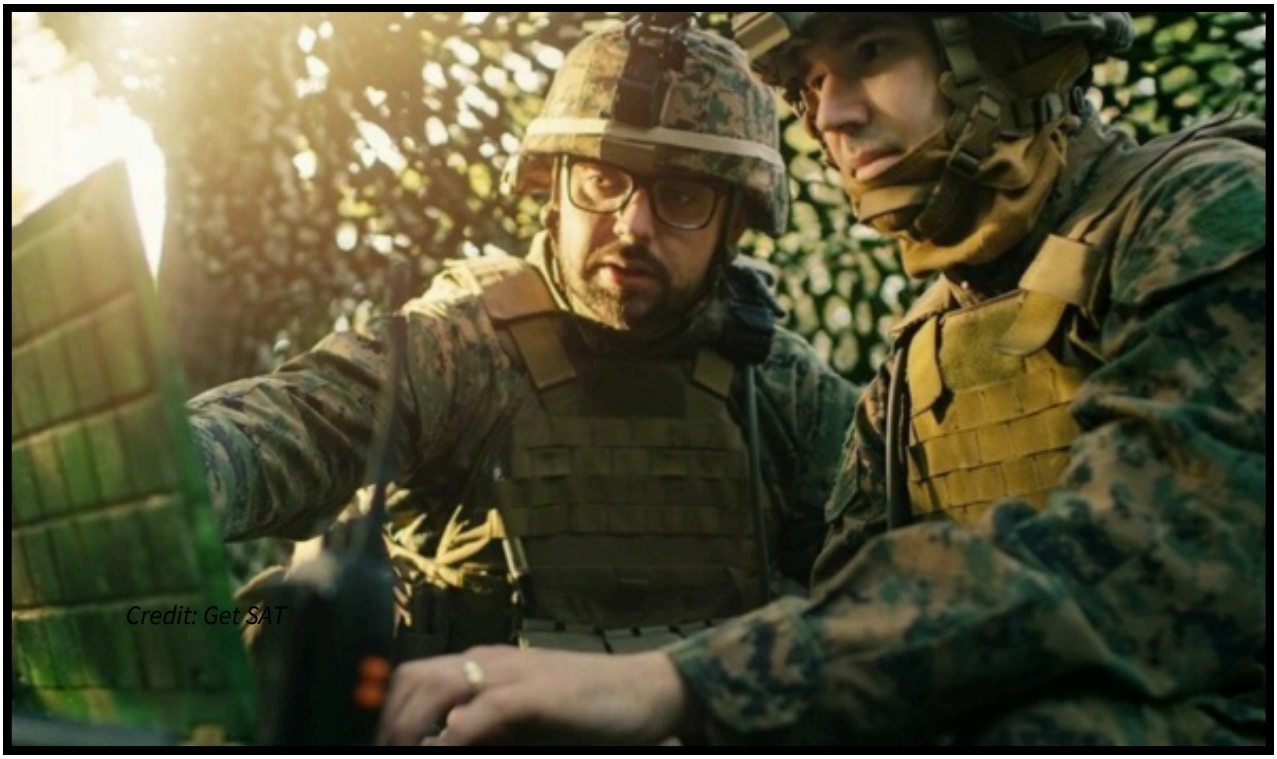
# How MilSatCom has transformed warfare and continues to shape the battlefield.

05 June 2024 Adam Jeffs, Editor, SAE Media Group

From the launch of the first SatCom network to beaming signals with lasers, the impact of MilSatCom on warfare cannot be understated.

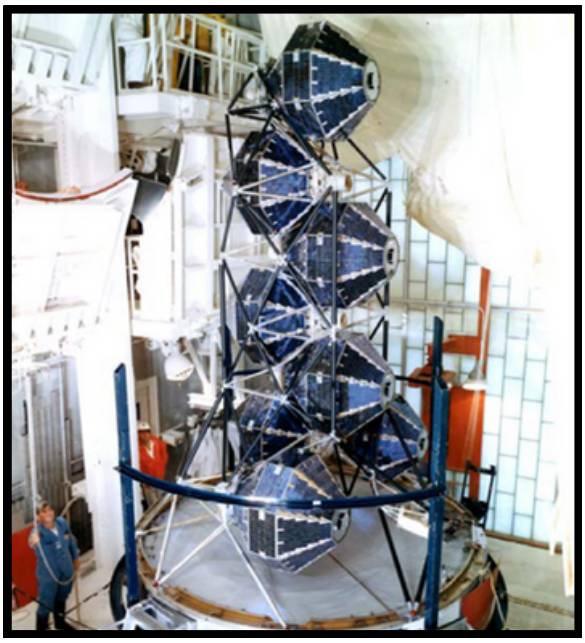



The advancement of space-based communications technologies, including the ever-increasing presence of military satellites for electronic and signals intelligence purposes, has dramatically changed the way wars are fought down on Earth.

