrics (an example is shown in Exhibit 4) provide an overview of the RF performance on a single satellite, useful for monitoring any signal degradation issues related to weather, interference or other signal impairments. Correlating performance issues to a network, terminal, or region is possible using RF metrics, particularly in contested environments. Note: “SNR” is generic for Es/No, Eb/No, etc.

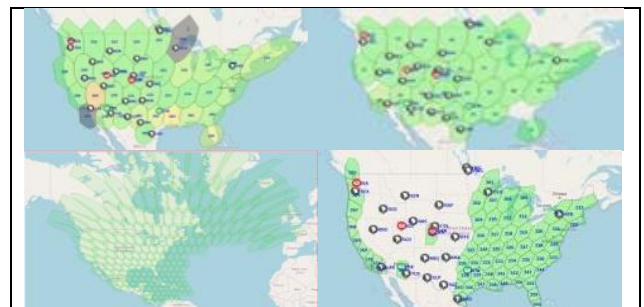
- Forward and Return SNR (dB) for identifying any issues from interference
- User Measured FL/RL SNR (dB) for identifying any issues with interference/weather
- Carrier Assignment: logical association of virtual connections to carrier(s) for each modem
- Burst Assignment: the burst time plan in TDMA/CDMA networks, to aid interference detection
- Carrier Utilization: usage and congestion of the carrier(s) in the network



**Exhibit 4:** Example Signal Quality Display to identify issues from weather or other interference sources

**Global Utilization Metrics:** Enterprise SATCOM monitoring provides a comprehensive and holistic view of the global network (or blended set of networks) that includes beam or satellite capacity. Additionally, it provides information on the activity of a user terminal traversing multiple beams / satellites (in-network) and the transitions across networks (out-of-network):

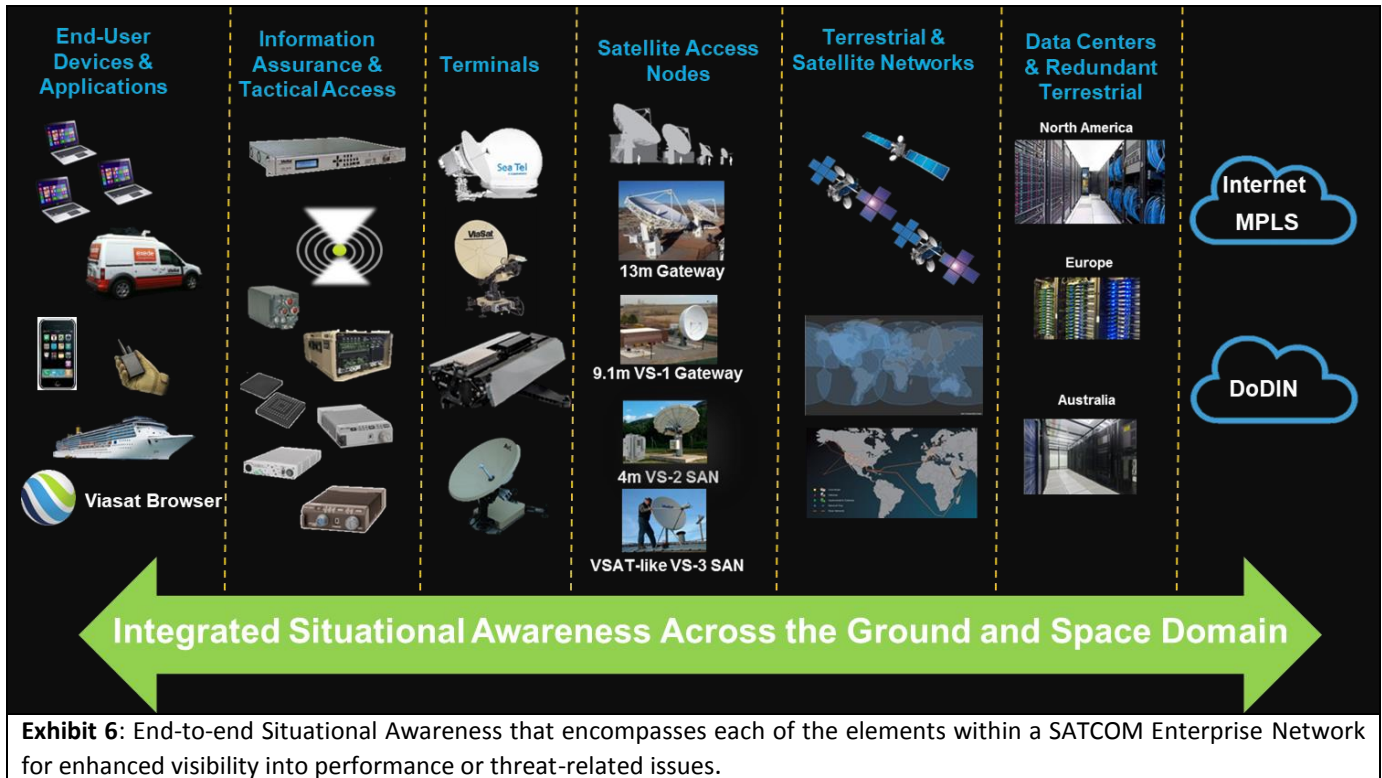
- Beam Assignment for displaying logical association of modems to beam(s) on satellite(s) in the network for identifying any service impacts related to a specific beam
- Network Utilization would provide performance, availability and congestion information for users within a specific region
- Performance and Coverage Maps (shown in Exhibit 5) provide network details to include availability, geography, and coverage information necessary for accessing a network



