ARTICLES

# Starlink and Commercial Satellite Networks in Conflict Zones: The Future of Military Communications

**Author:** Jaggari Veera Sai Krupakar • **Published:** June 19, 2026 • **Source:** Centre for New Age Warfare Studies



**EXECUTIVE BRIEF & KEY FINDINGS**

*The emergence of commercial satellite internet networks most notably SpaceX's Starlink has changed the landscape of modern conflict. This article examines how these systems are transforming military operations, challenging traditional ideas of state sovereignty and creating new strategic vulnerabilities. Drawing on evidence from the Current Russia Ukraine war. This article analyses how satellite connectivity reshapes command and control structures, empowers non state actors and forces governments to rethink their military policies. It also draws lessons for India regarding indigenous alternatives and integrated military communication planning.*

## 1. Introduction: A New Dimension of Warfare

When Russian forces invaded Ukraine in February 2022 few analysts anticipated that one of the most decisive factors on the battlefield would be an internet service provided by a private American company. Within days of the invasion SpaceX activated Starlink terminals across Ukraine giving soldiers and civilians access to high speed satellite internet even as conventional infrastructure was bombed into rubble. That moment marked a turning point not just for Ukraine but for how the world thinks about communications in war.[3]

Commercial satellite internet is no longer a civilian convenience. It has become a tool of military power, state strategy and geopolitical competition. Starlink alone operates over 6000 satellites in low Earth orbit (LEO) providing low latency broadband to users anywhere on the planet. As these systems use multiplies they are raising urgent questions about who controls communications in wartime, what happens when private companies become essential military partners and how states can protect themselves from new kinds of vulnerability.

This article addresses these questions by examining six interconnected themes .How satellite networks are transforming military operations, how they have altered command and control, what operational advantages they provide, how they challenge state sovereignty ,what new vulnerabilities they introduce, how major powers are adapting their military doctrines and what lessons India should draw for its own strategic planning.

## 2. How Commercial Satellites Are Transforming Military Operations

Traditional military communication relied heavily on fixed infrastructures like fibre cables, ground stations and military satellites all of which are expensive, limited in coverage and very vulnerable to attacks. Commercial Low Earth Orbit(LEO) satellite networks like Starlink have disrupted this model by offering wide area connectivity at a fraction of the cost.In Ukraine Starlink terminals have been used to coordinate drone, strikes transmit real time intelligence and maintain secure voice communications between frontline units and headquarters. Ukrainian soldiers have credited the system with giving them a significant tactical advantage particularly in fast moving operations where traditional radio communications proved inadequate or easily jammed.

The operational benefits are not limited to voice and data. Commercial satellite imagery from companies like Planet Labs and Maxar has provided real time reconnaissance to Ukraine supplementing military intelligence and enabling precision strikes. This convergence of commercial connectivity and imagery marks a new era in which the battlefield is monitored and managed largely through civilian infrastructure.[44]

## 3. Altering Command and Control in Recent Conflicts

Command and control(C2) the ability of military commanders to direct forces and gather information has always been a decisive factor in warfare. Historically destroying the enemy's C2 infrastructure was a primary strategic objective. Commercial satellite networks are making this task much harder.

Because LEO satellite constellations consist of hundreds or thousands of individual satellites they are very resilient to the kind of targeted attacks that can knock out fixed communication towers or military satellites. Even if several terminals or individual satellites are destroyed the network reconfigures around the loss maintaining connectivity.

In Ukraine this resilience has had concrete consequences. Russian forces struggled to degrade Ukrainian military communications in the way they had planned partly because Starlink allowed units to operate with decentralised distributed networks rather than relying on a few central nodes. Commanders could remain in contact with smaller units even when those units were operating deep behind enemy lines or in areas of heavy electronic warfare.This has begun to reshape military thinking worldwide. Armies are reconsidering the value of centralised communication hubs and investing in distributed satellite connected architectures that can survive degradation and still function effectively.One of the key example is Ukrainian drone operators have used Starlink to maintain data links with drones operating at long ranges enabling precision strikes on armoured vehicles, supply depots and command posts. This integration of consumer grade satellite internet into military drone operations is considered unprecedented in modern conflict history.

## 4. Operational Advantages for Military and Non State Actors

The most strategically significant aspect of commercial satellite internet is how it democratises access to advanced communications. Historically only well funded states could afford the satellite infrastructure needed to sustain military operations across large areas. Commercial satellite networks are changing this calculus for both state and non state actors.

For state militaries the advantages are clear rapid deployment of communication networks without the need for ground infrastructure, global coverage including in remote areas and cost savings compared to operating dedicated military satellites. The United States military has been expanding its use of commercial satellite services under programmes that blend military and commercial assets.

