Issue Brief

June 2025
No : 445

Starlink: Its Implications on the Defence Forces

Maj Puneet Singhal

Starlink: Its Implications on the Defence Forces

Abstract

Starlink, a Low Earth Orbit (LEO) satellite system offering internet services developed by SpaceX, has revolutionised global connectivity through its LEO architecture. This article explores Starlink's architecture, its strategic use in the Russia-Ukraine conflict, and its implications for India across strategic, operational and tactical levels. It highlights both the potential benefits, such as connecting remote and underserved communities to the digital world, enhancing disaster resilience as well as critical challenges related to security, sovereignty and regulation.

Keywords. Starlink, Cyber Security, Satellite Internet, Tactical Communication, Satellite-Based Warfare, Space Domain Awareness, Starlink and Cyber Warfare.

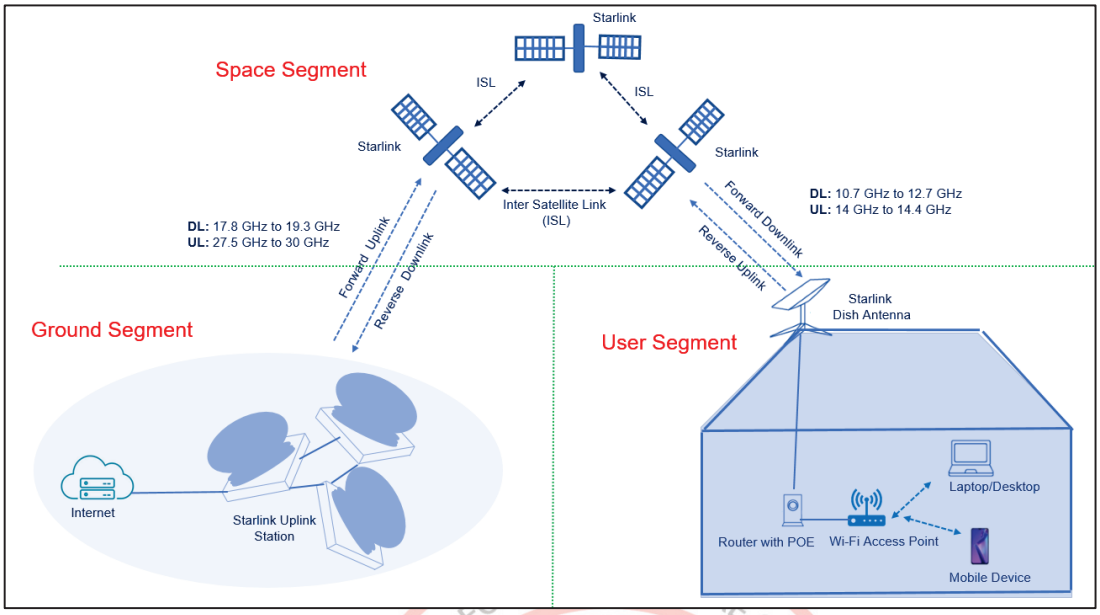
Introduction

Starlink, developed by SpaceX, is a project delivering internet via satellite technology, with the goal of offering high-speed broadband access worldwide. It relies on a large network of Low Earth Orbit (LEO) satellites to deliver internet connectivity, particularly targeting areas that are remote, rural, or lacks reliable infrastructure (Asim, T., 2025), (Pultarova, T.,2025), (Yasar, K., 2024), (Stewart, K., 2025), (ANI 2025) . Initiated by Elon Musk in 2002, SpaceX is a private aerospace company responsible for launching and operating the Starlink satellite constellation. The system is especially useful in regions wherein conventional internet services are limited or unavailable.

Working of Starlink

Starlink functions using satellite based internet technology. Satellite internet, unlike traditional wired connections like fibre optics, relies on radio waves that travel through space. In this system, ground stations send signals to satellites orbiting the Earth, which then transmit the data back down to user terminals on the ground (Yasar, K., 2024).