**Exhibit 5:** Ability to monitor the individual beams across an integrated network

End-User Metrics: End-user device (EUD) metrics show the number and types of end-user devices accessing the network. High Throughput Satellite (HTS) networks with integrated cyber capabilities can assess cyber-vulnerabilities of many end user devices by monitoring for specific signatures that are known threat sources. This information can be used to monitor and detection of intrusions or malicious activity from adversaries:

- End-user device identification for identifying compromised users or applications
- Active ports and protocols for identifying abnormal traffic patterns (e.g. large number of in-bound requests from a particular IP address)



As end-to-end enterprise monitoring capabilities, inclusive of the elements like those shown in Exhibit 6, continue to evolve to further expand the information available to both internal and government operators, the nature of conflict to maintain/gain positions of advantage will redefine and compress decision-response cycles by providing decision-makers access to real-time advanced Enterprise Situational Awareness. Today's modern SATCOM networks have the ability to analyze, detect, collate and report relevant information, either to local operators or remote government operators. This enables rapid threat response and attack mitigations from a myriad of threats to include real-time detection of cyber threats that can identify and prevent the attack from propagating through the network. Additionally, networks can identify, characterize, and geolocate jammers for a coordinated network response. While this information is necessary for maintaining the health of the network for reliable service continuity, it is also relevant to government operations centers to access this rich set of enterprise situational awareness already being utilized and expanded by enterprise networks.

