ST Engineering

GAINING OPERATIONAL ADVANTAGE THROUGH INNOVATIVE MILSATCOM NETWORKS

iDirect

For defense agencies, gaining an operational advantage is always a critical objective. In today's evolving world, that means military organizations need a sophisticated satellite communications network that can accommodate increasingly dispersed and complex operations while providing the utmost security and resiliency. This white paper focuses on building a multi-layered security and resiliency network in line with the six key requirements necessary to obtain information superiority, tactical advantage and successful operations.

Building a Multi-layered Security and Resiliency Network

Defense agencies have always relied on satellite communications, and this dependence will only continue to grow as military operations become more complex. From strategic communications to intelligence gathering, surveillance and tracking, satellite is essential for connectivity needs across land, air and sea.

As nations look to build satellite networks or replace decommissioned satellites, new programs provide the opportunity to adopt the latest satellite and ground segment technologies and find the right mix of capacity types to give them the operational advantage needed for successful missions. Building coverage and network diversity while guaranteeing the latest military-grade security standards offers nations a high level of redundancy, flexibility and security to meet the needs of a multi-layered, secure and resilient next-generation defense network.

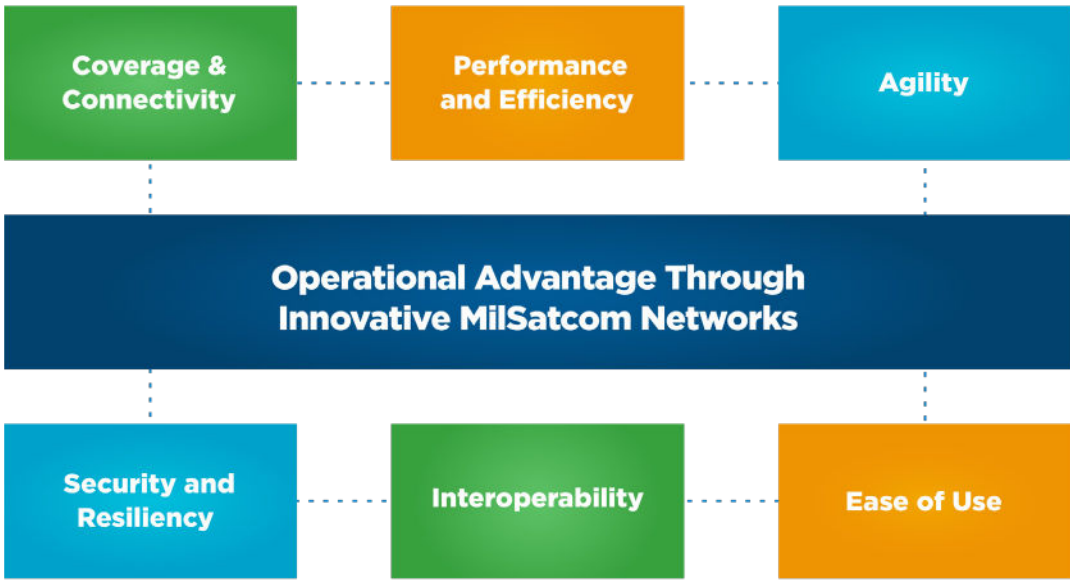
Such a network can lead to operational advantage by getting information quicker and at higher quality and granularity and by making sure an adversary has not blocked or intercepted that information. Advanced security standards, specialized enclosures, national waveforms and other improvements have been created for defense organizations to better their operations. The commercial satellite sector has also undergone an immense transformation, with highly efficient waveforms for greater performance, very high throughput satellites (VHTS), new non-geostationary (NGSO) constellations, network integration across access technologies and other key innovations. Defense agencies must harness all these innovations to ensure operational advantage at all times. They must plan now for their next-generation, multi-layered security and resiliency network that will guarantee success in their most critical operations.

