ST Engineering

STAYING AHEAD OF THE CHANGING SECURITY THREAT LANDSCAPE

A MILSATCOM Report Produced by NSR and ST Engineering iDirect

iDirect

NSR
NORTHERN SKY RESEARCH
An Analysys Mason Company

Introduction

The satellite industry is undergoing its greatest transformation with the launch of thousands of satellites across all orbits and the convergence of the telecom ecosystem. With this progression brings an increase of vulnerabilities and threat vectors. It is more imperative than ever that government and military entities continually improve their security posture to remain resilient in the face of adversaries.

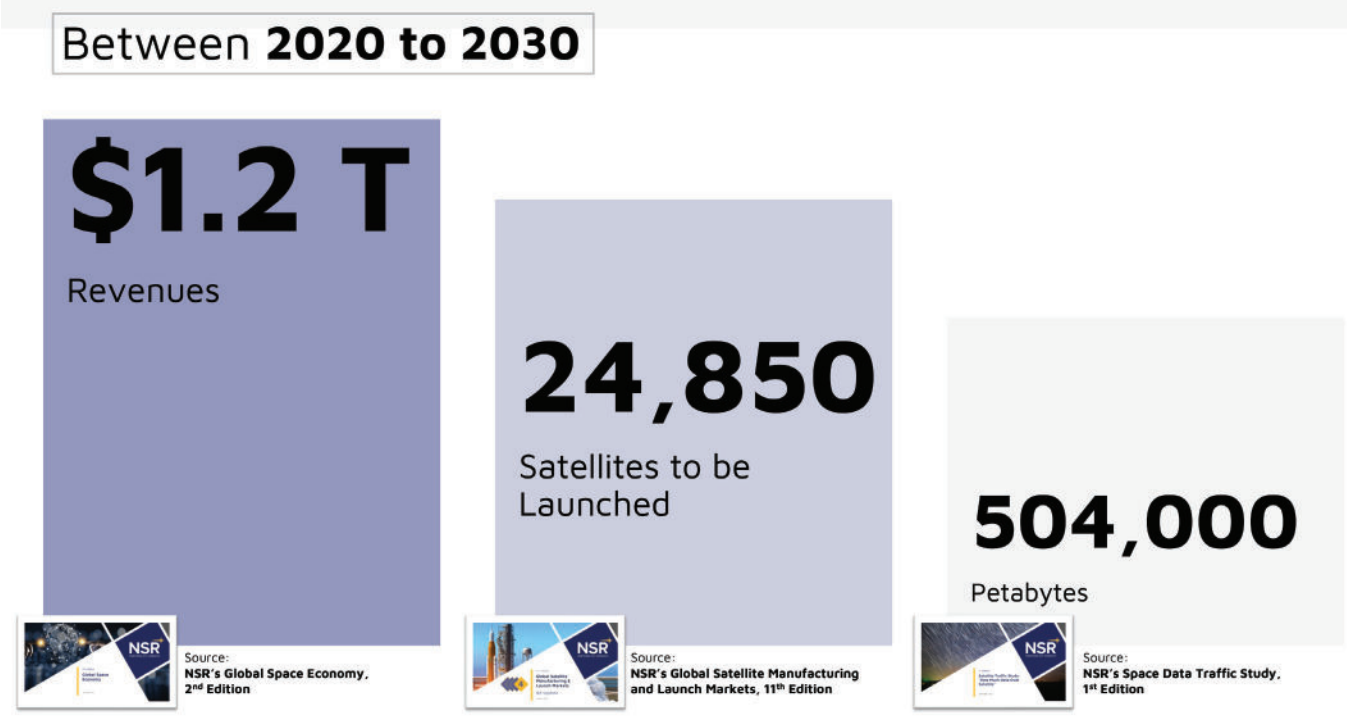
This whitepaper explores the changing landscape of satellite communications and the move towards multi-dimensional networks for governments and militaries. Adopting a multi-layered security and resiliency approach is essential to ensure greater battlefield awareness and mission assurance for warfighters and other personnel.