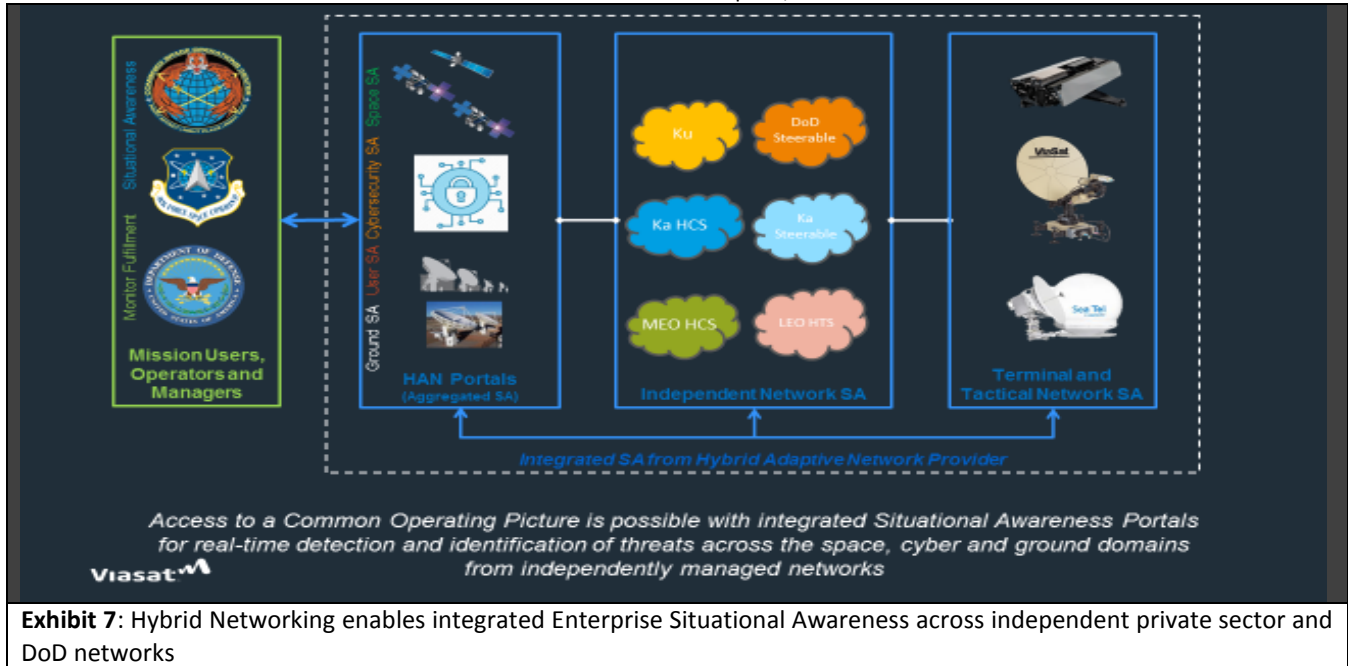
## **HYBRID NETWORKING COMMON OPERATIONAL ENVIRONMENTS FOR ENTERPRISE MANAGEMENT**

The Air Force Future Operating Concept envisions a 2035 future in which static and unadaptable communications systems have been replaced with more distributed, dynamic and automated networks that provide intelligence in machine-consumable formats and allows the Air Force to leverage more commercially available data sources to swiftly support decisions.<sup>5</sup> To that end, the Hybrid Adaptive Network (HAN) concept approaches SATCOM as an enterprise comprised of a layered, heterogeneous network encompassing a mixture of multiple private sector and purpose-built SATCOM systems. This hybrid network architecture provides the greatest performance and mission assurance using the best available network for intelligence collection/dissemination, increased lethality, and survivability in a contested domain. This layered system of systems also provides much greater resilience across all threat vectors than any single network can. By taking advantage of the resilience possible within each of the individual networks, and by layering multiple networks for diverse, agile communication options end-users are able to securely access multiple networks to service diverse mission needs and priorities.

In multi-domain operations, the government will continue to use a combination of government purpose-built and commercial SATCOM networks from a variety of providers. It will become increasingly necessary to access hybrid management portals able to integrate situational awareness and capabilities across an amalgamation of networks as a federated enterprise. Situational awareness can be extended across networks to provide a comprehensive, composite view of the battlespace. Individual networks will provide varying degrees of information. Individual SATCOM architectures that have less cognizance of the components, users, threats and missions may contribute less data in conflict, but when integrated with advanced enterprise architectures that data, in aggregate, can provide valuable situational awareness to the warfighter. With hybrid adaptive networking warfighters are able to gain situational awareness of layers of transport networks and prioritize path diversity based on mission and threat intelligence to seamlessly roam across a highly resilient enterprise network. However, in order to fully take advantage of the benefits of hybrid networking, an enterprise management system is needed to provide an integrated network and user view along with corresponding health information. Instead of multiple disparate and disjointed tools for government operators to monitor users and performance, the Enterprise Management system would establish a Common Operating Environment across each of the constituent hybrid networks. This cohesive capability will combine SA metrics, health, performance, threats, and outages for ensuring government operator timely access to relevant intelligence.

Viasat routinely conducts multi-system analyses of the enterprise (e.g., in evaluating gateway diversity), to gain greater insight into operational effectiveness. From our analysis, we have concluded (1) No single network is resilient against every combination of threat vectors and (2) individual networks with relatively low individual resilience can be combined to create a network that has very high aggregate resilience and increased situational awareness to inform risk decisions.