Figure 1: Working of Starlink



Source: https://www.techplayon.com/starlink-system-architecture/

Figure 2: Advantages of Starlink over other Satellite Communication Network

Feature	Starlink	Traditional Satellite Networks (GEO/MEO/Legacy LEO)	Advantage
Latency	~20–40 ms	~600 ms (GEO), 150–250 ms (MEO)	Near fiber-like latency.
Throughput	Up to 100 - 250 Mbps (consumer)	5 - 50 Mbps typical for GEO consumer services	Higher bandwidth per user.
Coverage	Global (including rural and underserved areas)	GEO - Broad but limited pole-to-pole, MEO - Patchy, LEO - Limited so far	Better polar & remote area reach.
Deployment Speed	Rapid constellation scaling	Single satellite, high cost	Fast to deploy and scale coverage.
User Terminals	Phased-array, self aligning antennas	Often dish based, fixed alignment	Easier installation, mobility-ready.
Resilience to Failures	Mesh network with multiple satellites in view	Single point of failure in GEO/MEO	More resilient & redundant.
Dynamic Routing	Satellites interlink for mesh routing	Often relies on ground station routing	Less ground station dependency.
Uplink/Downlink Flexibility	High-frequency Ka-band & Ku-band	Often Ku-band only (older tech)	More capacity and flexibility.
Innovation & Refresh Rate	New batches of satellites every few months	GEO satellites have 15 - 20 year lifespans	Faster tech refresh and upgrades.
Military & Emergency Use	Proven rapid deployment (eg, Ukraine)	Slower to deploy, less adaptable	Agile for tactical operations.

Source: Prepared by the Author

Starlink introduces several unique innovations in satellite internet technology (Kerifischer, 2024), (Techplayon, 2025):-

- Rather than relying on few large satellites, Starlink comprises of thousands of interconnected small satellites, enhancing coverage and capacity.
- These satellites are positioned in the lower region of Earth's orbital space— just 500 km above the surface, enabling faster data transmission while offering much lower latency than traditional geostationary satellites.
- The latest generation of Starlink satellites are equipped with laser-based communication systems, allowing them to relay signals directly between satellites. This reduces the reliance on ground stations and boosts overall network efficiency.
- With plans to deploy up to 40,000 satellites, SpaceX aims to expand Starlink's reach to even the most remote regions while minimising service interruptions.
- As part of SpaceX, Starlink benefits from frequent, cost-efficient satellite launches— an advantage that gives it scalability and speed unmatched by most competitors.

Figure 3: Technical Specifications of Starlink

Category	Specification
Frequency Bands	Ku-band (10.7–12.7 GHz downlink, 14.0–14.5 GHz uplink), Ka-band
Antenna Technology	Phased-array, electronically steered
Download Speeds	50–250 Mbps (residential); higher for enterprise use
Upload Speeds	10–40 Mbps
Latency	20–40 milliseconds
Temperature Range	-30°C to +50°C operational range
Coverage	Global, including polar regions
Services Provided	• Internet/ Data • VoIP (via 3rd party apps) • Video Conferencing (Works well with Zoom, Teams, Google Meet, etc) • Video Streaming • Cloud & VPN • IoT
Platforms	• Fixed Installations for homes, offices, etc • Maritime & Aviation kits for ships and planes • Starlink Roam service lets you use the dish **on the move**
Inter-Satellite Links	Yes (laser links for v1.5+, enhancing mesh network routing)
Cost	• User Terminal - ₹35,000 to ₹40,000 • Subscription (monthly) - ₹4,500–₹6,000
Security	End-to-end encryption; dynamic beam steering