NSR
NORTHERN SKY RESEARCH
An Analysys Mason Company

Leveraging a New Era of Growth for Security & Resiliency

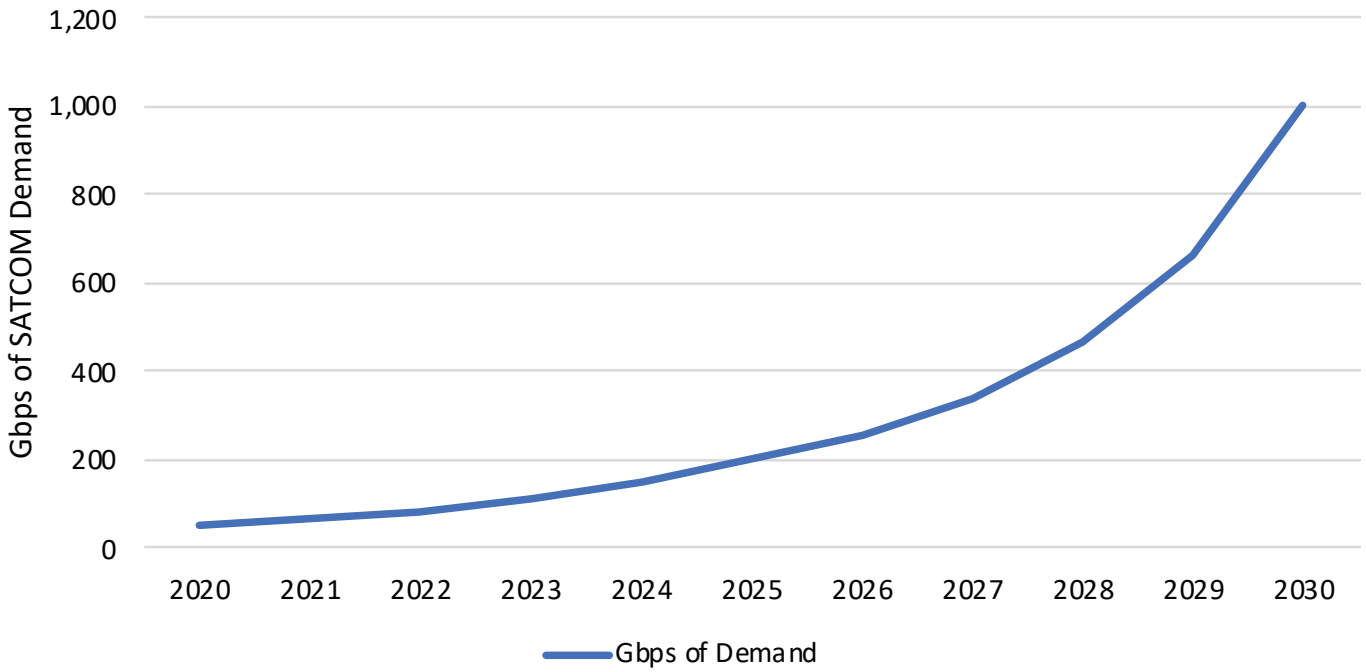
The Space and Satellite Markets are in a new era of growth. According to NSR's latest research, more than 24,500 satellites will be launched from 2020 to 2030, $1.25 Trillion Dollars generated in revenues, and over 500 exabytes of information transmitted to and from space.

EXHIBIT 1: COMMERCIAL CONNECTIVITY GROWTH, 2020-2030



Government and Military customers will navigate this future through a massive acceleration in their demand of commercial connectivity – from 52 Gbps in 2020 to over 1,000 Gbps by 2030, according to the latest research from NSR. Government-owned systems will likewise increase its capabilities across orbits and frequencies over this same period. A GEO-centric network paradigm today will transition to a complex multi-orbit, multi-band, multi-owner system. While this brings with it new capabilities and enables new applications, it comes at a cost. That cost is exponentially expanding threat plane which must operate in a complex, frequently contested environment.