Complexities of capacity planning

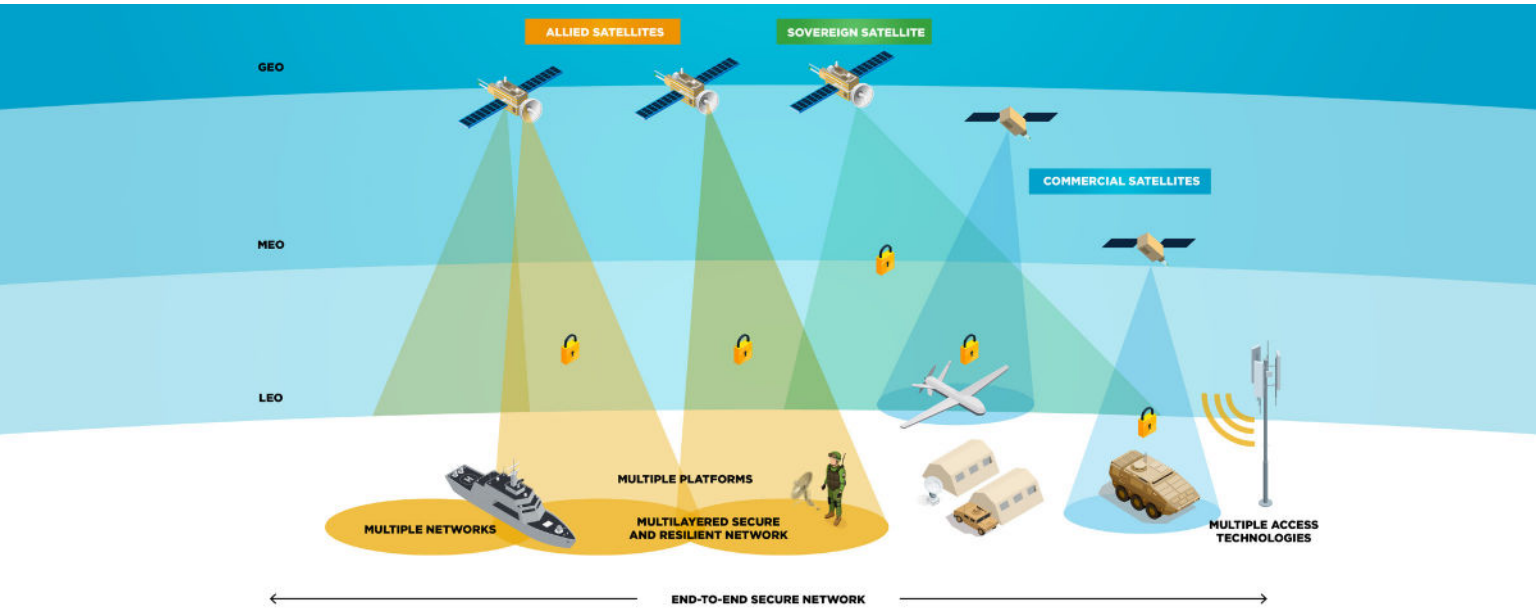
Nation A may procure satellite capacity and services as part of its communications infrastructure in distinct ways; it might employ its own sovereign satellites, buy managed services from satellite operators or service providers, use allied military satellite capacity through government-to-government arrangements or pooling and sharing, purchase commercial capacity or implement any mix of the above. By mixing different types of capacity, military organizations have extra flexibility for connectivity for their dispersed theater of operations at a moment's notice. They can operate without relying on a single provider and ensure interoperability for joint operations. This flexibility is also important in case of satellite signal jamming or interference so that Nation A has guaranteed resilient connectivity under any circumstance.

Six Considerations for Building a Successful Flexible, Multi-layered, Secure and Resilient Network

As nations look to build new satellite network programs or replace decommissioned satellites, they have the opportunity to adopt the latest satellite and ground segment technologies and find the right mix of capacity types to give them the operational advantage needed for successful missions. When looking for the ideal platform, defense and government organizations should consider six key requirements that are critical to building a secure multi-layered network.



MULTI-LAYERED SECURE AND RESILIENT NETWORK



1 Dynamic Coverage: Connectivity Anytime, Anywhere

When discussing coverage, military network operators must consider whether that network coverage is dynamic enough to meet the diverse needs of their regional and global deployments. For example, a military organization might want secure military capacity on GEO, high-throughput satellites (HTS) for critical, bandwidth-intensive intelligence, surveillance and reconnaissance (ISR) applications while reserving commercial capacity for morale, welfare and recreation (MWR) connectivity; they might want to use a mixture of commercial and military satellites to do so.