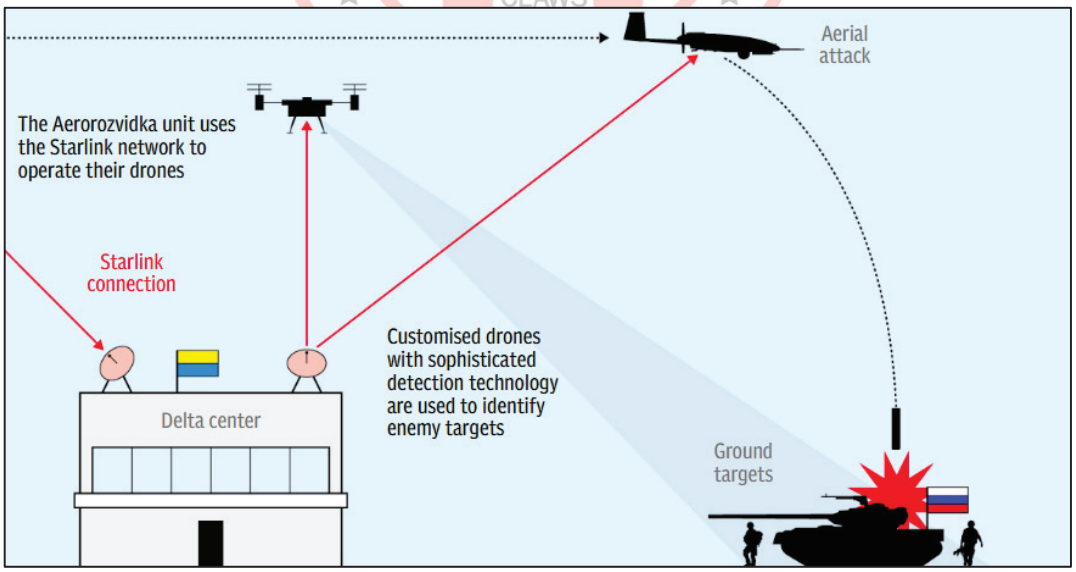
Source: Prepared by Author

Starlink in the Russia-Ukraine War

After Russia's 'military operations' in Ukraine (February 2022), Mykhailo Fedorov, Ukraine's Minister of Digital Transformation, urged Elon Musk to provide Starlink services. Within 12 hours, Starlink satellites were functional in Ukraine (Thakur, V., 2025), (Nick A., and Titcomb, J. 2022) . Starlink played a crucial and highly visible role in the Russia-Ukraine war especially in maintaining communication resilience amid infrastructure destruction. Key roles included:

- ***Restoring Communications.*** When Russian attacks disrupted Ukraine's mobile networks and internet services, Starlink terminals quickly restored essential communication for civilians, hospitals and government agencies (Singh, A., 2024).
- ***Secure Battlefield Communication***. Ukrainian military units used Starlink for encrypted, low-latency communications across front lines, thus helping with command, control and coordination (Singh, A., 2024).
- ***Drone Operations.*** Starlink enabled real-time video feeds and control links for drones used in surveillance, artillery targeting and even direct attacks (Singh, A., 2024), (Nick A. and Titcomb, J. 2022).

Figure 4: Drone Recce using Starlink



Source: https://www.telegraph.co.uk/world-news/2022/03/18/elon-musks-starlink-helping-ukraine-win-drone-war/

Figure 5: Precision Targeting by Ukrainian Drones

Source: https://www.telegraph.co.uk/world-news/2022/03/18/elon-musks-starlink-helping-ukraine-win-drone-war/

- ***Refugee Centres***. Provided internet to displaced populations and refugee aid centres.
- ***Educational Continuity.*** Helped schools, in waraffected areas, to conduct remote learning when possible.

Advantages and Disadvantages of using Starlink during the Russia-Ukraine (Asim, T., 2025)**,** (Singh, A., 2024)**,** (Thakur, V., 2025)**, (**Grover G., 2025)

- ***War Rapid Deployment.*** Within days of Ukraine's request, SpaceX shipped and activated thousands of Starlink terminals across the country.
- ***Decentralised Infrastructure.*** Lack of reliance on fixed infrastructure made Starlink hard to disable through conventional cyber or kinetic attacks.
- ***Resilience to Jamming.*** Russia reportedly attempted to jam Starlink signals, but SpaceX swiftly pushed firmware updates that neutralised these attempts.
- ***Cyber Shielding.*** While not immune, Starlink has proven more sustainable than traditional ISPs due to its encrypted communication channels and mesh-like architecture.
- ***Public-Private Partnership.*** The involvement of SpaceX (a private company) in an active warzone raised questions about influence of private companies in geopolitical conflicts.