EXHIBIT 2: GOVERNMENT AND MILITARY COMMERCIAL SATCOM DEMAND



Source: NSR

None of these figures illustrate the fundamental changes occurring within the SATCOM network stack. Software is replacing hardware in more and more core functions and systems. Automation is replacing manual orchestration workflows. Altogether, this results in the "softwarification" of the SATCOM technology stack -the process of turning hardware+manual into software. New hardware and enhanced workflows are already building single-orbit, single-band, single-owner networks of today. Softwarification is enabling multi-band, multi-orbit, and multi-owner networks. This is the multi-layered, highly resilient multi-dimensional networks of the future.

Resiliency Starts (and Ends) on The Ground

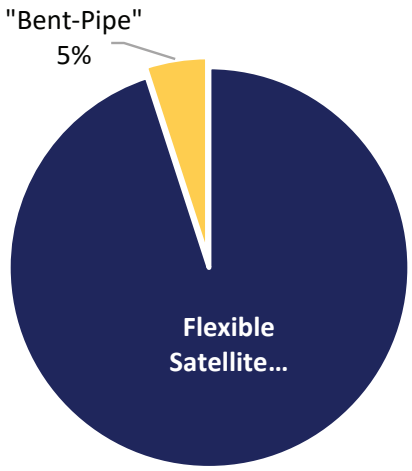
All roads to space start and end on the ground. Not just because satellites (for now) are built here on Earth – but the ground segment is the key piece of any satellite communications network. More than just a collection of antennas, modems, coax or fiber – this system is undergoing rapid changes as previously hardware or manual processes move towards software. The "softwarification" of space networks (replacing hardware + manual with software) is revolutionizing how satellite communication networks are built and operated – introducing new use-cases, flexibility, and resiliency to threats in cyber, RF, and physical planes. Resiliency via softwarification is perhaps best illustrated with the rapid ability to change operational characteristics of deployed satellite communications networks. In the proliferated, multi-orbit regime that military planners and procurement offices are working towards, the ground network must work closely as part of a holistic network – integrated space + ground operations.

A simple example of the power of software-enabled resiliency comes from the Ukraine conflict. Mainly, as quoted by the Pentagon's director of electronic warfare Dave Tremper, "[we] must be able to change very dynamically what we're trying to do without losing capability along the way." That flexibility and resiliency comes from softwarification. It enables a ground segment that operates as part of a holistic network – integrated space + ground operations. Overall, it unlocks a further layer of resiliency via the softwarification of the satellite ground segment.

There are no doubt extreme examples of software-enabled resiliency which comes at the cost of vendor lock-in – however, it does not mean that a single-vendor technology stack is the only way in which to achieve software-driven resiliency. As NSR is tracking, new investments across the space and ground segment are unlocking an open ecosystem of multi-vendor, multi-orbit commercial satellite communications networks. These multi-dimensional networks will require new business models and engagement between industry and governments – but the force multiplication can be tremendous.

In Space, between 2020 and 2030, NSR expects that $25 Billion will be spent on building and launching flexible communications satellites in GEO and Non-GEO. Resulting in more than 16,700 satellites, the stove-pipe architectures of Government and Military networks of today will not scale as flexible satellites proliferate. While most of these communications satellites will be commercially owned to service commercial markets, multi-layered security requires the capability to roam amongst any network of opportunity. To roam, next generation ground segments must be deployed. Resiliency requires an integrated investment strategy between space and ground, sovereign vs. commercial.

EXHIBIT 3: COMMUNICATION SATELLITES TO BE LAUNCHED, 2020-2030



Source: NSR

"Roaming" will not be easy for multi-dimensional networks. Ensuring data security and information integrity/assurance across the entire network mean things like 'make before break' or dual-path redundancy need to be clearly defined. Penetration testing of all components of the network must be done. Vendors must have clearly defined operational responsibilities.
Standards and regulations will need to continue to mature in a cyber-aware environment. In all, the challenges of implementing these networks without a systems-level approach are significant.

Overall, investments by Governments and Military End-users into orbit diversity or proliferation mean little without likewise investments in ground segment flexibility.