Using integrated HAN Enterprise Management Tools operators can access aggregated network information to determine the health of individual networks and status of the federated enterprise. Cyber threat information, alerts, geolocation of interference sources, and weather degradation are priority information requirements for government space operations in monitoring their deployed users and corresponding access to network information for mission success. The HAN Management system shown in Exhibit 7 can also enable disparate sets of commercial SSA data to be accessible through a standardized format used for the space catalog data processor. The standardized interface leverages an open architecture for facilitating the ingestion of commercial data sources and types which is directly accessible from HAN Portals.

#### **HYBRID NETWORKING WITH ENTERPRISE SITUATIONAL AWARENESS APPLICATION IN MDO**

The Hybrid Network Management Portal provides user/role-based views and access to enterprise network information. Secure, remote access eliminates the need for a single operations center and provides the ability for shared situational awareness. From an interactive portal users can utilize tailored dashboards in order to drill-down into network information for current operations, mission planning, Course of Action development/war-gaming scenarios, deliberate planning, and/or intelligence preparation of the battlespace with this evolved approach to SSA.

The Combined Space Operations Center (CSpOC) executes operational command and control (C2) of space forces to achieve theater and global objectives using a multi-layered network to coordinate, C2 and manage assets to ensure space capabilities are available to theater components at the right place and the right time to achieve the theater mission<sup>6</sup>. The SATCOM Integrated Operations Division (SIOD) reports to the CSpOC and is responsible for the integration, synchronization and coordination of all military SATCOM, to include commercial services leased by the AFSPC Commercial SATCOM Office, in any operating environment to improve collective SATCOM agility and resiliency to improve the Joint Force Space Component Commander's ability to deliver SATCOM effects to the warfighter.<sup>7</sup>

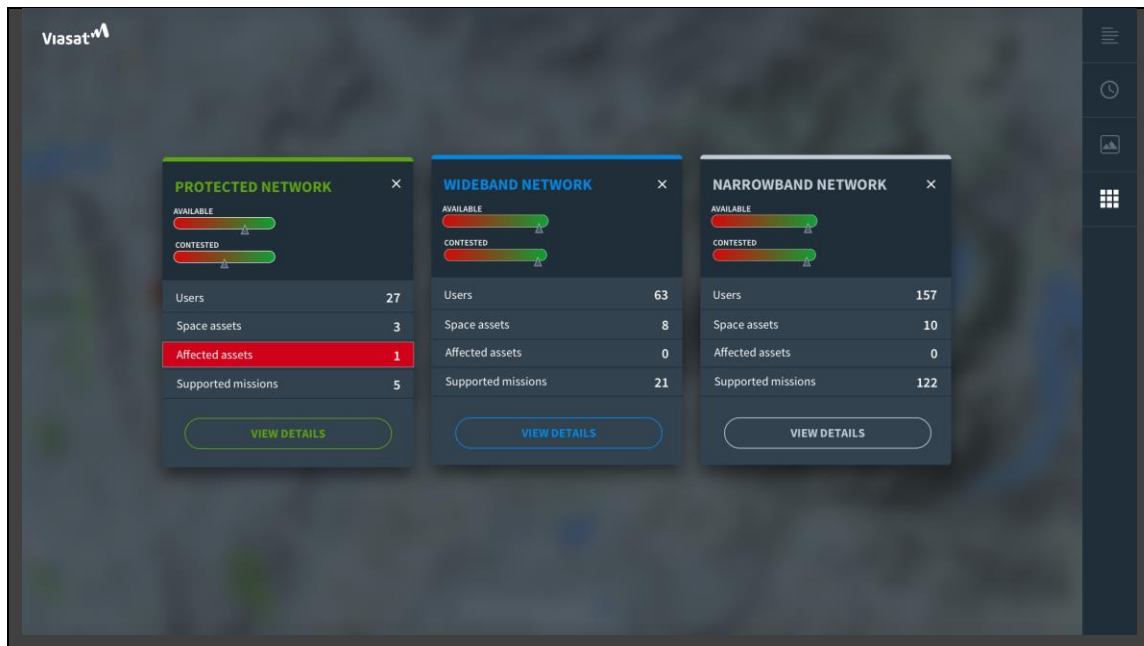
**SITUATION:**

In a notional operational scenario leveraging the HAN, the CSpOC is tasked to provide space effects in support of a Geographic Combatant Command (GCC) operation. A joint force package is ingressing into a contested area of operations to execute a cross-domain mission supported by assured SATCOM from government and commercial networks. The CSpOC provides C2 of space forces in synchronization with the theater Joint Operations Center. At the operational and strategic level operations centers and SIOD maintain shared situational awareness necessary for MDC2 across the globe.