- ***Dependency Risk.*** While a lifeline for Ukraine, it also highlighted the risk of over-reliance on a foreign-controlled infrastructure i.e. Elon Musk's influence on operational decisions (e.g., restricting use in specific locations) stirred global debate (Toropin K., 2024), (Thakur, V. 2025), (ANI, 2025).

Implications for India

Recent partnerships between Starlink and Indian telecom giants viz. Bharti Airtel and Reliance Jio and meeting between Starlink officials and Union Commerce and Industry Minister Piyush Goyal on 17 April 2025, marks a significant shift in the country's satellite internet landscape (Travelli, A., 2025), (Sudhir, SNV., 2025).While these collaborations could accelerate connectivity in underserved regions, they also raise serious concerns about national autonomy and strategic dependency. The entry of Starlink in Indian market brings several key implications which are as follows:

Strategic Level

- ***Sovereignty and National Security.*** Reliance on a foreign operated satellite system may compromise strategic autonomy. If Starlink infrastructure is used within India without sufficient control, it could expose critical national communications to surveillance or foreign influence (Patil, BM., 2025), (Grover G., 2025).
- ***Geopolitical Leverage.*** Starlink's involvement in global conflicts (e.g. Ukraine) demonstrates how satellite networks can shift power dynamics. India must ensure that foreign constellations do not provide unintended strategic leverage to adversarial nations (Singh, A., 2024), (Grover G., 2025).
- ***Space Domain Awareness.*** Growing foreign satellite presence in LEO increases the need for India to invest in its own space situational awareness and satellite defence capabilities (Stewart, K., 2025) (Grover G., 2025).

Operational Level

- ***Disaster and Conflict Response.*** Starlink could provide redundant connectivity during emergencies or border conflicts wherein terrestrial infrastructure is destroyed or absent. However, use of Starlink by the adversaries near Indian borders, could also enhance their own resilience and communication (Singh, A., 2024), (Grover G., 2025).

- ***Military Coordination and Communication***. If allowed, Starlink could support non-sensitive operations, such as logistics or humanitarian missions. Despite its advantages, the system remains susceptible to potential monitoring or signal interception, particularly when there is no end-to-end control (Grover G., 2025).
- ***Cyber security Management***. Operational use of Starlink would require robust policies to prevent unauthorised access— jamming, spoofing, or malware propagation through its network into defence systems (Peiwen, W., Huang Z., Kaiyue, Z., 2024), (Patil, BM. 2025).

Tactical Level

- ***Real-Time ISR***.As demonstrated in Ukraine, Starlink can support drone operations and battlefield coordination. India must consider both the advantages of using such a system as also the risks if adversaries deploy similar capabilities near Indian borders (Singh, A. 2024), (Patil, BM. 2025).
- ***Electronic Warfare Vulnerability***. India's tactical communications must be hardened against adversaries using Starlink-like systems to bypass jamming or intercept traditional communication links (Grover G., 2025).
- ***Local Command Communication.*** In remote areas (like Siachen, Northeast), tactical units could benefit from satellite based communication, thus improving situational awareness and decision making speed (Patil, BM. 2025).

Security Threats for Defence Forces

The integration or exposure to foreign satellite communication systems, like Starlink, introduces several potential risks for the defence foreces. These threats span across physical, cyber, and electromagnetic domains, hencemust be addressed comprehensively (Singh, A. 2024), (Peiwen, W., Huang Z., Kaiyue, Z., 2024), (Grover G., 2025).