NSR
NORTHERN SKY RESEARCH
An Analysys Mason Company

SATCOM Security is More than Anti-Jam

Space-based resources have always been under threat across physical and cyber vectors. Historically, those examples are most notable in the PNT-arena (positioning, navigation, and timing) with GPS spoofing in the South China Sea, jamming in conflict areas, and the war-gaming of kinetic attacks against PNT constellations. Only recently have satellite communications network vulnerabilities come into the public sphere via the incidents in Ukraine. The most notable of these SATCOM cyber incidents resulted in the US Government CISA alert from March 17th calling for a review and implementation of various cyber security practices. While some recommendations are good cyber hygiene – strong passwords, MFA, encryption, others such as integrating SATCOM traffic into other monitoring tools, review log files, baseline traffic profiles, and other analytics-focused cyber practices can only be enabled through a robust network management structure. Investments in the integrated and multi-layered security capabilities offered via next generation ground segments can further unlock security resiliency.

While virtualization and other 'terrestrially-derived' best practices bring their own set of vulnerabilities, satellite communications networks must add further protections against jamming, interception, and Electronic Warfare attacks. As highlighted in Ukraine, the capability to respond quickly to jamming conditions on the ground can 'make the difference' between operational and not.

Programs such as Europe's European Protected Waveform (EPW), the US Protected Tactical Waveform (PTW), and others across the landscape of major military operations all provide a solution to the jamming problem. However, they are only one side of the combined cyber + physical threat plane. Both must be addressed to provide highly robust and resilient satellite communications networks.
Exact spending on cyber security programs is largely unspoken or hidden, especially within the Space and Satellite Markets. However, spending by US Civilian agencies on cyber security is allocated at over $9.8 Billion in FY22 out of a budget request of $58.4 Billion. A report by the UK government states that the UK cyber security sector is, "now worth an estimated £8.9 billion, with a record £800 million of investment raised by firms." Germany created a dedicated cybersecurity unit within their armed forces in 2020 with upwards of 13,000 staff members once it reaches full capacity. Other nations across NATO and other regions are making likewise investments into their cyber capabilities. Space-based communications will be a key sector for on-going investments and protection.

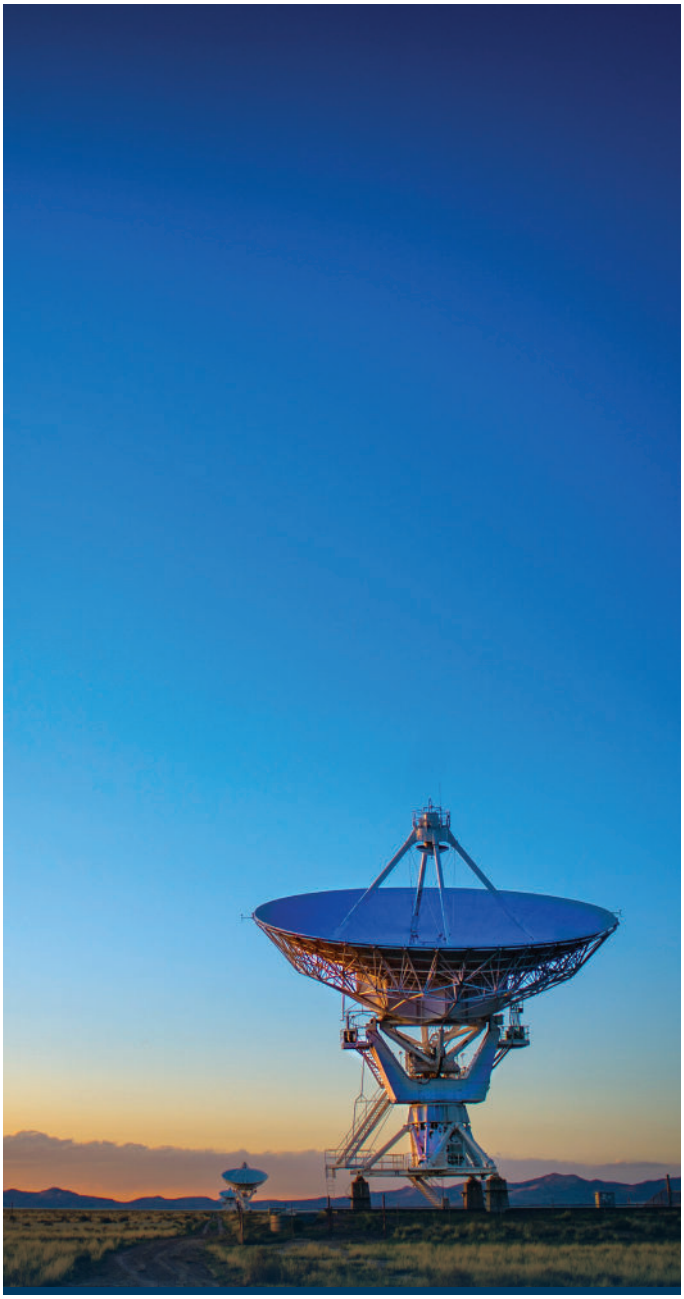
Overall, the satcom sector is already experiencing the new-normal of cyber and physical threats. Legacy, un-patched or un-upgraded infrastructure will only magnify threats and fall victim to exploitation. New capabilities and paradigms such as software-defined networking, virtualization and containerization, zero-trust principals, and other dimensions of good cyber hygiene are required to respond to these constantly evolving threats.