As the operation commences, indications and warning tip of a potential collect or attack -- jamming, kinetic, or cyber threat to an operational SATCOM network which could impact the mission. How quickly can the operations center identify which warfighter units are operating on the SATCOM network and monitor, assess, plan and execute an effective response? Should you maintain operations, maneuver to other SATCOM networks, organize dummy traffic, or other response in synchronization with other cross-domain operations?

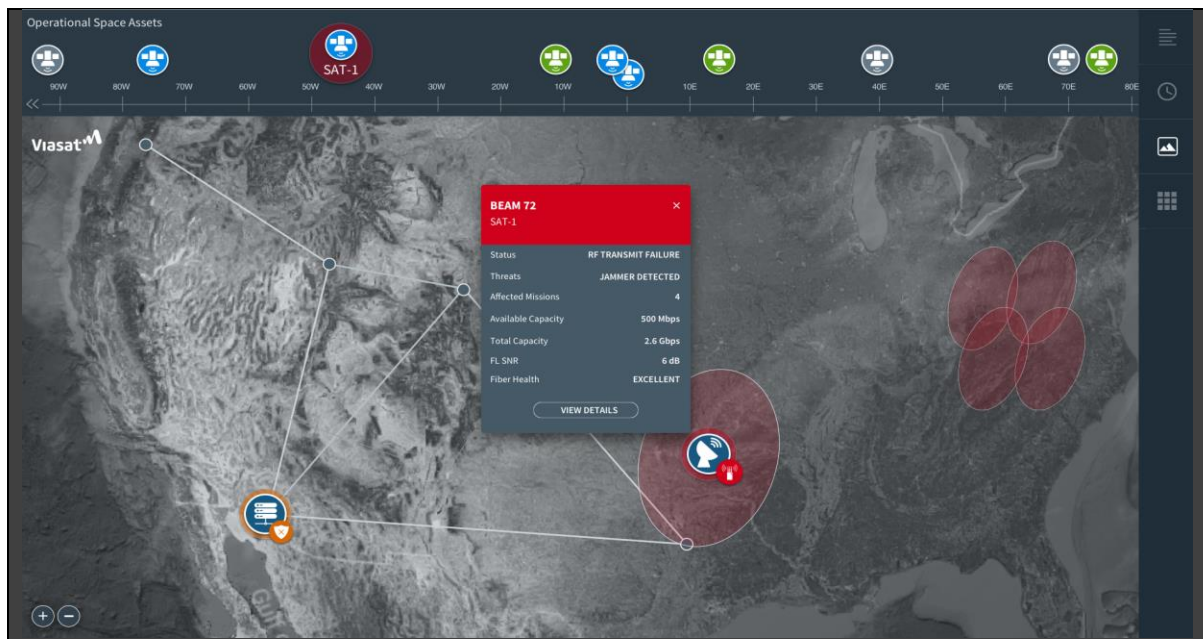
Shared situational awareness of the communication enterprise is maintained through a Hybrid Network Management Portal that provides visibility of all network service layers, DoD and commercial, in a multi-network integrated architecture to provide indications & warnings, correlate threats, respond to network and space segment attacks/outages.

Real-time operational situational awareness and visualization provides a tailored dashboard of global status (shown in Exhibit 8) and priorities in order to monitor, assess, plan and execute assured communications for joint missions that may scale to hundreds of simultaneous cross domain operations in a Hybrid Network. Operational priorities, requirements and threat indications inform overall operational status, availability and alert levels.