For non state actors the implications are more complex. The same terminals that helped Ukrainian defenders resist a large military invasion can be used by any armed group with access to commercial technology. There have already been documented cases of Starlink terminals appearing in conflict zones in Sudan and the Middle East outside of any formal military agreement raising serious concerns about proliferation.

The barriers to acquiring military grade communications capability have never been lower. A relatively small armed group with access to a commercial satellite terminal and a modest budget for bandwidth can now maintain encrypted resilient communications that would have been beyond the reach of most national armies two decades ago.

## 5. Challenging State Sovereignty Over Communications

Governments have exercised strong control over the communications infrastructure within their borders. Licensing regimes, spectrum management and the power to shut down networks during emergencies are all tools through which states assert sovereignty over the information environment. Commercial satellite internet challenges this control in fundamental ways.

Because LEO satellite signals are delivered from space they can in principle bypass national internet gateways and the filtering systems that governments use to control information flows. Starlink has been used by activists in Iran and Russia to access uncensored information despite government restrictions a use that authoritarian governments view as a direct threat to their control.

This creates a new form of tension between the sovereign rights of states and the global reach of private commercial operators. Elon Musk's decisions about where to activate Starlink including a reported refusal to enable coverage over Crimea to prevent a Ukrainian drone attack on the Russian fleet demonstrated that a single private individual can exercise what amounts to strategic influence over a military conflict. This is an unprecedented and deeply uncomfortable reality for governments and military planners.[5]

The question of sovereignty also extends to data. Satellite communications generate large volumes of data about user locations, communication patterns and network behaviour. When these networks are operated by foreign private companies governments must grapple with who has access to that data and under what legal frameworks.

## 6. New Vulnerabilities in Wartime Communication

While commercial satellite networks offer significant advantages they also introduce new categories of vulnerability that military planners are only beginning to fully appreciate.

### 6.1 Dependence on Private Actors

Ukraine's experience illustrates both the value and the risk of relying on a commercially operated network. The decision making of a private company including about pricing, coverage and operational parameters can have direct consequences for military operations. Reports that SpaceX geofenced certain Starlink capabilities to limit Ukrainian military use highlighted how dependence on private infrastructure creates a new kind of strategic vulnerability.

### 6.2 Electronic Warfare and Signal Jamming

Russia deployed sophisticated electronic warfare systems to jam Starlink signals with mixed results. SpaceX responded with software updates to increase resistance to jamming demonstrating that the cyber and electronic warfare dimensions of satellite communications will continue to evolve rapidly. This also signals an escalating arms race between satellite communication systems and the technologies designed to disrupt them.

### 6.3 Cyber Attacks on Ground Infrastructure

At the very start of the Ukraine war a cyberattack attributed to Russia disrupted the Viasat KA-SAT satellite network knocking out communication for thousands of users including military systems across Ukraine and few parts of Europe. This demonstrated that even space based communications are vulnerable to cyber attacks targeting ground infrastructure such as gateways and control systems.[6]

## 7. How Major Powers Are Adapting Their Military Doctrines

The lessons of Ukraine have been absorbed rapidly by major military powers each of whom is adapting doctrine to account for the new reality of commercial satellite dominance in communications.

The United States has formally integrated commercial satellite services into its military architecture. The US Space Force is developing frameworks for blending military and commercial space assets recognising that relying solely on expensive military satellites is no longer sufficient or cost effective. The Pentagon has also explored how to protect commercial satellite assets it depends on including by designating them as potential targets for adversary action and factoring that into planning.

China has responded by accelerating its own LEO satellite constellation programme the Guowang (GW) megaconstellation which aims to deploy over 13,000 satellites. Chinese military and academic publications have openly discussed Starlink as a potential military threat and have published research into counter satellite technologies including laser weapons and signal spoofing techniques.[7]

Russia despite its own limited commercial satellite capacity has integrated electronic warfare, cyber capabilities and anti satellite weapons into its doctrine as a counter to Western satellite dominance as demonstrated in Ukraine.

NATO has begun developing a space doctrine that recognises satellite communications as critical infrastructure extending the alliance's collective defence commitments to include attacks on space based assets.

## 8. Lessons for India: Indigenous Alternatives and Military Integration

India occupies a unique strategic position in relation to commercial satellite internet. It is a major space power with a well established national space agency, a fast growing private space sector and significant military communication needs spanning a vast territory and challenging terrain from the Himalayas to island territories across two oceans.The

lessons of Ukraine carry direct relevance for India's defence planning:

### 8.1 The Risk of Foreign Dependency

India has been cautious about allowing foreign commercial satellite operators to provide services that could touch military or government communications. Starlink's entry into the Indian market has been subject to prolonged regulatory review reflecting concerns about data sovereignty, spectrum allocation and the broader question of strategic dependence on a foreign private operator. Ukraine's experience demonstrates why these concerns are legitimate but also why the benefits of such connectivity cannot be ignored.