What's Next?

From new business models to on-orbit technologies to next-generation ground infrastructure, all can provide new capabilities to Government and Military End-users. Government and Militaries do not need to use yesterday's solution to solve today's problem. Nor can they afford to use these solutions for tomorrow's challenges. Instead, they must navigate through this new era of space while maintaining operational readiness and resiliency for now and into the future.

Multi-dimensional networks are a key solution towards solving operational readiness and resiliency. Yet, these networks are a converged set of individual pieces – antennas working with modems working with satellites and orchestration workflows. No one piece of a multi-dimensional network can provide high resiliency without a systems-centric approach.

As the space and satellite sector looks to move more than 500,000 petabytes of information across space-based resources, Government and Military End-users must adapt their CONOPs by leveraging commercial best practices. Sovereign SATCOM networks that are in the design stage in places such as Australia, the United Kingdom, United States, and elsewhere must remain focused on the complete network stack – ground + space. Softwarification is the force multiplier. Multi-dimensional is resiliency.



NSR
NORTHERN SKY RESEARCH
An Analysys Mason Company

Building Secure, Resilient MILSATCOM Networks from the Ground Up

As SATCOM networks become more complex, Government and Military end-users are naturally exposed to more vulnerabilities and threats. After all, more network components mean more potential points of weakness. That's why it's important that these users build in multiple layers of security and resilience, creating a robust bulwark against threats and reducing the potential attack surface. Of course, it's also essential to maintain network integrity and functionality in the midst of security measures.

ST Engineering iDirect is the strategic ground technology partner to the world's top satellite operators, government and defense network operators and service providers and a market leader in secure military satellite network technology, with a broad portfolio of military-grade products, as well as systems integration and terminal integration services for more complex and customized solutions.

The WGS certified Evolution® Defense portfolio of satellite hubs and modems is our key product line for military grade networks designed for the government and military requirements in terms of coverage and connectivity support, performance and efficiency, agility, multi-layered security and resiliency, interoperability, and ease of use to achieve operational advantage and successful operations.

By leveraging best practices, ST Engineering iDirect provides Government and Military entities an operational advantage that translates into on-the-ground results.

iDirect

Best Practice 1:
Adopt a Multi-Layered Security and Resiliency Approach

This dynamic posture is more important than ever for establishing the highest level of information assurance with the utmost security. The Evolution® Defense platform embodies the multi-layered security and resiliency approach where different security technologies cooperate in orchestration building multiple walls of defense to ensure seamless communications as well as information assurance.

The multi-layered security and resiliency framework consist of 4 main pillars: **Detect, Mitigate, Prevent** and **Predict:**

A network that is imbued with multiple layers of security and resiliency can **detect interferences** by using a sophisticated network management system, spectrum monitoring and geolocation services. Together, these defense measures can identify threats and provide actionable intelligence to deal with them.