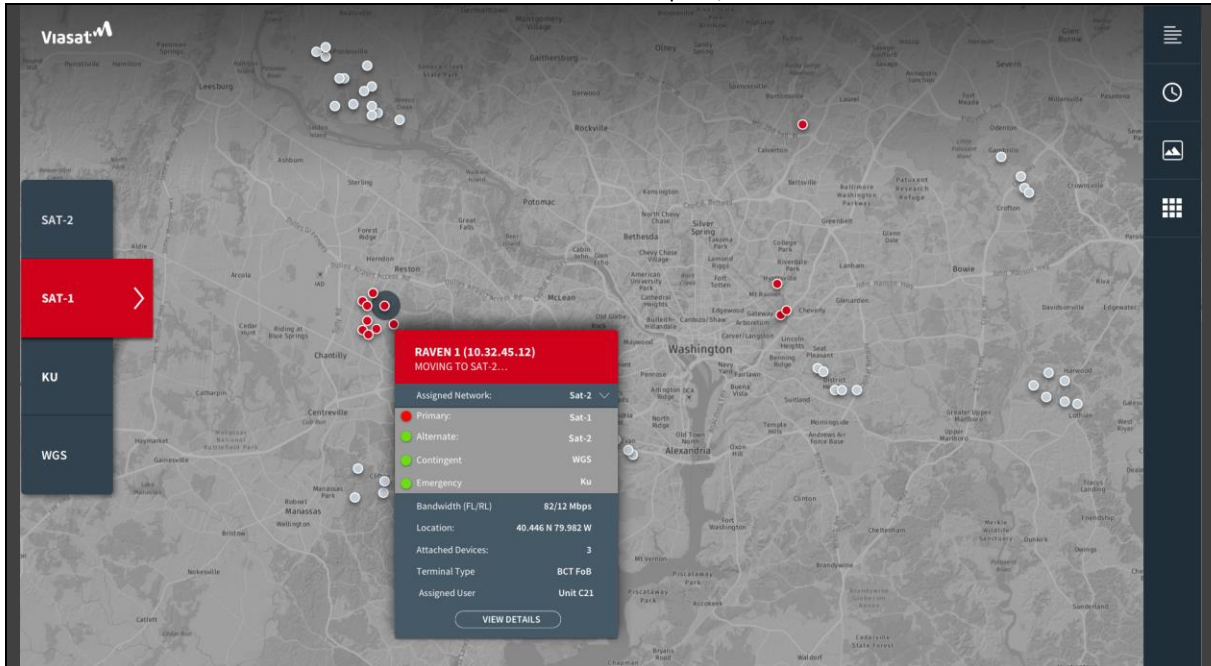


**Exhibit 8:** Macro level network monitoring enabling rapid detection of issues across the networks used for global operations

In machine time, indications and warning alert the SIOD of adversary actions impacting SATCOM service for the on-going mission. The SIOD is able to assess the situation while also managing other warfighter priorities. Real-time operational situational awareness and visualization provides an operator dashboard of global status and priorities to including beam usage statistics, individual user Forward Link/Return Link performance with management and control applications to plan, resource and track execution of the specified operation per the Joint Space/Air Tasking Orders for the mission Operational priorities, requirements and threat indications inform overall operational status. SIOD and other role-based users are able to securely monitor commercial SATCOM managed service delivery in real-time and adjust enterprise priorities through the portal application to address any changing warfighter requirements or system status.



**Exhibit 9:** Operators can drill-down into individual networks to isolate and identify issues in real-time.



**Exhibit 10:** Operators can drill-down into individual users to examine network assignment and examine service fulfillment.

The MDO concept is predicated on this integrated concept and data access feeds to analyze, respond, and automatically recover services in near-real time for assured cross-domain operations. The Hybrid Network Management Portal is able to collect operational status from the user terminal/warfighter and can automatically reassign the service to another network service layer in the event of an outage or congestion in accordance with user defined priorities and missions. Drilling down to lower-levels (Exhibit 9 and Exhibit 10), authorized users can gain additional information on the terminal and user applications. In this example, the SIOD can see that the impacted user is Raven-1 and is equipped with a Multi-mission terminal that can roam across networks and has already been automatically reassigned to an alternate communication network in another band provided by a commercial High Throughput Satellite. Real-time situational awareness and automated tools that monitor, correlate, report threats and operational status with real time visualization, analysis, management and response enable the SIOD to see the affected user(s) and other users across the theaters. This view is simultaneous shared and reported at the CSPOC and the GCC which triggers a decision to address the threat cueing airborne and space-based ISR and strike assets to service time-sensitive targets.