### 8.2 ISRO and the Private Space Sector

India's Indian Space Research Organisation (ISRO) and the growing private sector under Indian National Space Promotion and Authorisation Centre (IN-SPACe) framework offer a pathway to building indigenous satellite communication capability. Startups like OneWeb India and domestic players such as Dhruva Space are beginning to build local capacity though India still lags significantly behind in LEO constellation deployment.[8]

### 8.3 Military Communication Integration

The Indian military's communication architecture traditionally built around ground based systems supplemented by a small number of dedicated military satellites which requires urgent modernisation. The experience in Ukraine shows that future conflicts will demand resilient and distributed satellite based communication that can survive electronic warfare, kinetic strikes and cyber attacks. India's Defence Research and Development Organisation (DRDO) and the armed forces should prioritise satellite communication integration in next generation doctrine particularly for high altitude and island defence scenarios.

8.4 Anti-Satellite and Counter-Electronic Warfare Capabilities

India's demonstrated anti satellite capability through Mission Shakti in 2019 positions it as one of a handful of nations with the ability to physically target satellites.As Ukraine shows the most practical counter satellite strategies in modern conflict involve electronic warfare, cyber operations and the ability to harden one's own systems against such attacks. India must develop a comprehensive space warfare doctrine that integrates these dimensions.[9]

## 9. Conclusion

Commercial satellite internet networks have crossed a threshold. They are no longer simply civilian services that occasionally get pressed into military use they are strategic infrastructure that shapes the outcomes of conflicts, challenges the traditional monopoly of states over communications and forces governments worldwide to rethink their doctrines, procurement and alliance frameworks of satellites .The Russia Ukraine war has provided the most detailed real world test of these dynamics so far and the lessons are stark satellite connectivity can decide battles, private companies exercise geopolitical power, dependency on foreign commercial operators creates new vulnerabilities and states that lack indigenous alternatives are strategically exposed.[2]

For India the imperative is clear. Investment in indigenous LEO satellite constellations, integration of commercial and military satellite communications, development of electronic and cyber counter measures and the establishment of a clear regulatory framework for foreign satellite operators are not optional upgrades they are strategic necessities for a nation that seeks to protect its sovereignty and military effectiveness in the conflicts of the 21st century.

## End Notes

1. SpaceX, Starlink, commercial satellite internet system and constellation information.

2. United States Institute of Peace, Starlink, Ukraine, and the Future of Conflict, 2023.

3. Reports on Starlink activation in Ukraine following the 2022 Russian invasion.

4. Planet Labs and Maxar Technologies imagery support during the Ukraine conflict.

5. Reporting and analysis regarding Starlink coverage decisions over Crimea.

6. European Union Agency for Cybersecurity (ENISA), Threat Landscape: Cyberattacks against Satellite Communications, 2022.

7. China Aerospace Studies Institute, China's Space Narrative and the Guowang Satellite Constellation, 2023.

8. Indian Space Research Organisation (ISRO), Annual Report 2022–23.

9. Government of India assessments and reports regarding Mission Shakti and space security.

## References

Center for Strategic and International Studies (CSIS). Space Threat Assessment 2024. Washington, DC: Center for Strategic and International Studies, 2024.

China Aerospace Studies Institute. China's Space Narrative and the Guowang Satellite Constellation. Maxwell Air Force Base, AL: China Aerospace Studies Institute, 2023.

Defence Research and Development Organisation (DRDO). DRDO Annual Report 2022–23. New Delhi: DRDO, 2023.

European Union Agency for Cybersecurity (ENISA). Threat Landscape: Cyberattacks against Satellite Communications. Athens: ENISA, 2022.

Indian National Space Promotion and Authorisation Centre (IN-SPACe). Indian Space Ecosystem and Private Sector Participation Report. Ahmedabad: IN-SPACe, 2024.

Indian Space Research Organisation (ISRO). Annual Report 2022–23. Bengaluru: ISRO, 2023.

Rajagopalan, Rajeswari Pillai. India's Space Security Challenges and Opportunities. New Delhi: Observer Research Foundation, 2023.

United States Institute of Peace. Starlink, Ukraine, and the Future of Conflict. Washington, DC: United States Institute of Peace, 2023.

*?The views expressed are those of the authors and do not represent the views of CNAWS.*

*Image Source: ChatGPT*