This network will also be capable of **mitigating security threats** using signal excision technology and a combination of anti-jam methodologies. Excision technology dynamically filters or cuts away different types of interference or jammers. If the interference or jamming becomes severe, the ability for the modem in the field to automatically switch from one satellite to the other is a key advantage. Such methodologies include but are not limited to frequency hopping, spread spectrum, and low probability of intercept (LPI) and low probability of detection (LPD).

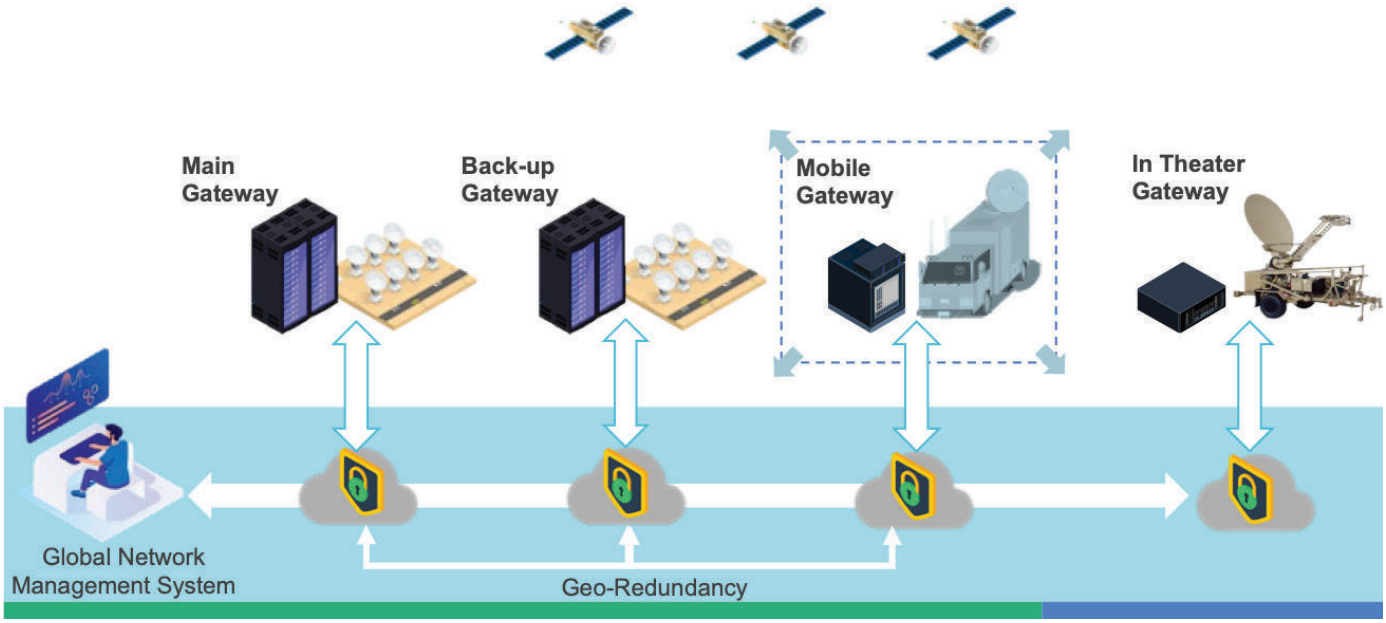
EXHIBIT 4: MULTI-LAYERED SECURITY AND RESILIENCY APPROACH

Upgrading your network with TRANSEC and FIPS 140-2 fortifies your system security

A multi-layered approach also helps to **prevent future security breaches.** By utilizing a combination of transmission security, or TRANSEC, and FIPS 140-2, the network ensures system security by keeping sensitive communications safe and encrypted. TRANSEC encompasses multiple security measures against intrusion, detection, and interception by adversaries and is available on our Evolution Defense platform for both traditional two-way and one-way broadcast networks where intelligence is being sent to different assets in operation. (Read more in the ST Engineering iDirect TRANSEC Whitepaper)

Lastly, a network that employs such security and resiliency measures is one that is capable of **predicting future interferences and threats.** To do so, the network uses comprehensive reporting tools that send alerts for potential network outages. And by running regular network health checks, the system can identify improvement opportunities in real time.