With dynamic coverage, military organizations can ensure critical operations run smoothly, whether they require low bandwidth at a fixed location or high-bandwidth rates on the move.

When planning their capacity, military network operators should look for a satellite platform that can handle dispersed operations' network complexity with a mix of capacities and global connectivity to fixed, on-the-move (OTM) and on-the-pause (OTP) assets. The ideal platform should allow military network operators to customize their connectivity networks to efficiently optimize bandwidth and prioritize critical applications while ensuring continuity of service to provide a seamless end-user experience.

One way to certify a streamlined process is to employ a single, centrally managed VSAT platform that simplifies management and improves network visibility. New VSAT platforms are increasingly designed to support multi-access and multi-orbit technology in orchestration with multifrequency terminals. This allows deployed assets to address changing operations; provide network diversity; roam across multiple satellite constellations; and operate on a variety of Ku-, Ka- and X-band frequencies to enhance overall assurance and resilience.

2 Providing Maximum Performance and Efficiency for Information Superiority

Information superiority is key in military operations. Massive amounts of data are sent back and forth across military networks to provide instant situational awareness for intelligent decision-making. Bandwidth-hungry applications such as ISR video and sensors consume tremendous capacity on the satellite transponder. Strategic communications — as well as demands from emerging 5G, machine-to-machine (M2M) and Internet of Military Things (IoMT) sensors and devices — will further increase bandwidth consumption. Military network operators will need to employ the latest VSAT and waveform technology advances to maximize throughput and efficiency.

They can do that by making sure their satellite and ground segment technologies work hand in hand. Although considerable focus is placed on the impact of new NGSO satellite constellations, an innovative VSAT platform is also essential to ensure ongoing adaptability to changing environments and to achieve higher spectral efficiency and throughputs at maximum service availability.

With a new military satellite launch or when planning capacity for operations, make sure the latest waveforms (such as DVB-S2X) and adaptive return channels are supported. With DVB-S2X, higher modulations up to 256APSK and roll-off factors down to 5% — in conjunction with adaptive coding and modulation (ACM) — allow for greater spectral efficiency. Adaptive return channels provide greater network availability by dynamically adjusting carrier configurations in case of rain fade and link degradation. Advanced waveforms create new opportunities to do more with the same amount of bandwidth.

3 Agility: One Platform for Multiple Applications

Military leaders want better, quicker, more detailed and continuous information to make informed decisions, maneuver more swiftly and always gain the tactical upper hand. This operational superiority can be best achieved by combining network performance with flexibility: in other words, by deploying anywhere, anytime and by connecting concurrent operations to a centrally managed satellite network.

A truly agile network can respond to changes in operations quickly and without excessive troubleshooting. This means a network operator can quickly groom capacity and reconfigure their satcom network for quick redeployments with the latest innovative features onboard the VSAT platform. Software-defined modems increase flexibility by supporting over-the-air upgrades, seamless compatibility for new capabilities and easy configuration for new operations.

Moreover, a flexible network allows for concurrency, or for end users to adequately address dispersed, simultaneous and constantly shifting operations through a single VSAT platform. Building a software-defined network is key. Satellite architecture should leverage network orchestration, virtualization and slicing functions to offer a truly smooth connectivity service anywhere in the world, as well as an affordable, highly flexible and scalable infrastructure to address quickly shifting needs.

Because greater numbers of vessels, aircrafts, vehicles, manpacks and deployable terminals are filling military networks, a centrally managed VSAT platform must take a multiservice approach to cater to different types of traffic and applications. Advanced quality of service (QoS) settings can help ensure optimal bandwidth allocation for high-priority traffic, whether voice, video or data. Each service is treated individually to make sure different priorities and QoS expectations are in line with the operations at hand most efficiently, taking into account challenging conditions and harsh environments.