From the launch of the first satellite communications network to the cutting-edge technology that is still in development, below we take a look at how far MilSatCom has come.

## A brief history of MilSatCom

The first military communications satellites were launched by the US in 1966, with 19 satellites entering orbit by 1967 comprising a constellation that would come to be known as the Initial Defense Satellite Communication Program (IDSCP). The IDCSP satellites, launched in five groups by Titan IIIC launch vehicles, were intended as testbeds and a proof-of-concept for the wider Defense Communications Satellite System (DSCS).



*Eight IDSCP satellites fixed in the Titan IIIC truss (Credit: US Air Force)*

With improving satellite communication technology, the US further developed the system in following iterations with DSCS II and III. The goal of the IDSCP was simply to provide a basic global communication link, with the DSCS later offering better reliability and capacity. DSCS II brought more significant improvements, with more powerful transmitters, greater bandwidth and improved anti-jamming capabilities.

The most significant leap came with DSCS III as, on top of further capacity, security and transmission capabilities, these satellites had longer lifespans, reducing the need for replacements, and onboard processing capabilities which greatly improved the quality of transmissions.

This early work has culminated in the Wideband Global SATCOM (WGS) network, with initial launches beginning in 2007, it is said that each WGS satellite offers more capacity than the entire DSCS network. The WGS network was expanded internationally, now serving various government agencies, the Department of Defense (DoD), international partners and NATO.

While the US has not been the only nation developing MilSatCom capabilities, for example Russia began launching its own communications satellites during the Cold War, they were the first.

## How MilSatCom changed warfare: From Vietnam to Ukraine

### Vietnam War

The first use of satellite communications in warfare came in the Vietnam war, with the US establishing the ability to transmit data and high-resolution images via the IDSCP. The capacity to transmit images almost instantly was a significant advantage for the US, as it allowed for near real- time battlefield analysis, something which previously would only be possible by being physically present on the battlefield.

The Vietnam War saw the capacity of signals intelligence (SIGINT) continue to progress. The US conducted various SIGINT operations over the course of the war, including a coordinated operation to monitor the Soviet response to the mining of Haiphong Harbour, known as 'Operation Pocket Money'.

Due to a delicate Strategic Arms Limitation Treaty, Russia had been previously warned about the operation by the US, but intelligence officials wanted to know if any Soviet ships had been impacted by the mines leaving the harbour too late. President Nixon spoke live on air to announce the operation, with all of the US SIGINT satellites redirected to determine the Soviet reaction.

This SIGINT operation was likely the first of its kind. Such activities are now commonplace however, with global powers constantly seeking to listen in on their adversaries, necessitating more advanced SIGINT technologies for encryption and avoiding detection.

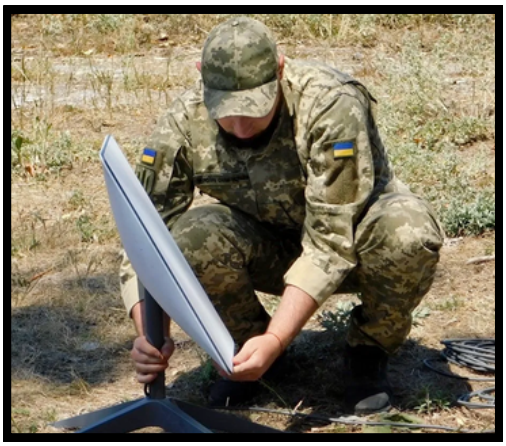
**Related military communications event: Global MilSatCom**

## Russo-Ukraine War

The Ukraine war is the first time we have seen the ever-expanding capacity of the commercial space industry being leveraged in conflict, largely due to Ukraine's distinct lack of military presence in space. Even five to ten years ago, access to military space capabilities was limited primarily to China, Russia and the US, with even major global powers such as the UK, France, Germany or Japan having only a handful of military satellites. Ukraine has been able to offset this by purchasing data and services however, primarily from private US companies, which has ultimately led many nations to realise the advantages of collaboration with the commercial space industry.

Even the US, which has been largely dominant in space, is now formulating plans to utilise commercial space assets in times of conflict.