Overall, a hybrid network can provide enhanced Enterprise Situational Awareness in contested environments across networks, systems, terminals and satellites driven by warfighter priorities. Enterprise SA allows the network operator to rapidly prioritize SATCOM capabilities leveraging a combination of government and commercial networks best able to deliver operational effects and sustain mission operations based on operational imperatives.

## CONCLUSION

The 2018 National Defense Strategy summarizes the state of affairs best: “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.”<sup>8</sup> Many of the technologies for advanced SATCOM networks and requisite Enterprise Situational Awareness directly improve the resilience, elements of deterrence, and the mission assurance of both commercial SATCOM/DoDIN networks. Situational awareness is essential for decisions, resource allocation and assured operations in a contested operational environment.

In multi-domain operations warfighters requires assured communications for timely information exchange. The foundation for successful operations is a robust network that can operate through attack, seize windows of opportunity, and detect and respond to outages or attacks in a complex operating environment. Using a systems of systems approach treats the communication network as an integrated enterprise solution, rather than severable parts. It is not merely the satellite that provides to capabilities of the system, it is the satellite, the ground segment, the network management and other components of the system working together to form a cohesive network that is greater than the sum of its individual parts. Evolving the approach to SSA to integrate the enterprise will enable faster decisions, converge responses and support the warfighter in a contested domain.

The private sector continues to improve its enterprises, services and situational awareness tools. By accomplishing the Congressional mandate to establish DoD processes that enable rapid adoption within the cycle times of commercial SATCOM network innovation the DoD can markedly improve its cognizance of SATCOM operational status and effectiveness to deliver operational effects in contested Multi Domain Operations.<sup>9</sup>

To advance DoD’s ability to evolve and enhance their Space Situational Awareness capabilities and gain Enterprise Situational Awareness necessary for Multi-Domain Operations requires:

1. Understanding the capabilities and information that is utilized by the private sector with aggregate service delivery through Hybrid Adaptive Networks and leverage that innovation in government network enterprise SATCOM services.
2. Gain access to relevant (and comprehensive) information in a unified fashion. This can be accomplished through a standardized interface from private sector networks through promotion and adoption of the interface within Government networks for exchanging situational awareness information.
3. Leverage the investments within the private sector for developing enterprise situational awareness monitoring portals, tools and infrastructure necessary for managing, operating and maintaining reliable communications across blended networks that is inclusive of each integrated element across space, ground, and terrestrial domains to enable automated and intelligent response to threats.

---

<sup>1</sup> <https://www.whitehouse.gov/wp-content/uploads/2017/12/NSS-Final-12-18-2017-0905.pdf>

<sup>2</sup> [https://www.afsig.af.mil/Portals/73/Documents/003%20-%20\(FA3\)%20MDC2%20I-Plan.pdf?ver=2018-10-15-125241-420](https://www.afsig.af.mil/Portals/73/Documents/003%20-%20(FA3)%20MDC2%20I-Plan.pdf?ver=2018-10-15-125241-420)

<sup>3</sup> <https://www.afspc.af.mil/News/Article-Display/Article/1523196/space-situational-awareness-is-space-battle-management/>

<sup>4</sup> <http://www.airforcemag.com/Features/Pages/2017/November%202017/Facing-the-Unknown-in-a-Multi-Domain-Command-and-Control-Environment.aspx>

<sup>5</sup> <https://www.af.mil/Portals/1/images/airpower/AFFOC.pdf>

<sup>6</sup> [https://www.stratcom.mil/Portals/8/Documents/CSpOC\\_Factsheet\\_2018.pdf](https://www.stratcom.mil/Portals/8/Documents/CSpOC_Factsheet_2018.pdf)

<sup>7</sup> <https://insidedefense.com/daily-news/stratcom-services-stand-joint-satcom-operations-floor>

<sup>8</sup> <https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>

<sup>9</sup> <https://www.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>