EXHIBIT 5: BUILDING RESILIENCY WITH MOBILE GATEWAYS IN A SINGLE NETWORK

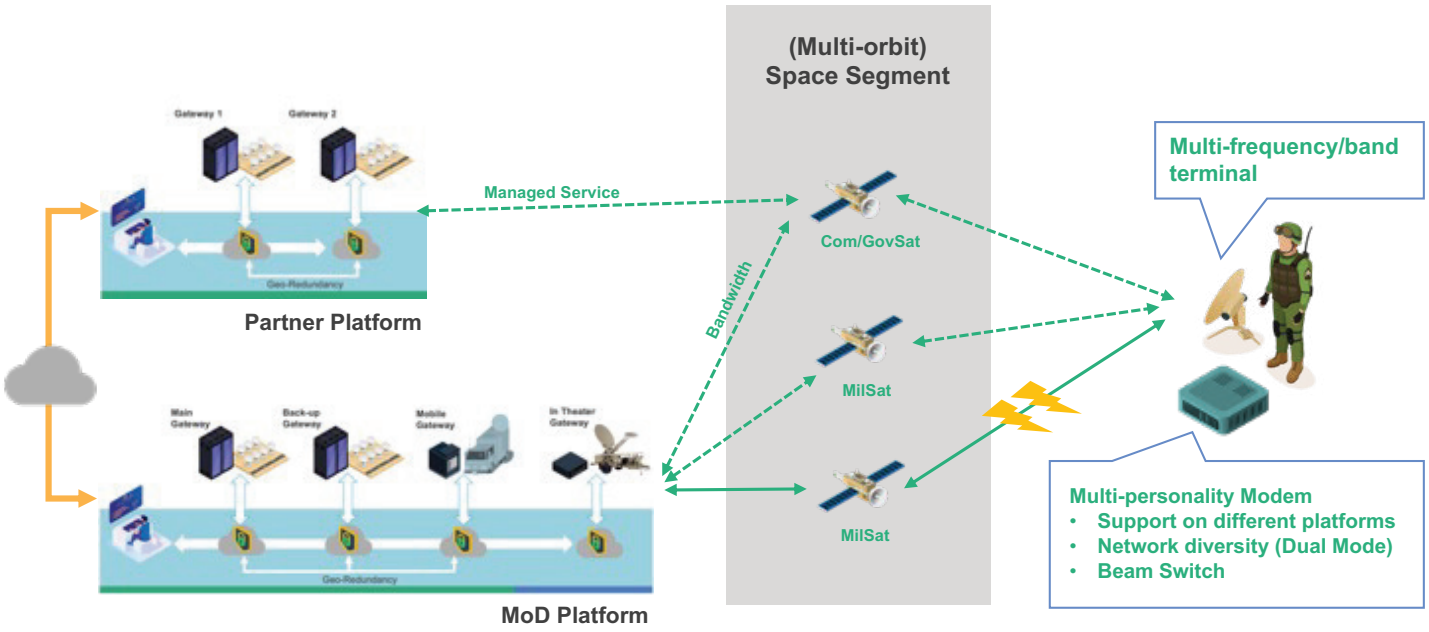


Best Practice 2:
Build in Redundancy and Resiliency with Fixed and Mobile Gateways

A network that's fortified with redundancy and resiliency is optimized for availability and interoperability. This is increasingly necessary as the industry sees a convergence of space, cloud, service, and user layers, along with the ground segment. A network that is integrated this tightly has numerous advantages, of course. But among its chief disadvantages is that instead of a security attack affecting just a single modem, gateway, spacecraft, or intentional/ unintentional interference on the waveform, the attack is now capable of penetrating the entire integrated system. Fortunately, there are myriad security technologies that, when incorporated into a network, can provide multiple layers of defense against ever-increasing types of threats.

One must-have redundancy for Government and Military networks is on the gateway end. Georedundancy of gateways—using one or many backup gateways in various locations—is one way to mitigate vulnerability. Another strategy that's being more frequently deployed is to implement and use a mobile gateway. Such a gateway can be used in-theater and it can be moved around periodically to reduce its chances of becoming an easy target. All of the gateways are connected through a common NMS to ensure real-time orchestration of services across the different locations.