Use of commercial satellites can provide better coverage, improved revisit rates over high-demand military satellites and added redundancy and resiliency.



*A Ukrainian soldier sets up a Starlink access terminal (Credit: Ukraine Military Centre)*

Ukraine has used the commercial SatCom industry to great advantage in its war with Russia, with SpaceX providing thousands of Starlink satellite access terminals. These terminals allow Ukrainian soldiers unfettered internet access on the battlefield and replace internet and communication networks degraded or destroyed during the war. This has allowed Ukraine to continue coordination of troops and maintain the operation of theatre command centres, with some calling Starlink the "essential backbone of communication" on Ukrainian battlefields.

## How MilSatCom technology continues to advance

## Artificial intelligence (AI)

AI-powered technologies have a number of applications in MilSatCom, including use in cognitive radio networks, signal classification and RF environment mapping.

Cognitive radio networks enhance MilSatCom and optimise spectrum usage by creating adaptive, self-organizing networks. These networks automatically switch between frequencies, helping militaries to avoid interference, detection and jamming for satellite communications. This allows for reliable command and control capabilities even in contested RF environments.

As we have seen with AI-based classification for surveillance images, AI can also be used to classify signals and their sources. This can allow for software which rapidly distinguishes between signals from allies or adversaries and classifies them as military, civilian or commercial. This would enable military communications specialists to focus on signals of interest by filtering out the unnecessary noise.

The data generated by AI-powered signal classification can be further used by AI systems to create RF environment maps, which highlight areas of high activity, potential threats or signals that may be of interest to military observers. This information could prove invaluable in planning and executing electronic warfare operations, ensuring that friendly communications are not impacted and directing the focus onto those of the enemy.

## Cyber resilience technology

The threat of cyber-attacks in space was fully realised in 2022 when, just hours before the invasion of Ukraine, Russia launched an attack on ViaSat's KA-SAT system. The attack disconnected thousands of Ukrainians from the internet and disrupted Ukraine's ability to coordinate and communicate with troops.

One of the key approaches to creating resiliency against kinetic attacks is proliferation, ensuring redundancy and making it much more difficult to completely eliminate satellite communications capacity. This is less effective against cyber-attacks however, which is why we are seeing technology developed to counter them, such as AI-driven cybersecurity and quantum encryption.

AI can be trained on data from past breaches, offering the ability to automatically detect and counter new cyber threats in a way that traditional systems are not able to.

This is a double-edged sword however, as AI can also be used to develop new methods of attack that will confound existing security measures. For this reason, additional security measures are necessary, such as quantum encryption, which is a technology that is still in development.

Quantum encryption utilises a field of physics known as quantum mechanics, relying on the inherently uncertain nature of particles and replacing binary ones and zeroes with specific polarities, or spins, for photons of light. What is key for quantum encryption is that, according to the laws of physics, the basic act of measuring or even observing a quantum system will always cause the system to change. In theory, this could essentially offer a passive defence against attempts to access quantum encrypted data and throw off attempts to manipulate or disable satellite communications.

## Free space optical communications

Traditionally, satellites rely on radio frequency (RF) signals to broadcast GPS or satellite imaging data. Laser-based optical communications offer significant benefits over RF signals, as they enable faster and more secure connectivity.

Fibre optics already offer speed-of-light connectivity, but in many environments laying fibre optic cables is not feasible, such as in space or contested theatres. Many military platforms use RF data links that operate at the speed of old-fashioned modems, so optical satellite communication would be a significant upgrade.

Optical communications also offer increased security over RF signals. RF is broadcasted widely over a pre-determined frequency, making signals susceptible to detection and interception while this is almost impossible for optical communications. Optical lasers travel directly from one platform to another, meaning that anyone hoping to intercept them would need to be physically present in the path of the beam.


**Learn more about how MilSatCom continues to transform warfare at the Global MilSatCom 2024 conference.**

Free to attend for military and government worldwide, this conference, supporting SSAFA, the armed forces charity, is the largest gathering of MilSatCom professionals as it returns for its 26th year.

The conference will feature insightful talks on some of the key topics discussed here, including:

- **Ensuring the Cybersecurity of EU Space Programs and SATCOM Systems** | EU Space Programme Security Accreditation Board
- **Providing Critical SATCOM Capabilities and Services to Enable NATO's Core Tasks** | NATO Communications and Information Agency
- **Utilising Laser Communications Technology to Enhance SATCOM Security** | NASA and TNO