- ***Data Interception and Surveillance.*** Communications routed via foreign operated satellites are constantly at risk of being intercepted or monitored by the host country or malicious actors. Even encrypted transmissions may be vulnerable to traffic analysis, metadata collection, or future decryption with advancements in computing (e.g. quantum computing) (Peiwen, W., Huang Z., Kaiyue, Z., 2024).
- ***Operational Security Risks.*** Use of such systems can inadvertently reveal troop movements, logistical patterns, or tactical plans. Persistent satellite coverage creates a risk

of constant location exposure for ground forces using connected devices (Singh, A. 2024), (Grover G., 2025).

- ***Electronic Warfare and Signal Manipulation*.** Foreign operated satellites may be susceptible to spoofing, jamming, or signal redirection, creating false situational awareness for Indian units or degrading their ability to communicate. Adversaries with access to similar satellite systems could establish resilient command and control in contested areas (Peiwen, W., Huang Z., Kaiyue, Z., 2024), (Grover G., 2025).
- ***Cyber security Exploits*.** Terminal devices and backend infrastructure could be compromised to plant malware, initiate DDoS attacks, or create backdoors into defence communication networks. Firmware level vulnerabilities in user terminals could be exploited without direct physical access (Peiwen, W., Huang Z., Kaiyue, Z., 2024).
- ***Dependency on Foreign Infrastructure.*** Amid crisis or conflict, access to foreign satellite services may be restricted, delayed, or denied, severely impacting critical missions. For instance, denial of GPS data by USA during the Kargil War highlights the risks of relying on foreign systems (Grover G., 2025). Such dependencies reduce strategic autonomy and could be used as leverage in diplomatic or military standoffs.

Key Recommendations for India

- Invest in domestic LEO satellite networks to ensure strategic autonomy and reduce foreign dependency.
- Implement clear policies and licensing requirements for foreign satellite internet services operating in India.
- Mandate regular security audits and enforce strict operational restrictions on Starlink terminals, particularly in border regions and strategically sensitive areas to prevent unauthorised access and data breaches.
- Support Indian startups and public-private collaborations to create homegrown solutions.

Case Study: Potential Exploitation of Starlink in Urban Terror Attacks Similar to 26/11 Scenario.

The proliferation of satellite based internet services such as Starlink marks a significant shift in global communication capabilities. Designed with the goal of connecting underserved and hard-

to-reach locations, this Low Earth Orbit (LEO) satellite constellation offers strategic advantages for development and disaster response. However, in the absence of strong regulatory controls, these technologies may also be exploited by malicious actors. A hypothetical replication of a 26/11 type attack highlights the critical vulnerabilities posed by unrestricted access to such services.

Phase I

- ***Infiltration and Setup.*** Using a refurbished fishing trawler, operatives approach target country's waters under the guise of commercial activity. Hidden onboard is a Starlink user terminal, powered by a compact generator that is connected to ruggedized laptops. The Starlink terminal self-aligns with the satellite network, providing high-speed encrypted internet directly via satellite and bypassing terrestrial infrastructure completely.
- ***Security Challenge: Bypassing Surveillance.*** No cellular tower pings. No ISP logs. Intelligence agencies monitoring domestic networks remain unaware of any operational traffic.