4 Security and Resiliency

Security is high on the agenda of military agencies looking to ensure continuity of operations in the face of previously unknown vulnerabilities and changing security threats. In a military satellite network, link security is no longer the sole point of focus. Security systems will **detect**, **mitigate**, **prevent** and **predict** the mix of threats that could hamper operations. As such, a multi-layered security approach using multiple security technology layers should be adopted to achieve the highest information assurance.

For interference **detection**, a network management system, spectrum monitoring and geolocation services can identify potential threats. A network management system provides useful statistics around radio frequency (RF) monitoring, IP levels, the Ethernet and QoS. A spectrum monitoring solution can further detect any anomalies by pooling bandwidth and comparing current conditions against a defined carrier plan. Geolocation can determine the latitude and longitude of an interfering signal and provide actionable intelligence by isolating and characterizing the interference source.

When a security threat occurs, a proper **mitigation** response is crucial. Signal excision technology and network diversity can help users swiftly leverage another network capacity to ensure persistent communications. Signal excision is any technology, either analog or digital, that can identify and remove an interfering signal without the need for additional bandwidth. This contrasts with the traditional method of anti-jam, which relies on spread spectrum and requires a large spread factor and thus enormous amounts of bandwidth to overcome even small jamming signals. No signal excision system can fully address all jam and interference threats; hence, a combination of anti-jam methodologies will be required for increased protection, such as low probability of intercept/detect (LPI/LPD), frequency hopping or spread spectrum.

Direct sequence spread spectrum (DSSS) in combination with signal excision technology leads to a highly efficient anti-jam solution for military-grade networks. A DSSS waveform is intrinsically compatible with existing TDMA VSAT architectures.

For **prevention** of future security breaches, transmission security (TRANSEC) and information assurance capabilities can ensure systems remain secure. TRANSEC technology keeps communications safe as sensitive data are transmitted over the airwaves. Securing transmissions can be achieved through three steps: masking channel activity, controlling channel information and ensuring hub and remote authentication and validation. TRANSEC is best when combined with FIPS 140-2, which provides stringent third-party assurance of security claims on any product containing cryptography that a defense organization may use. Adopting the latest software release and security patch updates is another way to protect against vulnerabilities.

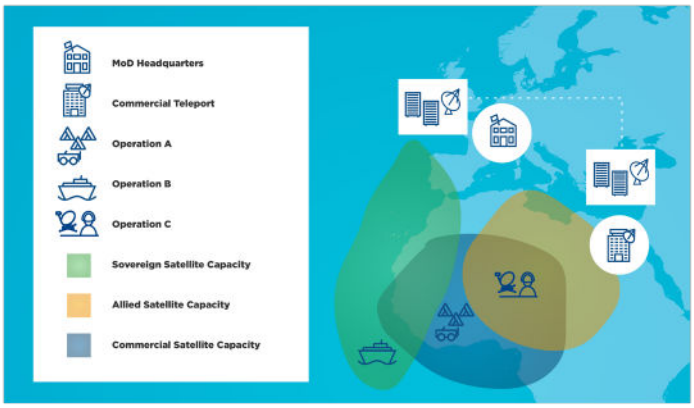
Finally, **predicting** future interferences and threats can be done by evaluating and understanding network activities, looking at historical data and ensuring rapid response to adjust for any inconsistencies. A network planning and link budget tool allows for optimization of space assets to meet throughput needs with network visibility and performance assessments. Network management systems can provide comprehensive reporting tools and send alerts for potential network outages, and regular network health checks can identify improvements along the way.

5 Joint Operations Support

For military organizations, it can be essential to share intelligence and information across government organizations, with partners and with allied governments during joint operations. Interoperability is a key enabler for the conduct of effective, collaborative, multiservice military operations across a wide range of scenarios.

Pooling and sharing satellite platforms built around a centrally managed network system can provide more flawless connectivity to regional or global operations across different nations' military agencies during a joint operation. Interoperability can be achieved when different nations use a common waveform standard (such as DVB-S2X) or the same military waveform (such as the European Protected Waveform).