EXHIBIT 6: NETWORK DIVERSITY AND MULTI-PERSONALITY MODEMS



Best Practice 3:
Network Diversity and the Role of Multi-Personality Modems

Another key component of optimized satellite network redundancy and resiliency is network diversity. On such a network, users have their own satellite platform while also having the ability to leverage a partner or commercial satellite platform network or capacity. The user can switch between all these platforms for multiple reasons. Firstly, to avoid presenting a single security target. Secondly, in case one of satellite links suffers from intentional or unintentional interference and thirdly to extend the connectivity reach to other locations of operation. Multi-personality modems, such as the kind that ST Engineering iDirect offers, help enable these platform-switching and beam-switching capabilities by assuming the "personality" of the individual network on which it is currently active. As such a military end user could easily switch between the network of a military sovereign WGS satellite capacity and a commercial satellite provider to maintain seamless high throughput connectivity for an ISR asset using the Evolution Defense 9-series modems.

Best Practice 4: Apply Secure, Efficient and Agile Waveforms

Waveforms play a key role in the multi-layered security and resiliency framework. Some prime examples are the involvement in the development of the DVB-S2X standard, the Mx-DMA waveform which is the dynamic industry's most efficient, dynamic return satellite technology for commercial applications and A-TDMA or Adaptive Time Division Multiple Access which delivers higher spectral efficiency and greater network versatility by optimally changing the return channel configuration to match the conditions of the over-the-air links and the constraints of the terminals.

Building secure and efficient commercial and military waveforms and standards has been part of the ST Engineering iDirect DNA since its founding 35 years ago.

Large nations with considerable military budgets have already invested in creating their own sovereign protected waveform to secure their communications over satellite. The fact that these waveforms have a sovereign character makes them difficult to share with other nations or international organizations. More 'exotic' and proprietary waveforms are perceived as more secure because the functionality and the encryption used remains within the nation's military user community. This approach does not enhance the interoperability between partner nations.

ST Engineering iDirect has been involved in the development of secure and protected waveforms that overcome the issues of security, efficiency, affordability and interoperability. A prime example is the EDF (European Defence Fund) European Protected Waveform (EPW) program where ST Engineering iDirect Europe as European Satcom Center of Excellence is leading a consortium of 19 companies from 11 EU nations to build a military-grade secure waveform. The EPW incorporates the latest disruptive innovations in waveform technology in line with today's and future military operational requirements, including multi-orbit satellite constellations, on-board processing satellites, 5G integration, smallsats etc.

Best Practice 5: Adopt a PACE Approach

Utilizing an approach known as PACE—primary/alternative/contingency/emergency—ensures always-on connectivity. This ability empowers Government and Military users to respond quickly to any situation, which, in operational situations, can provide an enormous advantage.
The technology solutions that ST Engineering iDirect provides to the market is the mainstay of the alternate and contingency portions of PACE, and our portfolio provides options for the primary and emergency portions, as well.

iDIRECT

Conclusion

As SATCOM networks become more complex, Government and Military end-users are naturally exposed to more vulnerabilities and threats. After all, more network components mean more potential points of weakness. That's why it's important that these users build in multiple layers of security and resilience, creating a robust bulwark against threats and reducing the potential attack surface. Of course, it's also essential to maintain network integrity and functionality in the midst of security measures.

ST Engineering iDirect is the strategic ground technology partner to the world's top satellite operators, government and defense network operators and service providers and a market leader in secure military satellite network technology, with a broad portfolio of military-grade products, as well as systems integration and terminal integration services for more complex and customized solutions.

The WGS certified Evolution® Defense portfolio of satellite hubs and modems is our key product line for military grade networks designed for the government and military requirements in terms of coverage and connectivity support, performance and efficiency, agility, multi-layered security and resiliency, interoperability, and ease of use to achieve operational advantage and successful operations.

By leveraging best practices, ST Engineering iDirect provides Government and Military entities an operational advantage that translates into on-the-ground results.

To learn more about ST Engineering solutions, visit iDirect.net/defense.
To contact a sales representative, visit iDirect.net/contact-us.

iDIRECT