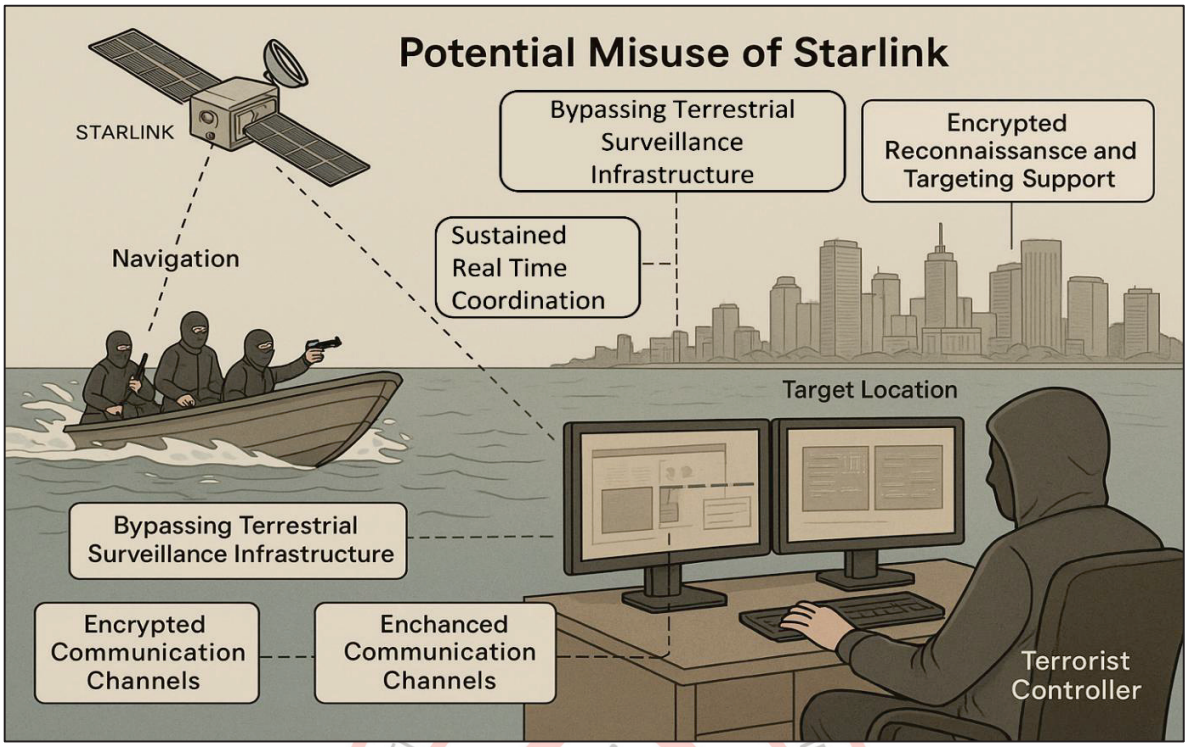
Phase II

- ***Real-Time Coordination.*** Once near shore, the operatives split into small mobile teams across the city. Equipped with rugged smartphones and communication headsets linked to a mesh network powered by the Starlink connection— they stay in continuous contact with a remote handler stationed in a foreign country.
- ***Security Challenge: Sustained Real-Time Coordination***. Despite jammers activated in response to initial events, the team faces no disruption. Starlink's LEO satellites offer low-latency, high-bandwidth coverage that remains functional in blackout conditions.

Phase III

- ***Tactical Intelligence and Reconnaissance.*** Before the actual attack, the teams use off-the-shelf drones integrated with GPS and mobile video to scout and stream live footage of critical targets viz. a naval facility, a stock exchange and major transit stations. The handler, sitting thousands of kilometers away, receives HD video feeds, tags GPS coordinates, and sends back tactical suggestions, all within seconds.
- ***Security Challenge: Enhanced Reconnaissance and Targeting.*** This kind of direct, encrypted communication network allows the adversary to plan dynamically in real time.

Figure 6 : Potential Misuse of Starlink



Source: Prepared by Author

Phase IV

- ***Encryption and Evasion***. Law enforcement attempts to triangulate communication or tap into local networks. However, end-to-end encryption over Starlink's private mesh thwarts all such attempts.
- ***Security Challenge: Encrypted Channels.*** Even as ground response teams activate, they're moving blind —unable to anticipate shifts in the adversaries' plans.

Phase V

- ***Concealment and Mobility.*** As operations escalate, one Starlink terminal is hidden inside a parked vehicle, while another is deployed on a building rooftop. These remains operational, concealed under tarps and camouflaged as HVAC equipment.
- ***Security Challenge: Terminal Mobility.*** Unlike large satellite dishes of the past, these terminals are portable, self-configuring, and can operate without fixed power infrastructure— they are difficult to detect with traditional signal triangulation methods.