Interoperability with Common Waveform Standards



With the shift toward more software-defined modems, increased virtualization and open interfaces, multiple waveforms and network configurations can now be preinstalled on a single modem unit. Once in operation, the correct waveform and network configuration can be triggered automatically to allow the modem to roam among the diverse networks and VSAT platforms. In peacetime, these multi-waveform modems can use an efficient, high-throughput and secure waveform; they can also switch to a more robust, resilient and protected waveform in times of high interference or jamming or during a sensitive tactical operation.

6 Ease of Use

Expertise for satellite communications is becoming less common among military agencies in several nations, and not every operation can afford to send a satellite communications engineer on every deployment. However, with each layer of complexity, the VSAT networks that many military organizations are building stand at an increased risk for security breaches or mistakes that could create satellite interference and potentially hamper operations. In most cases, the human factor is the weakest link in the security chain.

The quicker a terminal is up and running, the quicker deployed military personnel can focus on their core operational tasks. Terminals optimized for size, weight and power (SWaP) for ease of portability as well as rapidly deployable flyaway terminals are ideal for OTM and OTP applications. Remote commissioning tools allow a warfighter to point and set up the VSAT terminal through a comprehensive graphical user interface (GUI) and automated pointing procedures available on a PC or mobile device. After the terminal is pointed accurately, the network, auto-commissioning and authentication management will take over automatically and provide internet connectivity in a matter of minutes. This process ensures each terminal performs optimally, thus maximizing efficiency and reducing interference and implementation risks.

When done right, these requirements allow for a multi-layered, secure and resilient network. Military network operators must look for an ideal platform that can adopt the latest satellite and ground segment technologies combining flexibility, performance, efficiency, security, agility and ease of use to give them the operational advantage needed for successful missions.

Build Networks to Protect with ST Engineering iDirect

At ST Engineering iDirect, we are the market leader in satellite ground infrastructure and solutions for government and defense networks. For more than 35 years, our VSAT platforms have featured superior standards for performance, efficiency, security and mobility for government and defense agencies that rely on satellite to achieve mission success with the highest degree of visibility, coordination and safety. Regardless of whether a ministry of defense prefers to own its sovereign satellite infrastructure, rely on allied capacity, acquire managed services or employ a mix of capabilities, ST Engineering iDirect's VSAT platforms are built to support its satellite programs now and into the future — no matter how complex the configuration.

Our versatile modems can be deployed across platforms and networks for seamless, always-on operations in a network of layers. With our centrally managed VSAT platforms, defense and military network operators can choose the network architecture that best suits their needs, whether that involves running their own satellite network; selecting managed services; operating on multiple orbits; or mixing commercial, government and military capacities.

Our government and defense solutions feature the following:

- Dynamic coverage with flexible, modular hub systems that span multiple satellites, bands, transponders and topologies in a pay-as-you-grow manner. Alternatively, choose a compact tactical hub with military-grade defense line cards for field operations. We offer versatile software-defined modems in multiple form factors to meet any requirement.
- Efficient waveforms with DVB-S2/DVB-S2X, SCPC and adaptive return technologies (such as MF-TDMA and Mx-DMA) for increased network availability. ST Engineering iDirect leads the cohort in developing the next-generation European Protected Waveform.
- An agile, multiservice platform that supports a broad range of applications; advanced QoS technology; and an advanced mobility feature set including spread spectrum, automatic beam selection and skew angle mitigation.
- The highest assurance of security and resiliency with FIPS 140-2 Level 3, award-winning TRANSEC, Communication Signal Interference Removal (CISR™) and other Glowlink signal management and monitoring products.
- A centrally managed network system facilitating the pooling and sharing of capacity for joint operations. The use of common waveform standards (such as DVB-S2X) or the same military waveform (such as the European Protected Waveform or WGS) allows for interoperability.
- Ease of use with SWaP-optimized terminals and an Integrasys Satmotion remote commissioning solution for rapid deployment and secure communications.

At ST Engineering iDirect, we have designed satellite technology solutions that embrace the complexity of military networks both today and tomorrow. By combining multi-layered security and resiliency technologies with network diversity, multifrequency terminals and multi-orbit and multi-access software-defined modems, a military network provider can achieve the operational advantage for successful military operations.

To learn more about ST Engineering solutions, visit iDirect.net/defense.

iDIRECT