Conclusion

Starlink is changing how the world connects to the internet by offering fast, satellite based coverage in even the most remote regions. For India, this technology can be a game changer in narrowing the digital divide, especially in rural and disaster prone areas. It can also support sectors like healthcare, education, and emergency services where traditional internet access is limited. However, relying on a foreign operated satellite system brings serious concerns including national security risks, data privacy issues, and lack of control during critical situations. India must also be cautious about becoming too dependent on foreign infrastructure, especially when geopolitical tensions are involved. By balancing innovation with security and sovereignty, India can make the most of satellite internet while protecting its national interests.

Works Cited

ANI, (2025, March 15). Starlink's satellite broadband poses limited threat to Indian telcos: Report. *The Economic Times*. https://economictimes.indiatimes.com/industry/telecom/telecom-news/starlinks-satellite-broadband-poses-limited-threat-to-indian-telcos-report/articleshow/119035643.cms.

Asim, T. (2025, February 17). The Privatization of Warfare:https://thedialectics.org/the-privatization-of-warfare-role-of-starlink-in-the-russia-ukraine-war/.

Grover G., (2025, April 17). The National Security Implications of Starlink's Entry Into India. *The Diplomat*. https://thediplomat.com/2025/04/the-national-security-implications-of-starlinks-entry-into-india/.

Kerifischer (2024, October 6). Starlink Explored: A Complete Guide on Benefits and Drawbacks. *Code of Entry*. https://codeofentry.com/starlink-explored-a-complete-guide-on-benefits-and-drawbacks/.

Nick A., Titcomb J. (2022, March 18). Elon Musk's Starlink helping Ukraine to win the drone war. *Telegraph.com*. https://www.telegraph.co.uk/world-news/2022/03/18/elon-musks-starlink-helping-ukraine-win-drone-war/.

Patil, BM. (2025, March 12). Starlink And Indian National Security. *DefenceXP*. https://www.defencexp.com/starlink-and-indian-national-security/.

Peiwen, W., Huang Z., Kaiyue, Z. (2024). Starlink Militarization: Challenges and Responses to Space Intelligence and Information Security. *Center for Strategic & International Studies*. https://interpret.csis.org/translations/starlink-militarization-challenges-and-responses-to-space-intelligence-and-information-security/.

Pultarova, T. (2025, June 4). Starlink satellites: Facts, tracking and impact on astronomy. *Space.com.* https://www.space.com/spacex-starlink-satellites.html.

Singh, A. (2024, March 2). The Role of Starlink During Military Conflict. *Defence Research and Studies*. https://dras.in/the-role-of-starlink-during-military-conflict/.

Stewart, K. (2025, May 19). Low Earth Orbit. *Britannica*. https://www.britannica.com/technology/low-Earth-orbit.

Sudhir, SNV. (2025, March 12). Former bureaucrat raises concerns over Starlink's India entry, writes to DoT. *Deccan Herald*. https://www.deccanherald.com/india/former-bureaucrat-raises-concerns-over-starlinks-india-entry-writes-to-dot-3443918.

Thakur, V. (2025, February 24). Starlink Shutdown In Ukraine – How Badly Would Ukrainian Military Be Hit If Musk Turns-Off The "Trump Card"? *The EurAsian Times*. https://www.eurasiantimes.com/starlink-shutdown-in-ukraine-how/.

Toropin K. (2024, November 15). *Military.com*. https://www.military.com/daily-news/2024/11/15/pentagon-silent-elon-musk-and-starlink-risks-military-use-expands.html.

Travelli, A. (2025, March 13). Elon Musk's Starlink Pushes Its Way Into India. *The New York Times*.https://www.nytimes.com/2025/03/13/business/starlink-india-musk.html.

(2025, May 23). SpaceX – Starlink System Architecture for Internet. *Techplayon*. https://www.techplayon.com/starlink-system-architecture/.

About the Author

Maj Puneet Singhal was commissioned into Corps of Army Air Defence in Mar 2018. He is an alumnus of OTA, Chennai. The officer has served in High Altitude Areas along LAC in Eastern Ladakh and LoC in J&K, Counter Insurgency areas of J&K and deserts. Presently, the officer is tenating the appointment of System Manager in Research & Capability Development (RACD) Wing, Mhow.